Anti-Money Laundering/Countering the Financing of Terrorism

Typologies from a Jersey perspective

28 October 2008

Produced by BakerPlatt on behalf of the Law Officers, Joint Financial Crimes Unit and the Jersey Financial Services Commission

CONTENTS

1. Introduction

The Anti-Money Laundering/Countering the Financing of Terrorism Strategy Group (the "AML/CFT Strategy Group") published, on 17 October 2008, an Island strategy to counter money laundering and the financing of terrorism.

As part of its goals, the AML/CFT Strategy Group, has identified a need to "raise awareness of typologies[1] that are relevant to Jersey including the risks arising from the nature of the customer base and products associated with Jersey as an international finance centre."

An excerpt from the strategy document dealing with the issue of typologies is at **Appendix 1** and forms the basis for the production of this document.

2. Structure of the document

This document draws on two principal sources of information:

- Information based on cases which have been prosecuted locally drawing upon case and sentencing summaries and conclusions used in the cases and from direct input from those who were involved in the prosecutions (**Section 3**); and

- Information based on international cases and publicly available typology studies, principally from the FATF Working Group on Typologies and its predecessors and/or equivalents (**Section 4**).

Given the direct relevance of locally prosecuted cases which have led to convictions and/or asset forfeitures under local legislation, these cases have been isolated in a separate section. The case summaries in these situations are longer in nature than found in similar exercises due to their complexities circumstances and the need to identify key lessons for the finance industry.

Accordingly, each local case analysis is structured as follows:

- Synopsis of the facts of the case;

- An analysis of the lessons that can be learned.

[1] i.e. the methods used by money launderers and those who seek to finance terrorism

To the extent that no local cases are available which are relevant to the local finance industry, international cases and publicly available typology studies are used.

Section 5 of the document deals with emerging trends in the area of AML/CFT so that the local finance industry is aware of potential developments against which they may need to guard.

3. Local case analysis

Summary of case studies and their applicability to each industry sector:

	Financial service sector				
	Banking Business	**Funds**	**Insurance Business**	**Investment Business**	**Trust company Business**
Case study number					
1	√	√		√	√
2	√				√
3	√			√	√
4	√		√		
5	√			√	√
6	√				√
7	√				√
8	√	√		√	
9	√				√

3.1 Case study 1

Between 1988 and 1993 investors put up funds in various schemes, having been given the expectation that if they did so, the value of their invested funds would increase through profitable trading on foreign exchange markets. This was entirely false and the investors lost a large proportion of their investments through highly leveraged and unsuccessful foreign exchange trading.

Mr X was a foreign exchange dealer with investor funds placed at XYZ Bank. Mr X claimed to make large profits that transpired to be bogus. Mr X received commissions based on the notional amount of currency traded which he shared (on an undisclosed basis), with XYZ Bank. This resulted in the rapid expansion of XYZ Bank's foreign exchange department and a large increase in profits attributable to foreign exchange.

The profits claimed to have been made by Mr X for the investors were purportedly audited by a partner of a highly reputable firm of accountants for which 'certificates' were issued. No audit or meaningful check was ever carried out on Mr X's trading results.

Clients of Mr X were solicited by a money management group whose central message was that the investment was safe, conservative and profitable, with stop loss limits imposed in order to limit client exposure. The investment schemes were promoted through literature and also investment forums in exotic locations. Critically, XYZ Bank's representatives attended and spoke at these forums, promoting the schemes, despite the bank's knowledge of the losses.

As an added layer of protection, investors were also told that there was an independent trustee of their funds, ABC Trustees. During the relevant period the trustee failed in his duties and simply relied on the trading reports received from Mr X and did not seek to independently corroborate the results with XYZ Bank. XYZ Bank regularly sent bank statements to Mr X but not to ABC Trustees. Mr X provided false valuations to ABC Trustees.

Due to Mr X's losses, concerns were raised by an XYZ Bank account manager in two memoranda to senior management, neither of which led to any action by the bank. XYZ Bank's main concern was the potential impact of the loss of investors and lower foreign exchange dealing levels may have on the bank's profits as opposed to any concern for investors. As the funds dwindled, XYZ Bank informed ABC Trustees who in turn confronted Mr X. Mr X

claimed he had purchased 'options' which would offset his losses and put up a series of explanations and undertook a number of other actions in order to buy himself more time.

Ultimately, these led to criminal convictions against Mr X, the 'auditor' and XYZ Bank involving lengthy custodial sentences and significant fines.

Lessons learned:

- Lack of understanding of the full picture concerning the identity and role of the parties concerned in the management of funds. A failure by parties involved, principally XYZ Bank and ABC Trustees to recognise their obligations to discharge their functions and responsibilities to investors. Relationships between parties involved in investment funds, the fiduciary sector and the banking industry should be clearly identified and documented with a clear and coherent governance and control structure.
- The case highlights the integrated nature of Jersey's finance industry in that financial crime can often be committed using a number of sectors of the finance industry, whether locally based or abroad – in this case banking, investment management and fiduciary services. To believe that typologies exist in a vacuum is to underestimate the inter-dependencies of service providers.
- Despite the bank being aware of the apparently poor trading results and the lack of requests for redemptions from investors, it took no further action.
- Over dependence on key customers for revenues leading to a financial service business to acquiesce to customer demands for fear of losing revenues and profits.
- Basis for revenue generation – profits and revenue, the latter basis which encouraged churning.
- Failure to disclose fees payable out of trading profits which provided a motive to claim bogus profits.
- Involvement and use of credibility of highly reputable institutions to give a veneer of respectability, notwithstanding the fact that the role of these institutions is less involved than might otherwise be held out to be.
- Misleading literature which bore no relation to reality.
- Over reliance by parties on a single source of information, Mr X. Concentration of power in one individual with no effective oversight on a key process, namely valuations.

- Importance of training and vigilance of staff as evidenced by the memorandum sent from XYZ Bank's account manager to his managing director.
- The international nature of Jersey's finance industry was illustrated in this case, involving Jersey, Guernsey, Bermuda, Switzerland, Canada, England, Australia, Holland and various North American states. Extra vigilance should be employed by Jersey based finance professional in conducting due diligence on parties to arrangements, not only from an AML/CFT perspective, but also from a business, reputational and legal perspective.

3.2 Case study 2

Miss X was convicted under the Drug Trafficking Offences (Jersey) Law 1988 of knowingly possessing the proceeds of another person's drug trafficking and therefore assisting in the laundering process.

Miss X was in a relationship with her long term boyfriend, Mr Y, who was a significant drug dealer and who was in the process of organising a sizeable importation of heroin into Jersey. Mr Y was also connected to other subsequently prosecuted local drug dealers. Miss X's bank account was used as a medium through which Mr Y's drugs money could pass.

More importantly, Miss X was more presentable than Mr Y and worked at a responsible job in a trust company for limited periods each year as an assistant trust administrator, studying successfully for professional exams. She had no record of convictions and was above suspicion.

However, intelligence revealed she was aware of Mr Y's activities and through an analysis of banking records a 'surplus' of cash of over £20,000, which could not be explained by legitimate sources, was indentified. The 'surplus' cash was used, in part, to pay for the usual necessaries and in part to fund travel so that she could afford not to work for parts of the year. There was no evidence of lavish expenditure and no permanent fund was created which could be confiscated. The explanations provided by Miss X for this surplus did not bear closer scrutiny and she was convicted.

Lessons learned:

- Drug dealing in Jersey often involves a series of local importers and distributors. Attention should be given to those involved in businesses which could be used as a cover to import products.
- The use of close relatives or partners who have unblemished and often highly reputable jobs enables money launderers to use these individuals as cover in order to wash proceeds of crime through their bank accounts.
- Although the sums involved in the above case study were relatively small, had the bank had a clear picture of Mrs X's employment patterns and knowledge of her salary, the bank would have been able to identify anomalous payments in to her account. Further,

had the bank had a heightened level of sensitivity to cash transactions, it may have been in a position to file an SAR at an early stage.

- Whilst the presence of high value goods and an extravagant lifestyle, beyond the means of the individual's current economic profile, can be a valid indicator of money laundering, their absence does not necessarily mean the opposite.
- The case highlights the integrated nature of Jersey's finance industry in that financial crime can often be committed involving a number of sectors of the finance industry – in this case banking and fiduciary services (the latter to the extent that Miss X was an employee of a trust company)..

3.3 Case study 3

XYZ plc was listed on the London Stock Exchange and had a highly successful track record in e-commerce. With the decline of the e-commerce sector in the early part of the decade, the company ceased to be a going concern and wound down it operations, albeit with some £30m of accumulated profits in the bank.

At this stage, the board of XYZ plc appeared to have little direction – directors barely met, there were successive resignations month to month, there was no audit committee and the advice of non-executive directors was ignored. Mr X and Mr Y (the former having had a previous conviction for 'borrowing' company pension funds and the latter being a convicted fraudster) had two associates on the board of XYZ plc, put in place through a minority, although significant, holding in the company. Through these associates, Mr X orchestrated the moving of the company's money to an account in Jersey – to company accounts under Mr X's control. When a new chairman of XYZ plc asked about the whereabouts of the company's money, he was presented with a forged bank statement by one of Mr X's associates, who effectively acted as XYZ plc's finance director.

Despite not being on the board of XYZ plc, Mr X exerted considerable control over it through his associates and also via his shadow director activities through the company which was invested in XYZ plc. Mr X attended all board meetings (bar one) and also all other significant business meetings, including the removal of two non-executive directors.

XYZ plc's monies, once held in ABC Bank Limited in Jersey in a company account under Mr X's control, were then distributed to companies connected to Mr X. In relation to the account which was operated by XYZ plc at ABC Bank Limited, this was purported to have been opened pursuant to a board meeting signed by three individuals who were described as directors of XYZ plc (two of whom were Mr X's associates). There had, in fact, been no board meeting and none of the signatories held the positions they claimed at the time of the purported board meeting. There were further legal disputes as to the operation of the mandate concerning ABC Bank Limited's duty of care.

Lessons learned:

- A lack of corporate governance, even for a company which has little by way of ongoing activity, can expose it to abuse. This is primarily due to a lack of communication, control and oversight of the company's operations, which can make it vulnerable to exploitation to criminals who can identify an opportunity to exploit it.
- Vetting of board members. Detailed due diligence on board members is required in order to identify potential links with individuals who would otherwise not be employed by a company in such a capacity. By using internet based tools which are available to the finance industry, it is possible to identify such associations independently of the director concerned (i.e. without relying on self disclosure) and pick up on issues which would ordinarily not be reported..
- Shadow directors of investor companies and also of companies which are undertaking business in Jersey should be identified. Although not formally on the record as a director, it was clear Mr X was a de facto director and should have been treated as such or, more properly, dealt with as according to his formal status and his influence limited. This links in to the lack of corporate governance referred to above.
- Non-executive directors are of critical importance in any governance structure in order to provide an external, objective view of the company. In this case Mr X removed two non-executive directors as he felt they represented a threat to his influence. Equally, non-executive directors who are brought in by the chairman or figures with significant influence (such as Mr X) should be subjected to tests of independence so that they do not simply act as 'yes men'.
- Failure to disclose conflicts of interest. Although it is highly improbable that a money launderer would disclose any conflicts of interest which would jeopardise his activities, it remains a central tenet that conflicts of interest should be disclosed and a register of directors' interests maintained in order to identify potential conflicts.
- In relation to a bank's duty of care, banking institutions need to carefully examine whether they are exercising the necessary skill and care of a reasonably competent bank. This is especially so when dealing with high value, one off transactions involving newly opened accounts. In essence, banking institutions need to ensure that those giving instructions have been validly appointed, that instructions given by parties are those parties who are on the mandate and that directors are acting bona fide in the best interests of the company. Failure to consider, in detail, a banking institution's procedures in opening and maintaining accounts, corporate or otherwise, can lead to significant claims for breach of contract and/or negligence.

3.4 Case study 4

Mr X was convicted by a jury for offences of fraudulent accounting. He had pleaded guilty at an earlier stage to a number of smaller offences of fraud. He was sentenced to 3½ years' imprisonment in total. The total amount of the false entries proved was in the region of £300,000.

Mr X was a director of an insurance broker in Jersey and latterly a shareholder therein. He was in a very trusted position and had a wide discretion in terms of arranging insurance business and accounting for that business within the books of the insurance broker. He worked with a considerable degree of autonomy. Between 1997 and 2000 he placed numerous false entries in the books to hide the results of transactions for which he was responsible. The result was to give the false impression that his work for the insurance broker was profitable and that the business was in good financial health. The truth, concealed from the books, was that by 2000 the company owed large amounts of money to various companies and that it was insolvent.

The trial concerned entries relating to building insurance placed over four years in relation to a large UK property management company. The commissions available in such business are very large but Mr X promised to pay more of it out to others than could be funded from insurance premiums paid. He paid everyone out, such that the insurance broker bore the loss - but he hid this from the books by placing false entries in the client accounting system, understating the amounts paid out to insurers and introducers and painting a wholly false picture of the transactions he had entered into.

Mr X's motivation in making transactions that were unprofitable for the insurance broker was to keep clients and insurers happy when he had made promises that he could not keep. His motivation in hiding the reality from the insurance broker's books was to keep his employers happy and earn bonuses. Of his remuneration in the relevant years, the far greater proportion was made up of bonus and dividend payments.

The smaller counts of fraud to which he pleaded guilty involved deception of individual insurance clients by overcharging them for insurance and keeping the excess as a balance in the client accounts to use when he needed to fix other loss-making deals he had entered into. Each count involved one or two thousand pounds.

Lessons learned:

- This case demonstrates that white collar crime is often committed by those in trusted positions, whose judgement and integrity is rarely called in to question. It also often involves those who have an intimate understanding of and, very importantly, access to, an organisation's internal control system built up over many years' service.
- Notwithstanding any individual's remit to engage in business activities, there always needs to be some form of oversight which can hold a director or any other employee of a business to account. This applies to negotiating deals and their documentation through to accounting for the transactions. In short, not only does there need to be governance over these process but on a more detailed level, a segregation of duties between 'front office' and 'back office'. Whilst these concepts are familiar to those in investment banking and trading activities, whereby those involved in striking deals do not have responsibility and authority to account and manage the transactions, this should also apply to other financial institutions.
- This case also demonstrates the risks of 'hoarding of knowledge' both in terms of technical understanding and also of the nature of specific client relationships and deals. The combination of the concentration of authority and knowledge in the hands of one individual makes any control structure difficult to monitor as those doing the monitoring have little realistic prospect of understanding an individual's actions. This is particularly relevant in complex insurance products or other financial instruments.
- Motivations behind white collar crime, whilst to a large extent can be found in financial incentives such as bonus and dividend payments, can also be attributed to human factors which can be exacerbated by the culture of an organisation. In this case Mr X claimed that a combination of client pressures to achieve a good deal and a desire to avoid verbal recrimination and loss of personal prestige from his employer, were contributing factors. Cultural factors such as a barrier between owners and employees and also a culture of high performance can also lead to excessive risk taking and, in extreme cases, dishonest behaviour.
- Improper use of client monies. Client accounts were not adequately accounted for and segregated, with funds being inappropriately applied to the benefit of other clients in order keep them happy and also to make up losses on other transactions.
- As with many cases of a similar nature, the facts are only discovered when the money has run out and other individuals, who need access to the cash, start asking more probing

questions which should have been asked at an earlier stage. Equally, it does raise the question as to how many cases of a similar nature go undetected but where significant gains, made either through skill or luck, go undetected, thereby enabling money launderers and fraudsters to successfully hide their crimes. Organisations need to be alert to both possibilities and not turn a blind eye to the latter in the belief that it is better swept under the carpet. This will give money launderers and fraudsters the impression that Jersey is a light touch jurisdiction and does not take the prosecution of crime seriously.

3.5 Case study 5

Mr X was employed at a stockbroker based in Jersey, who was tasked with administering other people's money on a discretionary basis. This case revolves around funds of some US$1.25m entrusted to Mr X by a Mr Y. Mr Y was not financially sophisticated and relied on advice from others. The investment vehicle was originally set up whilst Mr X lived and worked in the BVI, but on Mr X's return to Jersey, took Mr Y's business with him to his new employer, ABC Fiduciaries Limited.

The money was supposed to be placed in safe, conservative investments and Mr Y was supposed to approve anything that was done with them.

Mr X ignored these instructions and abused the trust placed in him. Mr X opened accounts at a financial institution to receive the assets based on false information and, critically, that the mandate was to be operated on a sole signatory basis. Mr X's employers knew nothing of this and it went against company policy. He became involved with a number of disreputable stockbrokers, using Mr Y's money to buy and sell highly speculative shares. Having invested in safe, interest bearing Eurobonds before his move to Jersey, these were all sold and invested in technology shares on the US NASDAQ market. Mr Y knew nothing of this. Mr X's employer knew nothing of the fact that Mr X had opened an account with the US broker's clearing agent in its name to hold the shares.

Mr X left the employ of ABC Fiduciaries Limited shortly thereafter but, by that time, had already used his employer's official stationery to write several faxes and letters without anyone else reviewing or approving their contents. Meanwhile, the share price of the stock continued to fall and Mr X gained employment with DEF Fiduciaries Limited on much the same basis. Importantly, Mr Y never became a client of DEF Fiduciaries Limited and Mr X dealt with Mr Y's funds principally from his home address. Mr X instructed the institutions dealing with Mr Y's funds to send any correspondence to his home address. Mr X provided, when pressured, false valuation information to Mr Y which was, in any event, drastically out of line with his investment profile. Further, Mr X stole the remnants of Mr Y's portfolio.

Within a few months, other transactions of a similar nature occurred but most of the money was lost and the investment of US$1.25m resulted in US$18,000 being returned to Mr Y.

Lessons learned:

- This case demonstrates that the business of investment management still relies heavily on the bond of trust that exists between client and investment manager. This exists in addition to any documents which are prepared in order to establish any investment relationship governing the terms on which the investment manager will deal. As a consequence, the closeness of relationships with clients can easily be abused, especially with clients who are not financially sophisticated. This highlights a need for organisations involved in investment management to:

    - Carry out their own Client Due Diligence procedures which identify the parameters and risk tolerances of clients, in addition to those required from an AML/CFT perspective. It is noted that the advent of MiFID and the development of the investment management industry since this case should have caused investment managers to adopt such procedures.
    - Ensure that instructions from clients are recorded and documented by not only the contact point at the investment manager but also those charged with monitoring performance as against those instructions.

- From a banking perspective, there are similarities with Case Study 3 concerning the provision of false information. Again, this goes to the core of banks' procedures in opening and maintaining bank accounts and the questions which should be asked. In ordinary terms, it is highly unusual for one person to have total control over a client's bank accounts for the precise reason that it reduces the risk of fraud by rogue employees.
- The use of Mr X's employer's stationery without any review, which was in breach of company policy, increases financial institutions' vulnerabilities to fraud. Institutions should ensure that their policy on such matters is clearly communicated to staff and official stationery monitored so as to reduce potential abuse.
- Vetting of employees. This case illustrates the need to seek and obtain references from previous employers in the regulated financial sector. Whilst current practice on providing references, in order to reduce exposure to claims from departing employees, has reduced the qualitative content of references, it is vital that employers contact former employers in order to discuss any concerns they may have. Had they done so in this case, the outcome could well have been different, and Mr Y's loss reduced.

- Banking institutions and stockbrokers when presented with change of address forms from existing clients of known service providers should exercise vigilance over new address details. For example, a move from a regulated service provider to a private address should raise suspicion.

3.6 Case study 6

Mr X was sentenced to 6 years' imprisonment for 10 offences of money laundering. His employee, Mrs Y, who carried out the transactions that he devised on his instructions or those of his clients, was sentenced to community service for one such offence. Mr X was sentenced to 6 years' imprisonment and a confiscation order for £9.7m and £1.4m by way of costs was ordered.

Mr X was a chartered accountant and the sole principal of a financial services business trading as Mr X & Co. He acquired companies, provided directors, formed trusts and acted as trustee. He was signatory to hundreds of bank accounts. Mr X used these facilities as a tool kit to help foreign clients to cheat their fiscal authorities and launder the proceeds of crime. The common theme was that he was willing deal with the assets of clients according to their instruction.

Mr X laundered money in a variety of ways. He extracted money from foreign trading companies using false invoices drafted at the behest of clients, holding the sums received anonymously for his clients. He layered millions of pounds through his pooled accounts. He obtained and delivered cash from and to his clients. He lied about the beneficial ownership and purpose of his companies and the origin of property to the Jersey authorities and others. In the main Mr X's offences targeted the tax man, but he was also convicted of laundering the proceeds of wholesale duty evasion upon alcohol, and theft by a trustee and company director.

A key aspect of his business was his trade in bank notes. He obtained cash from clients who wanted to get rid of it, crediting bank accounts held for them with equivalent sums sourced from different money in return. The actual cash was then delivered to other clients who wanted their income secretly returned to them in this fashion – bank notes which he personally delivered to them in the UK. These dealings were hidden by the operation of a spider's web of bank accounts.

The result of these activities was that it was impossible to ascertain the origin and ownership of property without access to the records of Mr X & Co. Even then the tracing exercise was extremely difficult, requiring years of analysis by investigative lawyers, police, and forensic accountants to unravel.

Lessons learned:

- The offences described above took place in the days before trust companies were regulated under the Financial Services (Jersey) Law 1998 and the requirement to register in February 2001. It is reasonably to be supposed that the regulation since introduced would have precluded - or hugely reduce the opportunity for – the continued operation of a fiduciary services provider such as Mr X & Co. Any regulatory inspection by the Jersey Financial Services Commission would have clearly resulted in the closing down of such an operation.
- Mr X was in the business of deception to the point of forgery and beyond. It can simply be said that an honest observer would have been immediately alerted by labyrinthine transactions which made no commercial sense, including invoicing processes e.g. for services which could not possibly have been provided, and inexplicably complex money routes. The informal sourcing of cash from friends, and formally from banks repeatedly just below the supposed reporting threshold combined with huge volumes of 'briefcase' collection and delivery of cash would have caused an honest observer huge concern.
- A clear breach of the current span of control requirements which operate over fiduciary service providers permitted the total and unfettered control by Mr X over his client affairs with none of the safeguards that a span of control affords.
- For banking institutions involved in providing banking facilities, there is a clear cause for concern in the use of pooled accounts which can be exploited by money launderers who are in charge of fiduciary operations. The use of pooled accounts continues to be a cause for concern by the Jersey Financial Services Commission as they can be used to disguise the ownership of funds from the bank's own internal compliance function, whilst simultaneously accessing all the benefits thereof.

3.7 Case study 7

Mr X was accused of fraudulently converting the sum of £1,070,625 over a seven year period from a trust and corporate structure that he administered at the behest of a client, Mr Y.

Mr X had worked as a trust and company professional in Jersey's financial sector for many years and had become a director of many of these as he progressed in his career. Mr X began to administer the affairs of Mr Y over 20 years ago and formed a firm friendship, even to the extent of becoming a beneficiary under the terms of his will. Mr X became the trustee of a trust which had an underlying company, of which he was also a director. In 1995, Mr X requested Mr Z, the principal of the financial services business referred to in Case Study 6, to acquire a company, ABC Limited, for him to facilitate the secret transfer of assets between different entities of the trust and corporate structure for the benefit of Mr Y, in order to evade tax.. This entity was not disclosed to Mr X's employer.

Mr X subsequently decided use ABC Limited in order to steal from Mr Y, opening a bank account in its name and causing funds to be sent to it from Mr Y's trust and corporate structure. There were three principal methods used to effect the wrongful transfer of funds:

1. Transfer of funds to ABC Limited's bank account through the staging post of Mr Z's financial services business in order to disguise the true source of funds;
2. Direct transfer from the trust and corporate structure into ABC Limited's bank account; and
3. A stand alone diversion of part of the sale proceeds of a UK property belonging to Mr Y's trust and corporate structure in to ABC Limited's bank account.

In relation to transfers from ABC Limited to Mr X's personal account, Mr X told his bankers that this money represented drawings and bonuses from his employment. These funds were used to pay for his personal credit cards, a new kitchen, travel expenses, building works, share purchases, dining out etc.

Lessons learned:

- As with Case Study 5, involving investment management relationships, this case also has, as an attribute, a bond of trust that exists between client and relationship manager. However, in the case of a fiduciary relationship, the risk profile is different in that acting as either trustee of a trust or director of a company, there is a fiduciary duty which exists towards the administered entity. This contrasts with a direct investment management or banking relationship which is contractual and where the client's instructions must be acted on. Notwithstanding the nature of the relationship, a close bond of trust can increase the opportunity for a dishonest employee to exploit a trust and company structure.
- It is a striking feature of this case that one fraudster (Mr X) used the services of another fraudster (the principal of the financial services business referred to in Case Study 6) in order to facilitate his crime. This evidences the fact that in Jersey's close knit financial community it is often the case that there will be linkages with other cases and that criminals will often exploit the weakest point in the financial services industry in order to gain access to the rest of the services it can offer.
- None of the three methods by which the funds were diverted in to ABC Limited's bank account were highly sophisticated. They relied on the unquestioning acceptance of funds by Mr Z's financial services business, the bankers to ABC Limited accepting his explanations as to the source of funds, the solicitors involved in the sale of the UK property accepting his explanation as to why part of the funds needed to be sent to ABC Limited and, in general terms, his leveraging of his position at his employer where he acted as trustee and director. Both of these positions carried a high level of trust and implicit authority.
- At the heart of the matter is the corporate governance and control structure which surrounded Mr X's activities at his employer. Whilst no finding was made as to liability at trial, it is clearly critical that employers should be aware of, and monitor, the activities not only of staff, but also of directors. A common structure in many fiduciary service providers is that each director has his own client portfolio, for which he is responsible, along with a team of administrators. Whilst it is understandable, from a client service viewpoint, to have such a structure, *effective* governance over directors' and trustees' activities needs to take place in order to avoid rogue employees exploiting the system.

3.8 Case study 8

Mr X was accused of committing various fraudulent acts over a two and a half year period whilst employed at a local bank in Jersey by creating invoices to allow money to be paid to his personal accounts and also by forging invoices to hide expenses that were greater than would have been authorised by the bank.

Mr X worked as a company secretary dealing with the day to day management and administration of investment trusts, including all secretarial, legal, accounting and administrative aspects of those businesses. He earned in the region of £40,000 per year with a company car and performance related bonus. He also acted as company secretary for the bank both in Jersey and New York and in that capacity would arrange meetings and provide advice as to what was necessary for the effective operation of the companies. Mr X was highly trusted by the bank. Although he was a signatory on various accounts, he had fairly low levels of authority with respect to transaction levels and so further clearance was required from other bank employees.

Mr X employed three different *modus operandi* in order to fraudulently obtain money from the bank:

1. Fraudulent invoicing – Mr X used his own laptop computer to create false invoices requesting payments into his own account. These would be accompanied by a memorandum authorising payment and the required signatures would be procured by Mr X and then presented to either internal or external bankers or the relevant fund administrator. Funds obtained using this method totalled in excess of £290,000;
2. Fictitious shareholder payouts – Mr X used fictitious shareholders as the device by which he secured money from funds which were in the process of liquidation. Funds obtained using this method totalled in excess of £50,000; and
3. Forgery regarding hotel expenses – Mr X was authorised, whilst travelling on business, to stay in hotel rooms charged at a rate of approximately £150 per night. Mr X often stayed in more luxurious rooms. When reclaiming his expenses he would forge an invoice on his laptop computer and add additional nights of accommodation or pretend that a conference room had been hired for business meetings and so disguising the actual room rate although the total amount was identical. The benefit obtained using this method totalled in excess of £3,000.

Mr X's explanation for his apparent change from an honest worker to that of a criminal lay in relationship issues and also the accumulation of debt.

Lessons learned:

- This case again demonstrates that white collar crime is often committed by those in trusted positions, whose judgement and integrity is rarely called in to question. It also often involves those who have an intimate understanding of and, very importantly, access to, an organisation's internal control system built up over many years' service.
- In relation to the fraudulent invoicing, Mr X leveraged his position of trust within the bank and convinced his colleagues to supply the required signature. It is therefore key, from this case, that signatories to payments should ensure that they have sufficient third party documentary evidence to support any payment and not rely wholly on explanations, whether written or oral, from other signatories.
- Concerning the fictitious shareholder payouts and forgery of hotel expenses, these are clearly more sophisticated forms of deception which were necessitated by Mr X's role at the bank. The extent to which internal controls would have prevented fraud of this nature is a function of each institution's business and internal control structure and should be assessed accordingly.
- Turning to the issue of motivation, the case aptly demonstrates the ability of once honest individuals to turn to crime as a means, not only for self enrichment, but also as a perceived mechanism by which they can access fund in order to address perceived personal issues in, for example, relationships. As this case demonstrates, once one act of criminality has been 'successfully' undertaken it is a short step to repeating the offence for greater personal benefit.

3.9 Case study 9

During the mid 1990s, Mr and Mrs X operated a Delaware based company, ABC International LLC, based in Alderney. Mrs X was also the main director of a Jersey based trust company DEF Trust Company Limited. Whilst resident in Alderney, Mr and Mrs X became friendly with an elderly couple ("the Ys") whose assets totalled in excess of £3m and a bond of trust developed between the two couples.

Through ABC International LLC in Alderney and DEF Trust Company in Jersey, the Ys' finances were restructured through a series of holding companies which owned financial assets and real property. Two trust structures were used to own the shares in the holding companies and Mr Y wrote a letter of wishes in respect of each trust. The letter of wishes stated that in the event of the demise of both Mr and Mrs Y, that a company controlled by Mrs X should receive the remainder of the trust following certain gifts and the use of the trust fund for the benefit of both Mr and Mrs Y. The co-directors, at the time, of DEF Trust Company Limited were concerned as to this potential conflict of interest and a different trust company acted as trustee whilst Mrs X continued to act as director to the underlying holding companies.

Due to the resettlement of the Ys in Jersey and a resultant conflict with a clause in the trust deed, it was proposed that the trust funds be distributed and a new trust formed. Mr Y died in the meantime. Mrs X was dissatisfied with these arrangements and dispensed with Mrs Y's legal adviser (through a letter typed by Mrs X, but signed by Mrs Y) and also with the incumbent trustees. Mrs X arranged for the assets of the two trusts to be settled in to a Liechtenstein trust without Mrs Y's knowledge.

The new trust documentation identified Mrs X as the settlor and protector of the trust (with extensive powers in terms of appointments), aswell as a beneficiary. Mrs Y was also identified as a beneficiary. The letter of wishes differed from the original letter of wishes in that Mrs X was entitled to benefit from the trust assets during Mrs Y's lifetime. Mr and Mrs X retained control of all the underlying holding companies and proceeded to use the assets for their own benefit. Both Mr and Mrs X were subsequently convicted on several counts of fraudulent conversion and a confiscation order in a sum in excess of £2m was ordered.

Lessons learned:

- Mr and Mrs X were not part of a properly regulated trust company and indeed, the events described above occurred before the advent of the requirement to register as a trust company business. Notwithstanding this, this case identifies the risks associated when dealing with vulnerable clients who are not financially sophisticated and place their trust in others.
- The case also exposes some of the potential vulnerabilities of trust and company structures as follows:

    - Assets have been legally transferred to another entity; and
    - The management of the assets are only governed by letters of wishes and the reliance on the service provider to discharge their fiduciary duties honestly.

  In the instance where the fiduciary services provider is dishonest and the client is unable to challenge the trustee and verify his or her actions, the vulnerability to fraud increase.
- The use of Liechtenstein as a provider of fiduciary services was clearly designed to place control of the assets outside the jurisdiction of the courts and to make communications and enforcement of any action more problematic. Although there may be clear fiscal advantages to placing business in offshore locations, financial institutions need to question why the architecture chosen is as it is. Examples of valid issues to be raised could comprise : Why are so many jurisdictions needed in a particular structure? Are different voting rights necessary with different share classes? What is the purpose behind any bearer shares in issue? What percentage of the overall structure do we control?

  Challenges to a client on these lines should be made in order to identify any potential vulnerability to money laundering.

4. International/generic case analysis

On an annual basis, the Financial Action Task Force ("FATF") brings together operational experts from the law enforcement and regulatory authorities of FATF member countries to exchange information on significant money laundering cases and operations. These meetings enable these experts to identify and describe current money laundering trends and effective counter-measures and building on earlier analysis, examine particular concerns in the money laundering area. In relation to typologies which are relevant to Jersey, the following categories have been identified:

- Alternative remittance systems
- Money laundering vulnerabilities in the insurance sector
- Terrorist financing
- Non-profit organisations and links to terrorist financing
- Politically exposed persons
- Non financial professions in money laundering (solicitors, notaries and accountants)
- Money laundering through the securities sector
- Correspondent banking
- Corruption and private banking
- Bearer securities and other negotiable instruments

Alternative remittance systems ("ARS")

ARS is defined as any system used for transferring money from one location to another and generally operating outside the banking channels. ARS services range from those managed by large multinational companies to small local networks and can be of a legal or illegal nature and make use of a variety of methods and tools to transfer the money.

The use of ARS for criminal purposes starts with a simple transaction designed to dispose of criminal cash or obscure the audit trail for criminal money held in a bank account. The investigation of these operations from the entry of the funds into the ARS "retail outlet" to the ultimate beneficiary can, however, be characterised by a high degree of complexity. This level of complexity is mostly due to intricate settlement systems used and number of jurisdictions through which a transfer could pass. Each jurisdiction might hold a part of the evidence or intelligence impacting on the transaction. Therefore, obtaining an overall view of particular operations from beginning to end is made more difficult.

The Mechanisms of Alternative Remittance Systems

The systems used for alternative remittance can be considered as both simple and complex. They are simple in that the individual components of the system involve operations as basic as receiving cash for a transfer or communicating information on individual payment orders. ARS can appear to be complex, as they may rely on a series of seemingly unrelated operations at the clearing or settlement phase of the process. ARS operations may in fact appear to be more complicated in certain situations due to the lack of transparency inherent in certain types of systems. In any case, most ARS activity is carried out in ways that are very similar to those used by conventional banks to move funds. To examine the way the ARS work, it makes sense to view such systems by looking at each of the various components or players in this activity. This breakdown will make it easier to follow each phase in the alternative remittance process.

The Originator of the Transfer

For the sending customer (the originator of the money/value transfer), a transaction begins by the payment or handing over of funds to the ARS operator. At this point, the originator also specifies the recipient or beneficiary for the transaction along with his or her location. The funds can be paid in cash, cash equivalent, cheques, and other monetary instruments or in stored value cards. In certain situations, the originator may pay funds directly into a bank account belonging to or controlled by the ARS operator. Cash remains the most prevalent form of funds at this stage. In large ARS networks the customers generally have access to the ARS

services through local (sub)agents. The originator usually receives a unique reference to identify the transaction. This is then passed to the beneficiary. The originator's only other role in the transaction will be to follow up with the originating ARS provider if the beneficiary reports a failure of the transaction.

The Originator's ARS Service Provider

The ARS provider at the originator's location receives the funds and then sends an instruction for payment to a counterpart at the location of the beneficiary of the transfer. This communication may occur directly or through an intermediary as well as through different communication channels (for example, fax, telephone, Internet). ARS providers normally have a record of their partner ARS providers in the beneficiary's location who make payments on their behalf. With more organised multinational operators this list of partner ARS providers is usually available to the public; in some circumstances, it may be provided on request.

The operator may assign a code to the transaction. In an internationally franchised operation this will usually be an easily recognisable multi-digit unique number. In a hawala transaction it may be a banknote serial number. This unique number will be communicated to his customer (originator), and the disbursing agent. The originating customer will usually communicate this unique number to his intended beneficiary who will then be able to be identified by the disbursing agent.

The ARS Service Provider at the Transfer Destination

The ARS operator at the destination for the remittance makes the corresponding payment on instructions from the originating ARS operator, to the beneficiary specified by the originator who meets the identification procedure. This may be a formal and recorded identification procedure or simply the person who knows the unique reference number. The ARS operator may have to satisfy two standards of compliance, depending on differences in compliance regimes in the sending and receiving country.

The Transfer Beneficiary

The money, once received at its destination, may be delivered directly to the beneficiary, or else the beneficiary will be notified to go to the premises of the destination ARS operator to receive payment. Payments may be received in local currency, hard (international) currency or in the form of a cheque or bank draft. An identification code may be used to validate the payment. In a jurisdiction with money laundering controls, the ARS operator could apply CDD-

procedures to the beneficiary. The beneficiary will inform the originator of any failure of the ARS transaction.

Settlement

ARS transfers may occur in both directions, that is, the service providers may process both outgoing and incoming transfers at their particular location. Ideally, the transfer amounts should balance out so that the neither side has a surplus or deficit. In reality however, ARS operations seldom balance out between the service providers in two different jurisdictions. The originating ARS operator will accumulate a sum of money, whilst the destination ARS operator will have a deficit. This deficit has to be balanced out or settled in the longer term. In general, settlement of the amounts owed within a network of operators will not occur on a transaction-by-transaction basis. Often, settlement is effected on a weekly, bi-weekly or monthly basis. Given this length of time, the pricing of the final set-off transaction will often depend on a fluctuating exchange rate which takes account of the movements in currency over the period in question. Methods of settlement may vary according to the type of ARS service or its links to other commercial activities. Whatever method is used, the ARS service provider also seeks to preserve or enhance profits. Some of the more common ARS settlement procedures are indicated below.

Transfers through Conventional Banking Systems

The ARS service provider holding funds use wire transfers, the Internet or other methods of payment to make payment to the account specified by the deficit ARS provider (who has paid out remittances at the destination). This may be a simple operation but involves bank fees and exchange rate costs that have to be allowed for in the costing of the transaction. These payments may be made to an ARS provider who acts as a clearing agent for the transaction.

Offset of Remittances

Settlement by back to back transfers is a preferred method as it is the easiest and the most efficient. In this system each ARS provider is the originating ARS for one transaction and uses the funds to act as the destination ARS for another. No funds need to be moved and two commissions are shared between the two ARS providers. This is the principal on which multi-national franchised ARS operations work, but it is equally the ideal solution for informal systems. This category also includes manufactured offset of remittances. For example, an ARS operator in a country with a high level of migrant remittances may pool the proceeds of multiple

transactions in order to use this money to make a single commercial remittance to a third party. This activity is common between Europe and South Asia, but it is a high risk as a method of settlement as it may facilitate export and import fraud. The settlement flows will usually be different from individual customers' remittances flows. The ARS provider may pool the cash from the individual remittance transactions, and a large single transfer may then be made at a later date in order to settle all the previous remittance transactions. This both limits costs and allows the exploitation of cash balances and means that settlements cannot necessarily be traced back to the specific transactions. Unscrupulous ARS providers can use this method to cloak transactions relating to money laundering or terrorist financing.

Physical Cash Movement

Cash deposits can be a logistical problem for unlicensed or illegal ARS. Cash couriering and smuggling is a common method of moving value to jurisdictions which have less experienced banks and cash wholesalers operating. It also allows profits to be taken on currencies in high demand by ARS providers.

Cash pooling accounts

Cash pooling accounts are a common feature of complex ARS systems. They are used by multinational ARS providers to reduce the losses of currency exchange. Equally, they are used by informal ARS providers to facilitate complex settlements between different countries. The holder of the cash pooling account will have a series of accounts in different currencies; however, the US dollar has always been the predominant currency. Money is transferred into the cash pooling account from customer transactions and used by the originating ARS provider. The value remains to the credit of the destination ARS provider. The originating ARS provider can use the money to settle past, current or future transactions anywhere in the world. These settlement transactions may be effected by making personal or commercial remittances. This allows a great deal of flexibility in pricing and completing transactions in a variety of currencies.

TYPOLOGIES

Categories of Alternative Remittance Systems

The cases available show that some uniform categories of ARS are identifiable based on the structure of the business. The relevant categories are the following:

- Franchised multinational companies
- Multi premises or franchised national companies
- Signed shop-front premises (one or more premises)
- Overt ARS within another business
- Covert ARS within another business
- Covert ARS – no premises

Franchised Multinational Companies

This category includes ARS products offered by various large and often well-known international corporations that provide money transfer service through franchises. These operators tend to have a high degree of compliance with local legislation, also by providing effective procedures to prevent misuse. This is reflected in the relative expense of the service. The providers are household names, and their services are accessible around the world.

With franchised multinational companies, there is a fixed fee structure, and exchange rates used are often less competitive. These operators provide an accessible, quick and reliable service. They are undercut by a whole range of ARS operators but are still used by ordinary customers in preference to other ARS operators. This is an indication that some ARS customers value a reliable and legitimate service above other factors in selecting an ARS provider. They have sophisticated computer systems to ensure transactions are completed accurately and to prevent fraud against their services. All transactions can be traced, and they tend to have clear policies on identifying customers and reporting suspect transactions. Multinational companies are increasingly providing online and remote payment services. This increases the volume of transactions to be examined for detecting suspicious activity and may lead to problems in defining risk. Online services require use of bank accounts that provide a better audit trail. Terrorist financing through this form of ARS will be difficult to identify. Embedded terrorist

groups will be able to provide identification, and the amount transferred by each individual element of a terrorist operation will not lead to suspicion. The computerised tracking systems do however mean that historic transactions can be scrutinised effectively.

Multi-Premises or Franchised National Companies

These ARS are the next level in scale after the multinational companies. Within a particular country or community, these businesses are a recognised brand. They tend to support efforts to licence or regulate ARS services often have established and effective methods for identifying their customers and reporting suspicious transactions. ARS operators from this category servicing migrant workers in the UAE, for example, have developed "membership" schemes to streamline and reward frequent customers. This allows the ARS operator to conduct a high level of know-your-customer (KYC) procedures when enrolling a customer, who is given a unique number and photo identification card. Beneficiary names and, where possible, account details are also embedded in the card data file. Monitoring this "account" then allows the identification of suspect transactions against a profile of normal activity. These operators will often act as franchisees of the multinational companies but will also provide their own rival services. They tend to provide remittances to or through banking channels, making use of electronic transfers or bank drafts. Franchised national companies compete with banks and multinational companies by knowing their market and using economies of scale to provide better exchange rates or cheaper charges. This tier of ARS tends to be vigilant. Where they serve a particular ethnic group or community they are well placed to identify normal levels of transfer and so identify what is abnormal. The risks they face are similar to multinational franchised operations. In addition, they are vulnerable to organised smurfing which exploits the availability of rival companies servicing similar communities.

Where they offer commercial services they can be abused in large scale frauds, either as the remitting or receiving company. This means they have to be particular careful to identify the source, destination and business reason for transactions. Cash is a risk as with all ARS but bank to bank transfers via ARS in this tier are a particular risk.

Signed Shop-Front Premises (one or more premises)

These are familiar premises wherever ARS can operate legally. They generally serve a particular ethnic community and provide it with a cost effective and valuable service. They tend to be family run and are sometimes identified as "Mom & Pop" operations within United States. They can provide a cost effective service by using efficient settlement methods and making

economies of scale on bank transfer costs. They may use the services of another ARS to make transfers if this is most efficient. Customers either make cash deposits at the shop-front premises or make payments directly into the ARS provider's bank account. Direct cash deposits into their bank account help the shop-front ARS provider to streamline cash control, but there is a risk that they do not truly know their customer. The ARS operator will have a series of linked payment agents in the countries they serve. These payment agents may range from similar operations to individual hawaladar. The ARS will use an exchange rate agreed with their partner agents in the destination countries. These rates will constantly fluctuate.

Settlement will be by a form agreed with the destination agent. This tier will be particularly likely to use cash pooling accounts, back to back transfers and third party payments. A family business of this nature is particularly vulnerable to money laundering, either through having inadequate internal controls or through becoming complicit with criminal groups.

Overt ARS Operations within another business

These operators are visible, but do not necessarily advertise their services. This tier of ARS operator can be similar to a shop front ARS operator, with the same risks. In the same way as a franchise agent of a multinational ARS operator, they offer remittance services to local customers in addition to their normal business. The provision of remittance services may complement their normal business activity or be a totally separate venture. Where there is a registration or licensing regime, these ARS operators can be effectively controlled as long as their services are identified. Risks include those generated by possible commingling of funds coming from different activities. That could cause difficulties in the proper application of AML/CFT measures, also breaking the audit trail.

Covert ARS Operations within another business

Covert ARS operation within another business is the first category where the operator will actively seek to work outside the regulatory regime. A covert ARS operation will be illegal in that it operates without a licence or registration. It also violates regulatory provisions by performing ARS operations without carrying out necessary AML/CFT measures, such as identifying customers, recording transactions or reporting suspicious transactions. It is also likely to commit banking offences such as "structuring" where deposits are made below a disclosure limit to avoid identification of the ARS activity. ARS operators in this category tend to serve a particular migrant or ethnic community. They rely on referrals within the community they serve. This category will include most hawaladars, unless they are registered or licensed. This

category of ARS operator is particularly strong in communities where mainstream banking is not freely available in the destination country. This has been demonstrated in Somalia where overt and covert ARS operators dominate home remittances worldwide since there is little if any developed formal banking system.

This category will be most likely to use forms of settlement that do not rely on bank transfers, but because their transactions will tend to flow to one country they may still rely on depositing cash into a bank account in the other country in order to effect an offsetting settlement. Suspicious transaction reports from banks or referrals from another FIU are the most successful methods of identifying these ARS operators. Information gleaned from the community these operators serve is also valuable. In some cases, this category of ARS operator will be resistant to AML procedures. Their informality is key to their selection by individuals who may be operating illegally or within the "grey" or "cash" economy.

To law enforcement this tier is high risk for ML and TF. Even many "bona fide" ARS operators in this sector hide the volume and detail of their transactions. This secrecy or lack of transparency is a product of their history and business methods; however, it is this aspect of their operations that arouses suspicion among law enforcement personnel, since a lack of transparency is often a key factor exploited by criminal misuse of certain financial channels. The success of criminal money launderers is directly related to their ability to handle large amounts of cash covertly. Law enforcement experience has shown that successful covert ARS operators involved in criminal ML quickly attract levels of cash that make detection easier. Having an entire business that is cloaked in secrecy where illicit and genuine transactions take place, allows the criminal money launderer to hide more of the illegal business. In some cases, criminal money launderers may also progress to overt operations to ensure they can obtain banking facilities to service criminal customers.

In terrorist financing significant transactions may be small. There is no way of measuring the importance of covert ARS operators in terrorist financing without better intelligence on their activities. However, logic suggests that a covert ARS operator embedded in a community which also contains covert terrorist cells will be the natural first port of call for transactions. Terrorist cells have used franchised multi-national ARS operators, but this was in a situation where they were operating in a country where they were not supported by an embedded ethnic community.

Case Example 1

An investigation was conducted based upon the filing of four suspicious transaction reports on A Inc. of USA, a licensed ARS service provider operating in New Jersey. Although A Inc. of USA was a licensed service provider, the owners and operators of the service conspired with four unlicensed money remitters (couriers) operating out of New York to commit the criminal acts. The four couriers brought large sums of cash to A Inc. that were deposited into the business' bank accounts and then wired to the Middle East. A Inc operated with a very limited number of clients, but was responsible for over USD 100,000,000 in cash deposits over a 30 month period – all of which was ultimately transferred to Pakistan. A . Inc failed to complete the appropriate currency transaction reports and created fraudulent foreign exchange records. An unidentified employee attempted to deposit over USD 10,000 in cash and refused to provide identification when requested by a bank official. The bank then contacted the ARS owner and advised him of US Bank Secrecy Act regulations and bank policy.

Source: United States

Covert ARS Operation – No Premises

A covert ARS operator having no specific premises may operate in the same way as the previous category. They also include criminal money laundering groups who act as purely criminal ARS operators. These ARS groups will use the services of overt and covert ARS operators to move money within their systems, but they also act as their own network.

The roles of key players within these criminal money laundering networks can be broken down into three distinct functions: control, collection and cash disposal.

- ***Control.*** The controller organises the ML activity and thus has a complete overview of the operation. He buys cash from criminal groups and arranges payment at the destination chosen by the criminal. The controller may be associated with an ARS operator and is normally based in a third country, often in South Asia or the Middle East. The controller employs collectors to gather cash and disburse the money on his behalf. Finally, he uses various ARS techniques to move money or value from the originating country to cash pooling accounts, third party accounts or to settlement accounts via back-to-back transfers.

- ***Collection.*** The persons carrying out the collection function serve as the interface between the ARS operators and the criminal customers. The collector receives instructions by mobile phone or SMS from the controller with details of criminal customers who are holding cash. He may use pre-paid mobile phones to contact the criminal and collect the cash in a covert meeting. The collector counts the money and reports any shortages or counterfeit notes and stores the cash in a safe house and then disposes of the money on instructions from the controller.

- ***Cash disposal.*** For this function, funds may be sent to destination parties or third parties by money transmission through complicit ARS operators. Cash may be moved by

organised cash couriers to jurisdictions where the banknotes can be safely sold. The funds may also be used to complete back to back transfers through *cuckoo smurfing*. Finally, the money is handed over to individuals or criminals who want to receive cash. This may complete a separate criminal ARS transaction, including "grey economy" transactions.

ASSESSMENT OF RISK AREAS

Terrorist Financing

The level of vulnerability for ARS to misuse for terrorist financing differs from that associated with money laundering. In the terrorist financing area, the level of vulnerability may also differ according to whether ARS operations are used in providing funds for a specific terrorist action or if such operations are used in transmitting funds that have been collected from legitimate (or illegal) sources to support future terrorist activities. Terrorist financing is difficult to detect and can involve clean sources of funds. It is important that ARS providers screen transactions and customers against relevant terrorist financing related lists.

The expenses of an individual terrorist or terrorist cell may well be small. Often cells are largely selfsupporting and may derive funding from crime. The best defence against these transactions is the application of normal AML policies, that is, customer identification, know-your-customer procedures and suspicious transaction reporting. With fund raising activities, know your customer procedures are equally important. Any sector may be used for these activities, but as AML procedures are implemented worldwide, covert ARS will become increasingly attractive to terrorist organisations.

Money Laundering

The risks in money laundering are clearer. Any ARS can be misused to launder the proceeds of crime. The use of false identities and structuring are common techniques to which ARS is vulnerable. The highest risks, however, are to the ARS that can efficiently handle large volumes of cash. While specific risks will vary from one jurisdiction to another, several common elements can be identified. Some of the factors to be considered in assessing risks are:

- The effectiveness or existence of the regulatory regime;
- The volume and destinations of criminal money flows (criminal remittance corridors);
- The number and types of ARS operators;

- The extent of law enforcement interdiction and effectiveness of the suspicious transaction reporting regime;

- The extent to which banks provide accounts for ARS operations; and

- The size, origins and locations of migrant communities.

The risk analysis for each country will be different and should inform the regulatory and banking sectors.

Money laundering vulnerabilities in the insurance sector

The global insurance industry provides risk transfer, savings and investment products to a variety of consumers worldwide, from individuals to multi-national corporations and governments. The insurance sector, like other financial services, is exposed to the threat of money laundering. The insurance sector could be attractive to money launderers seeking to place funds into a financial product that will provide them with a reliable, clean return of funds invested. If a money launderer is able to move funds into an insurance product and receive a payment made by an insurance company then he will have made his funds appear legitimate.

TYPOLOGIES

Nine typologies have been identified as follows.

Typology 1: The use of life insurance single premium policies

This typology, which has already been identified in previous typologies reports, is still an often found typology in many jurisdictions. The availability of bespoke policies of this nature enables the laundering of large sums by making substantial payments into life insurance single premium policies, which serve as a wrapped investment policy. The customer actually does not seek insurance coverage but an investment opportunity. A variation on this is the use of large premium deposits used to fund annual premiums. Such policies, which are comparable to single premium policies, again enable the customer to invest substantial amounts of money with an insurance company. Since the annual premiums are to be paid from an account which has to be funded with the total amount an apparently lower money laundering risk life product will bear the features of the higher risk single premium policy.

Case Example 1

A fraudulently bankrupt subject used an account in the name of a family member to pay cash in and withdraw it out via a cheque to a lawyer. The lawyer then gave some money back in a cheque to the family member while the rest went to the subject's single premium life policy which was immediately surrendered. The surrender value was paid out to the family member's account.

Source: Belgium

Typology 2: Early policy redemption, especially when uneconomic or unusually early

This typology, which could be found in cases of several jurisdictions, is a means to receive clean funds at an early stage. It is very often combined with high single premium or deposit account life insurance policies. A conspicuous fact is that some of the respective customers opted for early redemption despite uneconomic consequences. In the case illustrated below the money launderer surrendered his policy despite a loss of 40 percent of the original investment. In some cases the money launderers redeem their policies very soon after purchasing them.

Case Example 2

The subject deposited 1m euros in cash with a life insurance company in 2 single premium life policies which were surrendered early incurring a loss of 40% of the investment cashed outside the jurisdiction concerned in an effort to evade creditors seeking remuneration from the subject's fraudulently declared bankrupt company.

Source: Belgium

Typology 3: General insurance claim fraud in insurance involving high value goods which were purchased with illicit funds

The cases which illustrate this typology represent a general structure of criminal behaviour in the insurance sector by transferring illicit funds into clean money paid by an insurance company. It has to be kept in mind however that the prime motivation for the transaction need not be money laundering (although it could be the case that premiums have been paid using dirty money, as described in the following case). Only these cases require special attention from an anti money laundering perspective.

Case Example 3

In Norway in January 2004 a person reported a break-in in his house to his insurance company. The person reported that some of the stolen goods were jewellery worth NOK 110,000. Pursuant to his report he had sold a boat for NOK2.7m and received jewellery worth NOK 500,000 as part of the payment for the sales amount. This person was on a low income and had no assets. In 2000 he had no income or assets at all. In 2001 his income was NOK 43,000 and in 2002 his income increased to NOK 233,000. Either it was not possible for him to have been the real owner of this valuable boat or it was the case that he paid for the boat with illicit funds.

Source: Norway

Typology 4: Cash payments to purchase insurance

Cash payments still play a certain role in insurance business, predominantly but not only in developing markets. Where large cash amounts are accepted in developed markets it is usually via intermediaries.

Case Example 4

Two subjects who lived outside the jurisdiction concerned deposited large cash sums in 4 single premium life policies. Subsequent premiums came from bank accounts which had been previously investigated for trade in illegal narcotics from Latin America to Western Europe.

Typology 5: Cooling off periods, which allow for refunds of premiums with clean money within the contract cancellation period

A vulnerability which relates to the easy access to products is to be seen in this specific typology. In some jurisdictions a number of life products provide the customer's right to cancel the contract within a short period of time ("10 days free look" or "cooling-off period"). The customer will then get a refund of the paid premiums with clean money.

Case Example 5

Mr P invested £25,000 in an Investment Bond [an investment type insurance policy], the monies had come from the sale of a house, which was confirmed by a letter from his solicitor. The monies having come direct from the solicitor's client account. The bond was taken out by Mr P's sister who has power of attorney over his financial affairs because Mr P is in prison.

Within the cooling off period the bond was cancelled, Mr P's sister stated that her brother was not happy with the chosen bond. The funds were returned to Mr P's sister. This appears to be an attempt to layer monies that may have been obtained through the proceeds of crime. By divesting his assets Mr P may be attempting to frustrate any attempt by law enforcement to confiscate his assets

Source: UK Based Insurance Firm

Typology 6: Collusion of customer intermediary and / or insurance company employees

Several cases have shown collusive behaviour between either the customer and the broker or intermediary or between the intermediary and the insurance company. The intermediaries involved accepted illicit funds and transferred them in exchange for high commissions.

Case Example 6

A drug trafficker purchased a life insurance policy with a value of USD 80,000. The policy was purchased through an agent of a large life insurance company using a cashier's cheque. The investigation showed that the client had made it known that the funds used to finance the policy were the proceeds of drug trafficking. In light of this fact, the agent charged significantly higher commission. Three months following this transaction, the investigation showed that the drug dealer cashed in this policy.

Source: Canada

Typology 7: Third party payments of premiums

This typology refers to the funding of insurance policies by third parties/ persons different to the policyholder who have not been subject to the regular identification procedures when the insurance contract was concluded. The source of funds and the relationship between policyholder and third party is unclear to the insurance company.

Case Example 7

A husband and wife had taken out a life-insurance policy each in their own name with annual premiums. In the event of the death of one of the spouses, the other spouse would become the beneficiary of the insurance. The holder of the account through which the premiums had been paid was found not to be the policy-holders but a company abroad of which they were directors. However, this was a life-insurance policy taken out privately by the couple and not by the company. Investigation revealed that the scenario set up had been intended to conceal the illicit origin of the funds which originated from serious and organized tax fraud for which the couple involved was known.

Source: Belgium

Typology 8: Risks involved in international transactions - both where this is source of business or a destination of policy payouts

International transactions exist in a variety of constructions: a rather simple pattern is the payment of premiums from a foreign bank account or the payout of policies to a foreign jurisdiction. Typologies include those with more complex transfers of money via bank accounts or cheques through different jurisdictions, which complicates the control of the (legal) source of funds by the insurance company. Other forms are foreign customers and customers domiciled abroad who seek insurance policies via domestic or foreign intermediaries. The policy payout is usually to a foreign jurisdiction.

Case Example 8

An insurance company was approached with an offer to conclude 4 life policies against one-off payments of 75m for euros each policy. The structure was to be: the policyholder and his 3 partners were to be granted a loan of 340m euros by a large foreign bank. Each would pay 75m euros of this into a deposit account with the insurer. The remaining 40m euros were to be held and invested by the bank to service the loan. The bank would guarantee annual interest of not less than 6% over the entire term of the loan. The loan would be settled in full on maturity by the insurance payments. The policies would be ceded to the bank.

Source: Germany

Case Example 9

A number of insurance companies, domiciled in the Isle of Man and the Bailiwick of Guernsey, were identified through information received in a narcotics smuggling investigation as having numerous policies which were paid for with drug proceeds. It was determined that narcotics proceeds were deposited into life insurance policies over a substantial period of time prior to 2001. These policies were primarily established by one "master broker" who operated in Colombia and other South American jurisdictions. For the policies that were identified as containing drug proceeds, the funds entered the policies in several ways. First, and most common, were via third party wire transfers. These wire transfers often originated from money brokers or *casas de cambio*. In many instances, one bulk wire transfer was sent to the institution on the order of the broker. Once credited to the institution's account, the broker provided detailed information of how to break up the wire and which accounts to credit the funds to. The insurer also received payments via third party cheques and structured money orders (to avoid reporting thresholds). Finally, some policies were paid with funds from the commission accounts of the brokers. In this scenario, the brokers accepted cash from the client in Colombia and credited the client's policy with funds from his business operating account or as a piece of his commission cheque.

Source: United States / Isle of Man

Typology 9: Fraudulent customers, insurance companies and reinsurance companies

Cases have been noticed where criminals established or took over complex corporate structures and then entered into business relationships with insurance companies to get insurance coverage. The purpose of the various commercial insurance contracts was to invest illicit funds. Sometimes this was facilitated by the fraudulent setting-up of insurance or reinsurance companies for money laundering purposes. Thus the criminals are able to invest proceeds of crimes and to apparently undertake legal business and initiate transfers of money behind the veil of an insurance company or reinsurance company.

Terrorist financing

Financial institutions have faced an ever increasing wall of new legislation and regulatory requirements over the past two years, a large proportion of which has focused on the topic of AML/CFT (Anti Money Laundering / Countering the Financing of Terrorism). Much has been written about the AML component and many of the red flags and typologies have centred around traditional views about the mechanics used in proceeds of crime cases.

These have almost universally been assumed to apply equally to the financing of terrorism.

However, experience shows us that the techniques employed by the money launderer are drastically different from those involved in terrorist financing. There are a number of reasons for this but perhaps the most obvious is that the objectives of the money launderer and those of the terrorist financier differ enormously. Put simply, whilst both need to achieve a disconnect between the source of funds and their entry in to the financial system, the money launderer seeks to achieve long term benefits from his crime and is prepared to obtain these in wide variety of forms, for example from the enjoyment of property assets through to the ongoing benefit from the income generated by a portfolio of securities. The terrorist financier is not interested in these outcomes. His objective is far simpler – to provide currency to those involved in supporting or committing acts of terrorism.

As a result money laundering typologies *tend* to involve long term strategies, large amounts and the use of vehicles which break the audit trail and which are interwoven with combinations of financial institutions forming various parts of the money laundering process. These have led to the identification of certain discernable transactions or account behaviour patterns known as 'red flags' which indicate potential ongoing money laundering. Such red flags have remained as part of static typologies and remain valid.

In the area of financing of terrorism the fundamental difference in the typologies is that they are a) predominantly based on banking institutions as the primary facilitator of the financing b) they are short term in nature (in exceptional instances this may consist of even 'one off' or dual transactions) c) they may involve differing combinations of money movement techniques and finally d) in general involve smaller amounts varying between £10,000 and £40,000. A further human factor which has also had an impact, highlighted by the 9/11 *ex post facto* analysis of hijackers and their actions in the US banks, is that there have been some incidents where

suspected individuals engaged in terrorist financing have been pinpointed by alert banking staff due to small actions of abnormal behaviour, such as:

- Indifference to the actual balance during substantial withdrawals;
- Abnormal preoccupation with speed time of transfer, whilst transferring the amounts in several phases to the same destination; and
- An apparent basic lack of knowledge by the depositor/transferor of the destination(s) themselves

Much depends upon the instinct and approach of the bank's staff at the time and occasion, but this can be enhanced by efficient training. Clearly, the difficulties for financial institutions and law enforcement agencies in being able to identify, investigate and prosecute terrorist financing activities lie in the speed, simplicity and disjointed nature of the various techniques. This is a far cry from the money launderer's use of offshore structures, involvement of other professionals and complex structuring activities. A note of caution though : Whilst terrorist financing in general involve smaller amounts this is not a golden rule, especially when it comes to the financial resources required in order to support sophisticated training, political and religious propaganda and support networks. Terrorist financiers operate at both ends of the spectrum.

So, what are the indicators or red flags which have been identified from the sources available to those researching this topic, including operational cases of suspected terrorist financing? A further note of caution : Whilst they are as up to date as possible, they may not stand the test of time in the light of future developments. This is due to the pragmatic and dynamic nature of terrorist financing. Like all supplementary assistance to operational criminal intelligence, they must be updated and adapted to ongoing intelligence.

TYPOLOGIES

Ten typologies have been identified as follows.

Typology 1: Bank to second bank transfers in two stages over an 8 day working period, followed by transfers of the majority of the funds from the second bank to third and fourth institutions simultaneously, with the remainder being withdrawn from the second bank in cash deposits, and then physically couriered.

Typology 2: Extra or 'top up' incoming transfers from overseas jurisdictions into a single account in which normal deposits and withdrawals are made compatible with the account holder's profile. These incoming transfers occur every two or three months with single spasmodic transfers over a period of six months made to the same overseas jurisdiction. Both incoming and outgoing transfers are about £40,000, which proves the exception to the universally held belied concerning small value transfers.

Typology 3: Use of credit cards having been applied for online, then drawing the card to the limit within a few days using cash advances through ATMs and over-the-counter at the same branch where the ID information was provided (then the card ceases to be used and ID details are subsequently found to be false).

Typology 4: Mixing cash with business turnover and phased increases. Small single premise enterprises or businesses, generally restaurants having steady turnover and banked daily, either by cash or electronic means, then after three to four months turnover increases, with the increase entirely cash based. There are also simultaneous single outgoing transfers which are made to a third party account(s) being slightly less than the turnover increase, but involving identical amounts.

Typology 5: Internet funnelling whereby the holder has internet banking access and receives electronic transfers from a number of accounts and every second or third day transfers the amounts received, less 5-10%, to another bank account in a different bank. The receiving bank account is then subject to a number of frequent comparatively small cash withdrawals.

Typology 6: Overseas transfers on a semi regular basis to a high risk country without any apparent business links to the account holder.

Typology 7: Use of debit cards. This involves the replenishing of issued debit cards by structured multiple short term deposits to avoid possible bank reporting thresholds, or wiring money into an account on which the debit card is issued from an account in a bank in a foreign country, followed by almost immediate multiple ATM withdrawals in that foreign country.

Typology 8: Short term NGO or charity accounts whereby charities or NGOs open accounts for a short period of time with no apparent reason, i.e. no short term fund raising events or stated aim of a raising funds in response to disaster or relief that has recently occurred.

Typology 9: Mixing of inbound charity funds whereby NGOs or religious charities hold a number of accounts with each account relating to a number of businesses, charities or educational operations which the charity undertakes. The donations originate from the UK, then two or more of the charities' accounts (generally two, which are obscure amongst the overall number of accounts and can be utilised alternatively) after three months start to receive international fund transfers from a similar religious charity or education facility in a high risk jurisdiction.

Typology 10: Credit card placement and staged internet transfers. This involves the holder obtaining a credit card through a bank and initially using it sparingly with payments made against the outstanding monthly balance of the credit card by cash over-the-counter at a number of branches, followed by a steady increase of the monthly outstanding amounts with a number of large purchases and cash advances. Each month the outstanding balance is repaid by cash but additional cash is also placed on the credit card making the account in credit. Purchases and cash advances continue to be made but now transactions are made over the internet to other accounts with other institutions.

In terms of the above typologies, these have been identified as being associated with the following countries and jurisdictions which should be considered as high risk for terrorist financing purposes:

- Pakistan
- Yemen
- Egypt
- Algeria
- Paraguay
- Thailand
- Malaysia

Although the last three jurisdictions are not high risk in terms of terrorism, they have been identified as countries used for onward transit of funds; and in the case of the last two, mainly in large scale cash amounts.

Conclusions

Whilst the focus in recent years has been on money laundering, financial institutions need to be alert to the very real differences between the terrorist financier and the money launderer. The consequences for failing to detect these signs can have significant reputational risks, both from a corporate and a personal perspective. As we have seen from the US authorities' willingness to export their own particular brand of litigation and international policy, it does not take much to envisage UK banking institutions and their officers on the receiving end of an Anti Terrorism Act lawsuit or proceedings under the Patriot Act.

Non-profit organisations ("NPOs") and links to terrorist financing

Most countries share the concern over the difficulties in detecting terrorist financing through misuse of NPOs. It is generally acknowledged that NPOs play a crucial social and financial support role in all societies, and it is obvious that this role is not being called into question. Nevertheless, the sheer volume of funds and other assets held by the charitable sector means that the diversion of even a very small percentage of these funds to support terrorism would constitute a grave problem. Therefore, the limited knowledge about the extent to which terrorists may be exploiting the NPO sector should be considered a matter of serious concern for the whole international community.

NPOs possess many characteristics that are particularly vulnerable to misuse for terrorist financing. They enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often exactly in or next to those areas that are most exposed to terrorist activity. Finally, depending on the country and legal form of the NPO, they are often subject to little or no regulation (for example, registration, record keeping, reporting and monitoring) or have few obstacles to their creation (for example, there may be no skills or starting capital required, no background checks necessary for employees, etc.)

TYPOLOGIES

Typology 1: NPOs used to raise funds

NPOs can be used by terrorists and terrorist organisations to raise funds. Often – but not always – these organisations have applied for and received a formal charitable or tax exempt status. Moreover, some of these organisations have been reported to have used rather aggressive fund raising techniques, sometimes seeking donations from the public at large, and in other instances focusing on certain target groups, particularly within specific ethnic or religious communities. As part of the fund raising, the importance of informal cash collection in many ethnic or religious communities and the difficulties in accurately monitoring those funds can not be underestimated. Although it is most likely that the vast majority of these funds are raised and used for entirely legitimate charitable purposes, the obvious potential for abuse is nevertheless problematic. The existence or pretence of cash collections can also facilitate the integration of the proceeds of criminal activities carried out by terrorist groups into the "legal financial system".

These funds are then represented as legitimate charitable cash collections for an NPO and thus are a form of money laundering for terrorist purposes.

Case Example 1

A registered charity, ostensibly involved in child welfare, used video tapes depicting religious "freedom fighters" in action in various countries, together with graphic images of atrocities perpetrated against members of that religion. The tapes contained an appeal to send donations to a post office box number to help in the "struggle". These tapes were apparently widely distributed around religious establishments throughout the region. The same post office box number was associated with a further appeal in magazines which published articles by well known extremists.

Typology 2: The use of NPOs to move funds

NPOs can also be used by terrorists to move funds. In these cases, terrorists exploit the fact that financial transactions that effectively transfer funds from one geographic location to another — often across national borders — are regarded as the normal business of certain types of foundations and charities. In some instances, the legal form and ostensible purpose of the NPO seems to have been chosen carefully in order to avoid regulation and monitoring (for example, cultural associations established in some countries by indigenous ethnic communities). Some specific sub-typologies exist whereby networks of related foundations in different countries are established within a particular ethnic community and then seem to function as a framework for illegal alternative money remittances. Although it is not clear whether any of these schemes are directly related to terrorist financing, the structure of the networks is interesting because of its unusual characteristics and potential for abuse. The examples also show that there can be little to distinguish between transfers within or among NPOs and the provision of illegal money remittance services. These "alternative money remitters" make use of NPO bank accounts to collect cash deposits and settle the accounts with their overseas contacts. In some cases, these transactions were considered suspicious by the competent authorities because of the incongruity between the amounts handled and the modest living conditions of the particular community that provides financial support to the NPO in question.

Case Example 2

An FIU in Country A obtained updated information from the United Nations Security Council consolidated list of designated persons and entities. One of the organisations conducted its operations under different variations of the same name in a number of countries. It was described as a tax-exempt NPO whose stated purpose is to conduct humanitarian relief projects throughout the world. Among the multiple locations provided by the United Nations for branches of this organisation, several of the addresses were in Country A. The FIU received a suspicious transaction report on the NPO listed at one of the addresses indicated by the UN list. The report indicated bank accounts and three individuals with controlling interest on the address in Country A. One of the individuals (Mr. A) had an address that matched one of the addresses indicated on the UN list, and the other two individuals had addresses in two different countries. A search by the FIU revealed that the Mr. A was linked to these organisations, as well as to four other international NPOs. Reports received by the FIU detail multiple wire transfers sent from locations of concern to the branches of the above-mentioned charity and to Mr. A.

Typology 3: Logistical support and cover

NPOs can also be used to provide direct logistical support to terrorists or serve as a cover for their operations. This type of terrorist misuse is particularly evident among those NPOs that have several branches operating in multiple jurisdictions.

Case Example 3

An NPO was registered in Country X as a tax-exempt charity whose stated purpose is to conduct humanitarian relief projects throughout the world. Although the NPO was incorporated in Country X, it operated in various locations using slightly different names. Financial and business records were seized from the NPO's head office and the homes of the NPO's chief executive officer and a member of its board of directors. On the same date, Country X issued an order blocking the NPO's assets and records pending further investigation. Eleven months later, Country X submitted the NPO to the UN for designation under relevant UN Security Council resolutions for its support of a terrorist organisation. Country X convicted the chief executive officer of the NPO for fraud and organised crime related offences for diverting more than USD 315,000 of charitable donations to terrorist organisations. Prior to these actions, there is evidence that the NPO had provided both direct and indirect financial support terrorist organisations.

Typology 4: Official vs unregistered NPOs

It is important to distinguish between NPOs that officially register as charities and then use their status to tap into a broader base of funding and those NPOs that perform a less visible function, sometimes avoiding registration or tax exemption altogether. Often these unregistered NPOs obtain their funds from or provide services for certain ethnic communities. Such NPOs may be more commonly known as cultural associations or associations or foundations with community-related activities rather than as charities.

Typology 5: International vs local NPOs

A distinction can also be made between NPOs that operate internationally and those that have a local function. There is a common misperception that NPOs can only be misused in an international context by raising funds in donor countries and then sending these funds abroad to terrorist groups in third countries. Although internationally active NPOs may be more vulnerable to misuse, terrorist financing may also occur within NPOs that operate exclusively within national boundaries. Countries that have an internal terrorist problem clearly have experience with NPOs operating within their borders being misused for the financing of local terrorist groups. A related misconception is that the misuse of NPOs by terrorists is exclusively related to religious extremism.

Typology 6: Complicity between the NPO and its donors

Another distinction that can be made relates to the differing degrees of complicity between an NPO and its donors. While many cases involve corrupt or complicit management of the NPO as a contributing if not primary reason for the link with terrorist financing, there are also reported examples of largely innocent NPOs that were exploited by a few infiltrators who were able to siphon off or divert the funds of the organisation. Moreover, an innocent NPO could also be the victim of an unrelated recipient organisation or related branch office. There are even cases of bogus fund raising, where the name of existing and unwitting NPO was used as a cover for illegal fund-raising.

Politically exposed persons ("PEP")

PEP is the term used for individuals who are or have been in the past entrusted with prominent public functions in a particular country. This category includes, for example, heads of State or government; senior politicians and government, judicial or military officials; senior executives of State owned corporations and important political party officials. Because of the special status of PEPs – politically within their country of origin or perhaps diplomatically when they are acting abroad – there is often a certain amount of discretion afforded by financial institutions to the financial activities carried out by these persons or on their behalf. If a PEP becomes involved in some sort of criminal activity, this traditional discretion given to them for their financial activities often becomes an obstacle to detecting or investigating crimes in which they may be involved.

Typology 1: Source of PEP funds

The sources for the funds that a PEP may try to launder are not only bribes, illegal kickbacks and other directly corruption-related proceeds but also may be embezzlement or outright theft of State assets or funds from political parties and unions, as well as tax fraud. Indeed in certain cases, a PEP may be directly implicated in other types of illegal activities such as organised crime or narcotics trafficking. PEPs that come from countries or regions where corruption is endemic, organised and systemic seem to present the greatest potential risk; however, it should be noted that corrupt or dishonest PEPs can be found in almost any country.

Case Example 1

A video tape aired in Country A showed presidential adviser Mr Z purportedly offering a bribe to an opposition politician. This publicity about Mr Z, widely regarded as the power broker behind then-President in Country A, led the president to appoint a special prosecutor prompting numerous other investigations in Country A into the illicit activities of Mr Z and his associates. An investigation initiated by authorities in Country B authorities froze approximately USD 48 million connected to Mr Z. Mr Z fled the country and was eventually captured and extradited to Country A to face corruption, drug trafficking, illicit enrichment and other charges.

Prior to the capture of Mr Z, an associate of Mr Z, Mr Y was arrested on a provisional arrest warrant and request for extradition from Country A. Mr Z and his associates, including Mr Y, generated the criminal proceeds forfeited in this case through the abuse of Mr Z's official position as advisor to former the President of Country A. Some of the principal fraudulent schemes involved the purchase of military equipment and service contracts as well as the

criminal investment of government pension funds.

Mr Y was involved in a huge kickback scheme that removed money from both Country A's treasury and their military and police pension fund. Mr Y and others used pension fund money and their own money to buy a majority interest in a Country C banking institution, Bank M which in June 1999 was bought by another bank in Country A. Mr Y was in charge of seeking investments on behalf of Bank M and identified construction and real estate projects for the bank and pension fund to finance. He also controlled the construction companies which built those projects. Mr Y established a pattern of inflating the actual cost of the pension fund investment projects by 25 percent and billed Bank M accordingly. Projects recommended by Mr Y were automatically approved by the board members at the police pension fund, as several of them received kickbacks. A USD 25 million project was fraudulently inflated by USD 8 million. Similarly, Mr Y covertly formed and controlled several front companies used to broker loans from Bank M in exchange for kickbacks from borrowers. When some loans defaulted, Mr Y would purchase the bankrupt projects at extremely low prices for resale at a profit.

In addition, Mr Y and members of Bank M's board of directors were authorised by Country A's government to arrange the purchase of military aircraft for the nation. In just two aircraft deals the government of Country A paid an extra USD 150 million, because of a fraudulent 30 percent mark-up added on to the sale price. This illicit money allegedly was funnelled through Bank M. From there, it flowed into numerous accounts under a variety of names in banks in foreign jurisdictions to conceal the origin of the funds.

Mr Y consistently used a group of banks abroad to launder his and others' share of criminal proceeds. Ms D, a banker who is married to Mr Y's cousin, formerly was a member of the board of directors of Bank N, helped Mr. Y conceal more than USD 20 million in one jurisdiction.

Mr Y opened a bank account in Country C, and moved about USD 15 million through it until he was arrested. Initially, the account opening did not raise any suspicion because Country A nationals often opened bank accounts in the Country C to protect their assets from inflation. However, financial institutions holding bank and brokerage accounts owned or controlled by Mr Y, Ms D and others gradually noticed unusual activity in the accounts. According to bank officials, Mr Y's financial transactions had no apparent business justifications and the origin of the funds was suspicious.

Typology 2: Use of middlemen to launder funds

PEPs, given the often high visibility of their office both inside and outside their country, very frequently use middlemen or other intermediaries to conduct financial business on their behalf. It is not unusual therefore for close associates, friends and family of a PEP to conduct individual transactions or else hold or move assets in their own name on behalf the PEP. This use of middlemen is not necessarily an indicator by itself of illegal activity, as frequently such intermediaries are also used when the business or proceeds of the PEP are entirely legitimate. In any case, however, the use of middlemen to shelter or insulate the PEP from unwanted attention can also serve as an obstacle to customer due diligence that should be performed for every customer. A further obstacle may be involved when the person acting on behalf of the PEP or the PEP him or herself has some sort of special status such as, for example, diplomatic immunity.

Case Example 2

The family of a former Country A senior government official, who had held various political and administrative positions, set up a foundation in Country B, a fiscally attractive financial centre, with his son as the primary beneficiary. This foundation had an account in Country C from which a transfer of approximately USD 1.5 million was made to the spouse's joint account opened two months previously in a banking establishment in neighbouring Country D. This movement formed legitimate grounds for this banking establishment to report a suspicion to the national FIU.

The investigations conducted on the basis of the suspicious transaction report found a mention on this same account of two previous international transfers of substantial sums from the official's wife's bank accounts held in their country of origin (A), and the fact that the wife held accounts in other national banking establishments also provisioned by international transfers followed by withdrawals. The absence of any apparent economic justification for the banking transactions conducted and information obtained on the initiation of legal proceedings against the senior government official in his country for embezzlement of public funds led to the presumption, in this particular case, of a system being set up to launder the proceeds of this crime. The official concerned was subsequently stopped for questioning and placed in police custody just as he was preparing to close his bank account. An investigation was initiated.

Typology 3: Use of offshore locations

Besides the use of third parties, PEPs involved in moving or concealing illegal proceeds generally do so by funnelling the funds through networks of shell companies or offshore banks in locations outside his or her country of origin that are not likely to divulge details of relevant transactions. In other cases, their financial operations may be concealed behind various other types of opaque legal arrangements such as trusts. Again, the ability of a financial institution to conduct full customer due diligence and apply know-your-customer principles to PEPs in this instance is severely restricted.

Case Example 3

An investigation into a senior government official Mr A, an employee of state owned Company A, uncovered that he was in receipt of excessive payments into a number of accounts that he owned and operated. Mr. A was the vice president of Company A and had a yearly income of over USD 200,000. The investigation revealed Mr. A had 15 bank accounts in several different countries through which over USD 200 million had been transacted. Mr. A used the money placed in these accounts to gain political influence and to win large contracts from foreign governments on behalf of Company A.

The investigation discovered that a trust account had been created to act as conduit through which payments from Company A were then transferred to a number of smaller accounts controlled by Mr. A. Mr. A would then transfer money from these accounts or make cash withdrawals. The funds, once withdrawn were used to pay for bribes. The recipients of these payments included: heads of state and government, senior government officials, senior executives of state owned corporations and important political party officials in several countries and family members and close associates of Mr. A.

Further investigation into the financial transactions associated with the accounts held by Mr. A revealed that a shell company was being used to make and receive payments. In addition to account activity indicated there were irregular cash deposits (often more than one a day) and unusually large of cash withdrawals; one account revealed that in one six week period over USD 35 million had been withdrawn in cash. This was inconsistent with all the previous activity on the account. The investigators noticed that there was also a deliberate smurfing of the cash deposits into smaller amounts indicating Mr. A had an awareness of reporting requirements and was attempting to avoid them. The beneficial owners of payments from Mr. A made both in

cash and by wire transfer implicated several PEPs and associates of PEPs:

The senior politician, senior official

An intermediary received a payment of USD 50 million from Company A. The intermediary then transferred the money into two accounts held off-shore; the funds were then moved to company accounts that were also held offshore. The beneficial owners of these company accounts were discovered to be a former head of the secret service in Country B and a state secretary for the Ministry of Defence in Country C.

Wife of a PEP

Money was transferred from Company A to one of the bank accounts owned by Mr. A; Mr. A then placed funds into a solicitor's client account and an off-shore bank account. The beneficial owner of the off-shore account was the recently divorced wife of a PEP - Ms. C. The account was provided with funds for the purchase a property valued at over USD 500,000, a car, the redecoration of Ms. C's flat and a monthly allowance of USD 20,000.

Friend and associate of the PEP

Company A made a payment to a bank account in Country D. The bank in Country D was then instructed to transfer the money to an associate of Mr. A, who held an account in the same bank in Country D. The associate then 'loaned' the same amount of money to a PEP.

Non financial professions in money laundering (solicitors, notaries and accountants)

As anti-money laundering measures are implemented in financial institutions, the risk of detection becomes greater for those seeking to use the banking system for laundering criminal proceeds. Increasingly, money launderers seek out the advice or services of specialised professionals to help facilitate their financial operations. This represents an increasing trend toward the involvement of various legal and financial experts, or gatekeepers, in money laundering schemes.

Solicitors, notaries, accountants and other similar professionals perform a number of important functions in helping their clients organise and manage their financial affairs. First of all, they provide advice to individuals and businesses in such matters as investment, company formation, trusts and other legal arrangements, as well as optimisation of tax situation. Additionally, legal professionals prepare and, as appropriate, file necessary paperwork for the setting up of corporate vehicles or other legal arrangements. Finally, some of these professionals may be directly involved in carrying out specific types of financial transactions (holding or paying out funds relating to the purchase or sale of real estate, for example) on behalf of their clients.

All of these perfectly legitimate functions may also be sought out by organised crime groups or the individual criminal. They may do so for purely economic reasons; however, more important is the desire to profit from the expertise of such professionals in setting up schemes that will help to launder criminal proceeds. This expertise includes both advice on the best corporate vehicles or offshore locations to use for such schemes and the actual establishment of corporations or trusts that make up its framework. Gatekeepers may also be used to offer the veneer of legitimacy to their operations by serving as a sort of intermediary in dealing with financial institutions. If one looks at the types of assistance that these professionals may provide, it is apparent that some of these functions are the gateway through which the launderer must pass to achieve his goals. Thus the legal and accounting professionals serve as a sort of "gatekeeper" since they have the ability to furnish access (knowingly or unwittingly) to the various functions that might help the criminal with funds to move or conceal.

Professional Services Provided by . . .	
Lawyers	**Accountants**
Legal advice	Financial advice
Advocacy	Audit practice
Wills / probate	Tax advice and tax structuring
Property transactions	Bookkeeping
Investment services	Company formation
Trust	Company administration
Company formation	Trust
Company administration	Property transactions
Introduction to banks	Introduction to banks

The typologies below focus on one of the key activities of non financial professionals, namely as trust and company service providers although other services, such as tax advice may also form part of any money laundering scheme.

TYPOLOGIES

Typology 1: Multi-jurisdictional structures of corporate entities and trusts

In many instances, a structure consisting of a series of corporate entities and trusts — created in different jurisdictions — is used to hide identity and carry out a fraud scheme. The complex structure can give the appearance of a legitimate purpose, which can then be used to easily attract investment from third parties. For the third parties that are victims of such schemes, it is almost impossible to see behind the structure of the various corporate entities to find out who is liable for their loss. By setting up such a complex multi-jurisdictional structure, the seemingly logical money flow between these entities is used to move and launder criminal money. These structures can also be convenient for diverting the money flow or hiding payments.

Case Example 1

Mr. S headed an organisation importing narcotics into country A, from country B. A lawyer was employed by Mr. S to launder the proceeds of this operation.

To launder the proceeds of the narcotics importing operation, the lawyer established a web of offshore corporate entities. These entities were incorporated in a Country C, where scrutiny of ownership, records, and finances was not strong. A local management company in Country D administered these companies. These entities were used to camouflage movement of illicit

funds, acquisition of assets, and financing criminal activities. Mr. S was the holder of 100% of the bearer share capital of these offshore entities.

In Country A, a distinct group of persons and companies without any apparent association to Mr. S transferred large amounts of money to Country D where it was deposited in, or transited through Mr. S's offshore companies. This same web network was found to have been used to transfer large amounts of money to a person in Country E who was later found to be responsible for drug shipments destined for Country A;

Several other lawyers and their trust accounts were used to receive cash and transfer funds, ostensibly for the benefit of commercial clients in Country A. When they were approached by law enforcement during the investigation, many of these lawyers cited "privilege" in their refusal to cooperate. Concurrently, the lawyer established a separate similar network (which included other lawyers' trust accounts) to purchase assets and place funds in vehicles and instruments designed to mask the beneficial owner's identity. The lawyer has not been convicted of any crime in Country A. Investigators allege however that his connection to and actions on behalf of Mr. S are irrefutable.

Typology 2: Specialised financial intermediaries / professionals

The cases related to this typology highlight the fact that, when there is evidence of the misuse of corporate vehicles, a specialised financial intermediary or professional has often been involved, to a greater or lesser extent, in facilitating the formation of an entity and exploiting the opportunities presented by foreign jurisdictions to employ various arrangements that can be used for legitimate purposes but also can be used to help conceal true beneficial ownership, such as corporate shareholders, corporate directors and bearer shares. The degree of complicity of these financial intermediaries and professionals varies widely, with some unknowingly facilitating illicit activities and others having greater knowledge of their clients' illicit purposes.

Case Example 2

A law enforcement operation identified an accountant, Mr. J, who was believed to be part of the criminal organisation involved in money laundering and re-investment of illicit proceeds derived from drugs trafficking led by Mr. X. Mr. J's role was mainly that of a "legal and financial consultant". His task was to analyse the technical and legal aspects of the investments planned by the organisation and identify the most appropriate financial techniques to make these

investments appear licit from a fiscal stance. He was also to try as much as possible to make these investments profitable. Mr. J was an expert in banking procedures and most sophisticated international financial instruments. He was the actual financial "mind" of the network involved in the re-investment of proceeds available to Mr. X. Mr. J operated by sub-dividing the financial transactions among different geographical areas through triangle transactions among companies and foreign credit institutions, by electronic transfers and stand-by credit letters as a warrant for commercial contracts which were later invested in other commercial activities.

Typology 3: Shell companies

The use of shell companies to facilitate money laundering is a well-documented typology. Shell company typologies can be complex, using non financial professionals to hide the origin of the beneficial owners as well as the origin of the money. The complex case included here provides a "textbook" typology as an example of misuse of corporate vehicles. The scheme established here was intended to launder criminal proceeds through real estate investment. A complex structure was set up by legal professionals to hide the origin of the beneficial owners as well as the origin of the money.

Case Example 3

The investigations started in September 2003 by cross referencing data from an investigation on drug trafficking, with information coming from another investigation on assets owned by Eastern European citizens living in the Costa del Sol (Malaga).

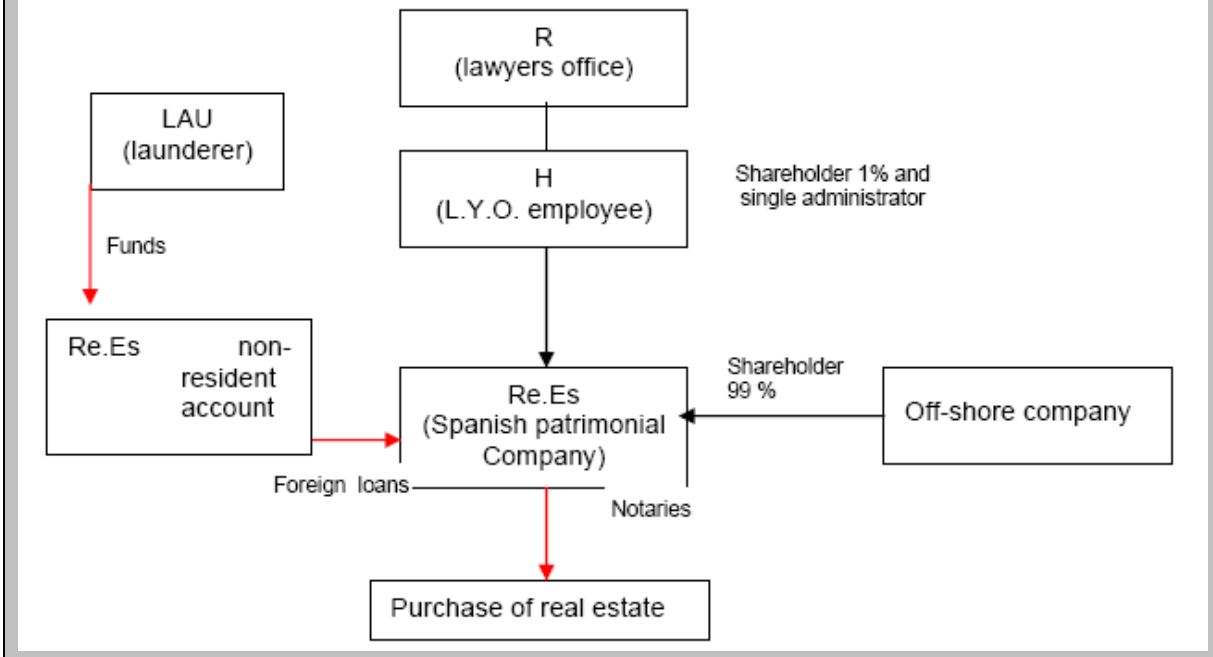
In such cross referencing of information it arose that [H] appeared as administrator of more than 300 companies established through [R], a lawyer's office in Marbella (Malaga).

All of the companies had similarities: companies established off-shore, except one held by [H] who was the single administrator of the companies and, at the same time, an employee of [R]. Giving support to clients of H by establishing companies was one of the activities of [R], which also offered the management of client's bank accounts and real estate buying and selling. The investigators knew that several clients of [R] were allegedly connected with international organized crime groups and/or with people involved in serious crimes in Spain and abroad.

The board of [R] was aware of the likely criminal activities of some of H's clients, because they had been the subject of media and press reports as possible criminals, and because the board knew that some clients were in prison in Spain or in other countries since documents had been

sent to them there. In other cases, members of the board were called to testify as witnesses in judicial proceedings against those clients. Additionally, the board deliberately ignored the activities of their clients. In their advertisements they even advertised that the office conducted company´ "engineering", that they guaranteed anonymity and that they did not ask any questions or respond to requests for information.

Diagram of the money laundering scheme



The Spanish companies were established for use as an instrument for money laundering schemes based on the real estate market. They were companies created exclusively for the management and administration of real estate properties. Re.Es. was one of these companies.

The off-shore companies which participated in the Spanish companies were "shell companies" established in an American State whose laws allow a special tax regime for these companies and for their transactions. The companies were pre-constituted in the name of an agent (usually a lawyer) before the incorporation of the company. In other words, the document of incorporation of the company would remain inactive in the hands of the agent until the company was bought by a client, and at that moment the company would be effective.

Therefore, the board of the companies when first registered was made up of the agent and his associate, without any link with the real owners of the company who subsequently purchased the shell. Consequently, the ultimate beneficiaries of the off-shore companies and, consequently, of the Spanish companies, remained hidden.

The launderer (LAU) transferred funds from a foreign country to a non-resident account owned by Spanish company Re.Es. The use of non-resident accounts provided other advantages, including the advantage of being subject to less control by the tax authorities. The funds described above were gathered in the account of Re.Es under the guise of foreign loans received. The destination of the funds received was the purchase of real estate properties in the name of Re.Es., in the last stage of the money laundering process, taking advantage of the hidden situation of the launderer and of the beneficial owners.

Three public notaries documented all the transactions, from the incorporation of the companies to the purchase of real estate. The suspicion of money laundering was clear: incorporation of several companies by the same persons in a short period of time, concurrence of the same partners in several companies, several real estate purchases in a short period of time, etc. Despite this, and even though the public notaries were obliged to report under the Spanish anti-money laundering law, such transactions were not disclosed to the Spanish FIU.

Money laundering through the securities sector

The securities sector on a global scale is characterised by its diversity, the ease with which trading can now take place (through electronic trading for example), and the ability to perform transactions in markets with little regard to national borders. These characteristics make securities markets attractive to the ordinary investor looking for a good return on his or her money. These same characteristics, along with the sheer volume of transactions in many markets, also make the securities sector a potentially inviting mechanism for the laundering of funds from criminal sources.

The illegal funds laundered through the securities sector may be generated by illegal activities both from outside and from within the sector. For illegal funds generated outside the sector, securities transactions or the creation of legal entities are used as the mechanism for concealing or obscuring the source of these funds. In the case of illegal activities carried out within the securities market itself – for example, embezzlement, insider trading, securities fraud, market manipulation, etc. – the securities transactions or manipulations generate illegal funds that must then be laundered. In both cases, the securities sector appears to offer the launderer the potential for a double advantage in allowing him to launder illegal funds and to acquire an additional profit from the related securities fraud.

TYPOLOGIES

Typology 1: Acceptance of cash and the entry of illegal funds into the securities sector

In many securities markets, only certain permitted persons or firms, such as stockbrokers, banks or certain independent financial advisors may perform transactions. These market operators are generally restricted or prohibited outright from accepting cash to carry out such transactions. Given that criminal funds in the form of cash must therefore be introduced into the financial system before entering the securities sector, the use of the securities sector for laundering was considered by the experts to be primarily part of the layering and integration stages of money laundering.

Despite this view that the securities sector is unsuitable for the placement stage of laundering, a few cases have occurred in which a broker has accepted cash payments in violation of industry practice or formal rules against the practice. While the acceptance of cash likely represents the minority of laundering operations in most markets, the reliance on commissions as a source of

income for securities market professionals can exert pressure to accept cash in violation of rules or procedures.

Case Example 1

A stockbroker in Country C continuously accepted cash deposits from a client in the range of USD 7,000 to USD 18,000. The funds were placed in the money market fund of the client's sister and withdrawn through the issuance of cheques. After the broker was arrested on unrelated embezzlement charges, the client's identity became known to law enforcement. When the police conducted a background check on the client, it was revealed that the stockbroker's client was a known drug dealer.

Typology 2: Layering of illegal funds

Another way to use the securities sector to launder illegal funds generated by non-securities related criminal activities is to purchase securities with illegal funds that have already been introduced into the financial system, that is, at the layering stage of laundering.

Case Example 2

A brokerage firm opened several accounts for a group of twelve linked individuals, including a non-resident account that was used to record very large movements and apparently to centralise most of the suspected flows, which totalled more than USD 18 million.

The launderers used the following two mechanisms:

- the accounts of some of the parties involved were credited with large sums received from countries of concern, which were invested in the stocks of listed companies in Country W; and

- the accounts of the individuals concerned were credited with sums from regions of concern, which were transferred to the non-resident account (the first accounts were used as screens).

This securities buy/sell mechanism was used to filter the flows through the broker and subsequently the clearer and custodian. Once filtered, the funds were sent to locations in regions of concern and offshore financial centres. This information showed that the co-opted broker had been used to launder the proceeds from various forms of frauds. The manager of the brokerage firm served as a relay for the criminal organisations involved.

Typology 3: Setting up a company as a front for money laundering

In certain instances, mechanisms within the securities sector may be used for laundering funds regardless of whether their illegal origin is within or outside the securities sector. One such method is the establishment of a publicly traded company specifically to serve as a front for a money laundering operation. The typical example of such a scheme is for a criminal organisation to create a company for a legitimate commercial purpose and then to commingle illegal funds with funds generated by the legal commercial activity. Usually, the company would have to use various fraudulent accounting practices in order to succeed in such an operation. The establishment of various offshore entities through which funds may be channelled offers another way of obscuring the true intent of the operation. The advantage of using a publicly traded company for such a scheme is that its owners could profit twice from the mechanism: first in creating a successful means of laundering criminal funds and secondly in selling shares in the business to unwitting investors.

Case Example 3

In 1994 a small eastern European enterprise was incorporated in Country A and started trading on a venture capital market. Company B supposedly manufactured magnets at its European subsidiary and was also in the business of trading oil to and from the former Soviet Union. During this period, the company was reporting tens of millions of dollars in sales and its year over year sales growth was double digit. The company's head office was located in Country C and in 1996, as a result of its dramatic growth, it met the listing requirements and its shares started trading on one of the stock exchanges of Country A.

The company was able to attract a high profile board of directors, including a former high ranking politician and was represented by a well-known established law firm. It had been identified that the founding shareholders of the European enterprise were connected to an Eastern European organised crime group and whose interest in the company had been relinquished through a series of transaction in European and Caribbean "tax havens".

In the spring of 1997, Company B sought to raise an additional USD 74 million to make acquisitions and assist in the operations of the Company. The staff of the securities regulator agency in Country A became aware of "soft" intelligence that was impossible to confirm that raised concerns about the ongoing role of the Eastern European organised crime group in Company B. After an initial audit by a firm located in Country C, with the help of subaudit by an accounting firm from the country of the European subsidiary, after a special review by a

major international accounting firm of the original audit and after a new audit by a different major international accounting firm, all of which gave Company B a clean audit, the USD 74 million prospectus was receipted. Four months after giving Company B a clean audit opinion, the auditors advised the company that they were extremely concerned about connections to organised crime and that many transactions may have been bogus. Eventually it was determined that the company was a front for laundering money and that:

– Sales were fictitious and bank accounts belonging to Company B were commingled with accounts belonging to entities controlled by the Eastern European crime group.

– Many sales transactions were conducted on a "cash" or barter basis.

– Assets were purchased from entities controlled by the Eastern European crime group valued at ten times their real value.

– Bogus sales commissions were paid to individuals belonging to the entities controlled by the Eastern European crime group.

– A Company B operating account was controlled by a member of the Eastern European crime group, and transactions involving millions of dollars went through the account.

– Company B engaged in transactions whereby suppliers of magnets, providers of goods and services, buyers of magnets and sellers of technologies were the same parties, that is, entities controlled by the Eastern European crime group.

– In respect to the USD 74 million offering, approximately USD 32.2 million was placed in an "unacceptable offshore bank" by an entity controlled by the Eastern European crime group.

In addition to laundering substantial sums of money for individuals and entities connected to the Eastern European crime group, original shareholders were able to sell their original shares on the open market and transfer the profits to Eastern European banks. At the end of the day, the original shareholders and their nominees profited from the sale of Company B stock in excess of USD 65 million. In May of 1998, Company B's headquarters in Country C were raided by the police, and in the same month the securities regulatory agency in Country A halted trading of Company B shares. In November of 1999, the securities regulatory agency initiated proceedings in this matter.

Typology 4: Market manipulation and money laundering

The term "pump and dump" is used by securities regulators and law enforcement authorities to describe the artificial inflation of a stock based on misleading information. This typical sort of securities fraud generates proceeds and is therefore a predicate offense for money laundering in most jurisdictions. In addition, there have been cases where this type of securities fraud has been set up with the proceeds of other crimes, and sometimes money laundering can be used to advance this fraud.

In a "pump and dump" scheme, individuals obtain large blocks of stock in a company before it is publicly traded or while it is dormant or not yet operational. A money launderer may use proceeds to purchase these large blocks of stocks. The shares are usually obtained at an extremely low price. After the perpetrators have accumulated large stock holdings in the company, they may utilise unscrupulous brokers to promote the securities to their clients. At this point, the securities fraud begins. Misleading information is released to the public – including in one example through the Internet – to promote the company and its business operations. Often, the company is misrepresented as having a revolutionary new product that will lead to future business success. As this false information is circulated, the share prices for the company rise due to public interest and increased demand. In the typical operation, the company has no legitimate operation and the information given to the public is simply provided to inflate the price of the shares. In order to create the appearance of market demand, the perpetrators of securities fraud may divide transactions among several brokers and / or channel transactions through multiple jurisdictions.

When the shares reach a peak price, the perpetrators of this securities fraud sell off their share holdings and obtain a profit from the artificial inflation of the price. Eventually, the company is permitted to fail and the shares become worthless. At this point, two events have occurred: (1) the money launderer, by selling his stock in the company, has layered the illicit funds he originally invested; and (2) as a perpetrator of a securities fraud, he has generated additional illicit proceeds that require laundering.

Case Example 4

The money in question came from a drug-trafficking organisation and was used to purchase two listed companies. During an investigation by the police of Country V into the laundering of money from drug trafficking, it was found that a money launderer had planned and executed a plan to feed large sums of money from a mafia related organisation into the stock market. The

money, which was the proceeds of various frauds, was deposited in a private bank, controlled by the mafia organisation itself, located in Country R located in the Caribbean region.

The plan included the purchase of two companies established in Country V and listed on the stock market. These were a stock brokerage and a small bank. The first stage took place as planned. Numerous small investors from abroad using false names bought the shares in the two firms. The aim was to ensure that none of the investors bought more than the percentage of ownership that would have required reporting under country V's laws.

Through fictitious general shareholders' meetings in which lawyers were involved, a new board of directors was appointed with people acting as front men for the money launderer, Mr. W. Upon gaining control of the two companies, Mr. W immediately granted full powers to the members of the criminal organisation, thus guaranteeing their control over the money.

Subsequently a share increase was applied for, and all the legal requirements were met. Again, they took care to ensure none of the investors exceeded the 5 percent limit. The share increase in the two companies came to approximately USD 42 million, which was subscribed and disbursed through banks in Country V. In reality the proceeds of the market manipulation, including the original funds, were then laundered by transferring the money from Country R to banks in Europe, from where it was transferred to Company N was located in Country Y, another offshore financial centre, and owned marble mines in South America. The money then returned to Country R, having first passed through accounts in Europe and North America. The same money then went around the circuit again, so as to simulate foreign investments in the share capital of the two companies.

Through this circular process of share buying and selling the price of the shares rose to 640 percent of their face value. To achieve this, the complicity of the brokers trading in the shares on the stock market was necessary. The over-priced shares were subsequently delivered to the mafia investors who were the final victims of the fraud when the police prevented the money launderer from controlling the price of the shares.

Correspondent banking

Correspondent bank accounts are accounts that financial institutions maintain with each other on their own behalf and in their own names. International correspondent banking relationships have a variety of legitimate business purposes. However, these relationships are vulnerable to misuse for money laundering. Shell banks, certain offshore financial institutions and banks from non-cooperative countries and territories (NCCTs) are of particular risk to legitimate correspondent banking relationships.

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). By establishing multiple correspondent relationships globally, banks can undertake international financial transactions for themselves and for their customers in jurisdictions where they have no physical presence. Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks obtain a wide range of service through the correspondent relationship, including cash management (for example, interest bearing accounts in a variety of currencies), international wire transfers of funds, cheque clearing, payable-through accounts and foreign exchange services. The services offered by a correspondent bank to smaller, less well-known banks may be restricted to non-credit, cash management services. Those respondent banks judged to be sound credit risks, however, may be offered a number of credit related products (for example, letters of credit and business accounts for credit card transactions).

TYPOLOGIES

Typology 1: Laundering facilitated through lack of direct contact

By their nature, correspondent banking relationships create a situation in which a credit institution carries out financial transactions on behalf of customers from another institution. This indirect relationship means that the correspondent bank provides services for individuals or entities for which it has neither verified the identities nor obtained first-hand knowledge of the respondent's customers. In correspondent banking therefore, the correspondent institution must rely on the respondent bank's having performed all of the necessary due diligence and continuous monitoring of its own customers' account activity. Some additional risks incurred by the correspondent bank include in particular:

- Assessing the quality of anti-money laundering mechanisms in place at the respondent bank. For example, a foreign respondent bank may apply less stringent anti-money laundering standards due to weaker laws and regulations, inadequate regulatory supervision, or failures in applying standards or internal controls. While the correspondent bank may be able to determine the legislation in effect for the respondent bank, it is much more difficult to know the degree and effectiveness of the supervisory regime to which the respondent is subject;

- Existence of sub-respondents through which a respondent bank may itself be offering correspondent banking facilities to other credit institutions. An oversight in not establishing the extent to which this occurs can mean that the correspondent bank is even farther removed from knowing the identities or business activity of these sub-respondents, or even the types of financial services provided; and

- Monitoring individual transactions involved in large-scale transactions between correspondent accounts since the bank is usually not in contact with the originator or the beneficiary of such transactions.

Case Example 1

A bank in an FATF member country (Country D) monitored activity over a given month through a correspondent account maintained at the Country D bank by a bank from another FATF country (Country E). The Country D based bank detected a particular customer of the Country E bank that appears to be a shell company and has either sent wire transfers to or received wire transfers (a total of 51 received transaction totalling USD 7.4 million) from other suspected shell entities. Some of these other suspected shell companies are based in Country D and maintain accounts at a bank in Country F. The Country D reporting bank notes that some of the transactions appear to be petroleum/oil products, but sample internet searches conducted on some of these possible shell companies involved as parties to the wire transfers did not provide additional information.

The same Country D bank, in continuing to monitor the activity in the same Country E bank's correspondent account, pinpointed another suspected shell company involved in suspicious wire transfer activity. Public and official company registry searches conducted by the Country D bank did not reveal any substantiating information on the particular shell entity. Address directory searches, for example, simply led to an apartment and individual's name. Over several

months, the suspected shell entity, for example, had received USD 6.4 million in wire transfers from various other suspected shell entities (some of which are also based in Country D and maintain accounts at Russian banks). At least one of these entities is the subject of prior multiple STRs submitted by this and other financial institutions.

Corruption and private banking

Private banking is the term used for "preferential" banking service provided to high net worth individuals. Within the institution, this service usually entails a higher degree of discretion and confidentiality for the client in comparison with the ordinary retail customer. Financial institutions often separate private banking from other retail banking operations as part of their customer segmentation strategy, that is, specific financial services are marketed across a customer base according to the value of the service offered. Private bank accounts can be opened in the name of an individual, a commercial business, a trust, an intermediary or an investment company. These services are administered by a relationship manager and his support team who sometimes are on call 24 hours a day and 7 days a week in order to build a strong rapport and intricate knowledge of the client's financial affairs. The services offered by private bankers are often self-administered and frequently go beyond the call of duty of a normal retail banker.

TYPOLOGIES

Typology 1: The PEP problem

Private banking's vulnerability that could be exploited by corrupt PEPs or their associates relates to when the private banker simply fails to apply appropriate and thorough due diligence to a customer and his activities. A criminal or PEP will generally seek out private banking services, as they offer the ideal opportunity for them, their family members, and close associates to carry out sophisticated and/or complex financial transactions that will further protect their illicit assets. Since a private bank is often involved in helping the client to invest or protect his or her assets, a private bank that fails to apply due diligence could find itself unwittingly assisting a corrupt politician to set up nominees and shell companies, ensuring therefore that the beneficial ownership remains hidden. The use of a professional intermediary to open an account on a client's behalf can also enable a corrupt public official to open and operate an account virtually anonymously.

Anti-money laundering procedures for due diligence and suspicious transaction reporting in FATF jurisdictions generally apply to all banking operations, including private banking, even if most members have not established specific procedures for this latter category. However, the low numbers of suspicious transaction reports from private bankers and the fact that reports are sometimes not made until a PEP is publicly exposed (for example through the media) as allegedly involved in corruption or other crimes indicates that there still might be a problem.

A failure to apply necessary due diligence in the private banking may simply be because of a lack of knowledge of the family, business or business connections that would indicate a PEP. Even if private banking customers are well known, their potential for corruption may not be. It is perhaps relatively easy to name the leaders of countries with a serious official corruption problem; however, it may be more difficult to name other members of the government, senior officials or their family members. Corrupt officials often use their relatives and other associates to launder their illegal obtain funds.

Case Example 1

The example relates to a merchant bank whose services included institutional brokering, retail brokering, private client services, global equity derivatives, securities, futures and margin lending. Clients of the merchant bank may enter into a private client agreement, which enables the client to perform transactions by telephone or facsimile. During the course of the investigation, difficulty was encountered in matching money coming into the suspect's trust account to any funds that had been sent out of the country by a co-offender. Upon reconstructing the money trail through bank deposit and withdrawal records, it was found that the co-offender had sent an equivalent amount of funds out of the country through international telegraphic transfers; however, the transfer did not record the co-offender as the ordering customer. The ordering customer was recorded in the name of the merchant bank. This provided a way to disguise the remittance of funds offshore.

Case Example 2

In Country A, an institution is established whose chairman is also the ruler of that country. This institution is the ordering customer in a payment transaction. Both the ordering customer and the beneficiaries are established in different parts of the world. Neither party is a customer of the bank in Country B.

A bank in Country B is affiliated with the national bank of Country A and is charged with a large part of that country's external payments. Payment is made through the bank in Country B, which acts solely as a correspondent bank for the banks of the ordering customer and the beneficiaries. Due to the lack of adequate due diligence on customers by the ordering institution in Country B (only the respondent has been monitored), the nature, motivation and exact (complete) purpose for the transaction can only be guessed at. These could be either

legitimate (many external payments are performed through the Country A bank) or illegal proceeds.

The exact role of Country A's ruler, the beneficiaries of the transactions, the basis for the payment, etc. are not available. This lack of information means that the bank in Country B would not normally be able to determine the significance of the transactions.

Bearer securities and other negotiable instruments

Securities instruments in bearer form consist of bearer bonds and bearer stock certificates or "bearer shares". As with registered securities, both of these instruments are issued by a particular corporate entity in order to raise capital. The difference between registered securities and securities in bearer form, among other things, is the method of transfer. In the case of registered securities, the instrument is issued to a particular individual, and the "owner" is recorded in a register maintained by the issuing entity. In the case of securities in bearer form, the instrument is issued; however, the owner is not recorded in a register. When registered securities are transferred to a new owner, the new owner must be recorded in order for the transfer to be valid. When bearer securities are transferred, since there is no register of owners, the transfer takes place by the physical handing over of the bond or share certificate.

Share certificates, whether in registered or bearer form represent equity within a corporate entity, that is, they represent shareholdings or ownership of a particular corporate entity. The number of shares owned by a person determines the degree of control that such an individual may have over the legal entity that issued the shares. In the case of registered shares, determining ownership is relatively straightforward, as the record of ownership is maintained in the share register of the issuing entity. Determining the ownership of bearer shares, in contrast, is not so easy since it depends on who possesses or has physical control of the share certificates. The obstacles to determining easily the ownership of bearer shares (and thus the ultimate owner of the corporate entity that has issued such instruments) are a factor that has been exploited by launderers to conceal or disguise true ownership of entities used in some money laundering schemes.

With regard to bearer bonds, it should be noted that their use in laundering operations has not yet been documented to the same extent as that of bearer shares. Because of the nature of bearer bonds as debt instruments however, it is possible that their anonymous transferability represents the chief characteristic that could be exploited by launderers rather than an ability to conceal ownership.

TYPOLOGIES

Typology 1: Transferability of ownership

In general terms there are considerable potential risks of abuse of these securities by launderers, primarily stemming from their ease of transfer and their utility in concealing or disguising

ownership of assets. In the case of bearer shares, it is particularly this last characteristic that poses the greatest problem. Especially when combined with excessive banking secrecy or other negative features, bearer shares seem to offer a very effective method of hiding the links between a criminal proceeds and the criminal himself.

Case Example 1

As a result of a drug importation investigation, approximately USD 1.73 million was restrained in combined assets from residential property and bank accounts. These assets were located in four countries in North America, the Caribbean and Europe. Significant assets restrained involved two offshore companies incorporated in Country A. Investigators also seized original bearer shares of three offshore companies and original articles of incorporation. The investigation revealed that one of the suspects used the services of a lawyer form Country B to design a money laundering scheme that included the incorporation of offshore companies with bearer shares. The lawyer hired the services of a management company in Country C, who in turn used the services of a company in Country A to incorporate bearer share companies in Country A.

There was no requirement to register the names of the shareholders at the corporate registry office, company head office or anywhere else. The only names that appeared were the original incorporators of the company in Country A, who then forwarded the bearer shares and articles of incorporation to the Country B management company. The management company then forwarded the original bearer shares and articles of incorporation to the lawyer, who in turn handed them over to his client. The files held by the management company only contained the names of the nominee directors, nominee administrators and the directions given by the Country B lawyer who acted on behalf of the suspect shareholder.

The use of bearer shares companies and professional intermediaries in this investigation almost offered absolute anonymity to the person in possession of the bearer shares and is clearly a powerful tool to conceal proceeds of crime. If investigators had not seized the bearer shares in the possession of the suspect, it would have been impossible to determine the owner of these companies and ultimately to identify and restrain their assets as proceeds of crime. In this case, the offshore companies held significant assets alleged to be the proceeds of crime, bank accounts in Country C, and residential property in Country B and Country D.

5. Emerging trends

Money laundering is an evolving activity, driven by the need for criminals to legitimise the proceeds of crime. Whilst national governments and supranational bodies continue to introduce further measures to prevent and combat money laundering, this serves to push criminals in to more sophisticated and complex ways to legitimise illegal assets, increasing the professionalism of the process, the use of various sectors of the financial system and of the economy, and the recourse to new geographical routes. Accordingly, although there is no single method of laundering money and no definitive list of typologies in relation to money laundering or terrorist financing, there is a need to identify emerging trends in ML/CFT techniques.

The early emphasis on cases studies and more recent focus on a thematic approach in examining typologies has helped to build up a significant expertise in the methods used for money laundering. This emphasis on the methods – the "how-to" – of money laundering and terrorist financing has however meant less emphasis on identifying new or potential ML/TF trends. While the importance of studying ML/TF methods and techniques cannot be overstated – such studies provide decision makers and operational experts with the material toward which to target policies and strategies for combating financial crime – the "how-to" of ML/TF is only part of the picture.

Understanding the evolution and prevalence over time of particular ML/TF methods — the current and emerging trends — provides the rest of the picture. T he study of known or perceived trends enables the development and refinement of indicators that law enforcement and supervisory authorities and especially the private sector can use to help detect specific ML/TF activity. Identifying trends ensures that, in the longer term, the relevant ML/TF methods are themselves examined in a systematic manner and understood and acted on with reference to their context. It is this extra context that also allows the identification of further links between apparently different ML/TF methods.

This section of the document identifies emerging themes and will be developed with the passage of time.

Emerging Trends in Alternative Remittance Systems

ARS operators are flexible and progressive in finding new, profitable and efficient methods of transmitting money. It is important to note that these services are being developed to respond to a particular consumer demand and for the most part have not been designed to circumvent existing AML/CFT measures.

For example, ARS and credit card companies are developing new products allowing debit cards to be bought for cash and then the value moved or paid out via automated teller machines (ATM) and purchases by anyone holding the personal identification number (PIN). This is an efficient way to move money securely and provides a flexible way for the money to be stored and retrieved. The card providers place limits on the value that can be stored in the cards, some of which can only be loaded with value once. AML measures are limited to the card purchaser.

In Africa bus companies with scheduled routes are in some cases furnishing remittance services. The drivers use cash received for tickets to pay out remittances. This gives the bus operators extra revenue and improves security for drivers who previously had to carry the cash proceeds of ticket sales. In other countries taxi firms operate similar systems, delivering money to customers' homes.

Mobile phone companies are using the ability of SIM cards to be loaded with value and have that value removed to use phones as a method of storing, exchanging and remitting value in countries with developing mobile phone infrastructure.

Internet-based Remittance Services

At least one Internet-based remittance agency – "IBR" – has been encountered by the authorities in Hong Kong, China. The IBR in question is based in the United States and uses the global Integrated Funds Transfer System (GIFTS). In conjunction with a major credit card service provider, it provides for the transfer of funds to any beneficiary worldwide through the issuance of an ATM card, and settlement for the transactions occurs by direct debiting of the nominated credit card of the remitter.

Remitters simply open an account with the web-based service provider. The service provider dispatches an ATM debit card to the nominated beneficiary in any one of 130 countries. The ATM debit card can be utilised at any ATM carrying the service of the major credit card or used to make purchases worldwide within seconds of being credited by the remitter.

The remitter simply enters a secure area of the IBR web site and authorises the transfer of funds to the beneficiary's account. The funds are then immediately available to the beneficiary anywhere in the world through the worldwide ATM network. IBR even allows for beneficiaries to request money from the remitter via the IBR website. The beneficiary simply completes a request message, and then the system automatically forwards an e-mail to the remitter requesting that he or she authorise the further remittance of funds.

The ATM cards used in this process are easily transferable thus allowing for greater anonymity than the more traditional use of supplementary credit cards. Regulators and investigators face great difficulty in monitoring such activities, and there is an obvious potential for misuse by criminals and terrorists.

For example, even in jurisdictions where regulated ARS exist, individuals in one jurisdiction can make remittances to a second jurisdiction without leaving easily traceable records that could be used by competent authorities. The only information available is credit card activity relating to the remitter in the sending country, which will only reflect payments to the web-based remittance agent. Checks on the beneficiary would then have to be routed through many agencies in a number of jurisdictions including the sending and receiving jurisdictions as well as the location in which Internet-based transfer service is located.

Appendix 1 : Excerpt from "An Island strategy to counter money laundering and the financing of terrorism"

Goal 2:

RAISE AWARENESS OF MONEY LAUNDERING AND TERRORIST FINANCING TYPOLOGIES THAT ARE RELEVANT TO JERSEY

Vulnerabilities:

Sections within a number of business sectors - in particular, smaller less well-resourced firms - are considered to have an inadequate awareness of the money laundering and terrorist financing risks inherent in: the services or products that they provide; the type of customer/client involved; how the service or product is delivered; and, where the service or product is delivered to.

Potentially, this heightens the risk that such businesses may be targeted by money launderers or terrorist financers and that businesses may not identify their involvement in money laundering or terrorist financing. This can hamper Island AML/CFT efforts.

Action points:

1. The Commission's AML Unit, with assistance from the JFCU and Customs, will produce and publish a booklet on typologies, for use as a training aid by Island businesses that are subject to the Money Laundering Order. The booklet will focus on those typologies that are most relevant to Jersey - as garnered from local prosecutions, intelligence, and co-operation with enquiries and requests from other jurisdictions. The booklet will highlight those typologies associated with the predicate crimes that the Island is considered especially vulnerable to, including: drug trafficking; fraud (including fiscal fraud); corruption; and insider dealing.

2. The Commission's AML Unit, in conjunction with the JFCU, will run a programme to raise awareness of risks that are faced by the finance sector, including:

   - meeting periodically with industry bodies;
   - assessing particular knowledge gaps though questionnaires; and
   - visiting the largest and highest risk businesses that have failed to make any, or a surprisingly low number of, SARs.

Measurement of effectiveness:

a) An increase in the number of SARs that are properly submitted by businesses in sectors which, historically, have submitted a disproportionately low number of reports.

b) The provision of additional typologies in the proposed booklet (post publication), reflecting greater awareness of risks that are inherent in the financial sector.