

Appendix A

Money Laundering Typologies

The following typologies have been drawn from the typologies reports published by the FATF during the period 1997–2003.

Introduction

The techniques used by money launderers are many and varied; they evolve to match the volume of funds to be laundered and the legislative/regulatory environment of the ‘market place’. The sophisticated money launderer is like water running downhill; both seek out the line of least resistance. Thus in a cash-based society that has lax legal and regulatory controls, little effort is needed to disguise the cash or its ownership; consequently the launderer will fund his/her lifestyle in cash or, where funds need to be transferred or surplus funds deposited or invested, the launderer will deal directly with the banks in order to abuse basic banking facilities.

Where cash is not the norm, and legal and regulatory controls are sound, greater effort will be required to disguise the source of criminal cash and other funds and also to disguise their beneficial ownership. In consequence, the launderer may seek to set up corporate structures and trusts (both onshore and offshore) and attempt to present an appearance of legitimate commercial or financial enterprise as a disguise. It is an added bonus if such structures can be set up in a jurisdiction that itself has lax legislation and regulation or strict confidentiality controls. Finally, it is important to recognise that the launderers’ techniques will evolve and change in line with the development of banking and other financial sector products and services.

This ‘dynamic’ view of the launderers’ techniques is confirmed by the regular typology exercises that have been carried out over several years by the FATF and in addition, more recently, by other international and regional bodies. The reports of such exercises are available both in hard copy and over the internet; they should be considered essential reading in order to keep up-to-date with emerging trends.

In broad terms, typologies/techniques tend to fall into a number of discrete groups:

1. Cash and Banking Services

Cash deposits, basic banking and money transmission services remain the core means of laundering criminal proceeds. The small-time launderer will seek the benefits of the basic savings, deposit and current accounts, and personal and mortgage type lending. The more wealthy launderer will, of course, seek the services of specialist banking facilities serving the needs of the ‘high net worth’ individual.

The typical mechanisms for using banking services are as follows:

Deposit structuring/smurfing

This technique entails making numerous deposits of small amounts below a reporting threshold, usually to a large number of accounts. The money is then frequently transferred to another account, often in another country. This method is widely used, even in countries which do not require cash transactions above certain thresholds to be reported. Countries to which these funds are transferred often find the funds being promptly removed as cash from the recipient accounts.

Connected accounts

Identification requirements tend to deter criminals from opening accounts in false names. However, this is often replaced by the use of accounts held in the names of relatives, associates or other persons operating on behalf of the criminal. Other methods commonly used to hide the beneficial owner of the property include the use of shell companies, almost always incorporated in another jurisdiction, and lawyers. These techniques are often combined with many layers of transactions and the use of multiple accounts – thus making any attempts to follow the audit trail more difficult.

Collection accounts

Collection accounts are a technique which is widely used by ethnic groups from Africa or Asia. Immigrants pay many small amounts into one account, and the money is then sent abroad. Often the foreign account receives payments from a number of apparently unconnected accounts in the source country. While this payment method is certainly used for legitimate purposes by working immigrants and labourers who send money to their home country, this fact has been recognised by criminal groups who use this method to launder their illegitimate wealth.

Payable through accounts

Payable through accounts are demand deposit accounts maintained at financial institutions by foreign banks or corporations. The foreign bank funnels all the deposits and cheques of its customers (usually individuals or businesses located outside the country) into one account that the foreign bank holds at the local bank. The foreign customers have signatory authority for the account as sub-account holders and can conduct normal international banking activities. Payable through accounts pose a challenge to 'know your customer' policies and suspicious activity reporting guidelines. It appears that many banks offering these types of accounts have been unable to verify or provide any information on many of the customers using these accounts, which poses significant money laundering threats.

Cash deposits and telegraphic transfer

Large cash deposits are often made by drug traffickers or others who have smuggled criminal funds out of the country where the crime originated. Often the cash deposit is quickly followed by a telegraphic transfer to another jurisdiction, thus lowering the risk of seizure.

Bank drafts, etc.

Bank drafts, money orders and cashiers' cheques, usually purchased for cash, are common instruments used for laundering purposes because they provide an instrument drawn on a respectable bank or other credit institution and break the money trail.

Loan back arrangements

Loan back arrangements are often used in conjunction with cash smuggling. By this technique, the launderer usually transfers the illegal proceeds to another country, and then deposits the proceeds as a security or guarantee for a bank loan, which is then sent back to the original country. This method not only gives the laundered money the appearance of a genuine loan, but often provides tax advantages.

Bureaux de change

Bureaux de change, exchange offices or casas de cambio offer a range of services which are attractive to criminals: (i) exchange services which can be used to buy or sell foreign currencies, as well as consolidating small denomination bank notes into larger ones; (ii) exchanging financial instruments such as travellers' cheques, euro cheques, money orders and personal cheques; and (iii) telegraphic transfer facilities. The criminal element continues to be attracted to bureaux de change because they are not as heavily regulated as traditional financial institutions or not regulated at all. Even when regulated, the bureaux often have inadequate education and internal control systems to guard against money laundering. This weakness is compounded by the fact that most of their customers are occasional, which makes it more difficult for them to 'know their customer', and thus makes them more vulnerable.

Remittance services

Remittance services (sometimes referred to as giro houses) have also proved to be widely used for money laundering, since they are often subject to fewer regulatory requirements than institutions such as banks which offer an equivalent service. They are also popular with many ethnic groups as they charge a lower commission rate than banks for transferring money to another country, and have a long history of being used to transfer money between countries. They operate in a variety of ways, but most commonly the business receives cash which it transfers through the banking system to another account held by an associated company in the foreign jurisdiction, where the money can be made

available to the ultimate recipient. Another technique commonly used by money remitters and currency exchanges is for the broker to make the funds available to the criminal organisation at the destination country in the local currency. The launderer/broker then sells the criminal funds to foreign businessmen desiring to make legitimate purchases of goods for export. This correspondent type operation resembles certain aspects of 'alternative remittance systems' (see Typology No. 2).

Credit and Debit Cards

Structured cash payments for outstanding credit card balances are the most common use of credit cards for money laundering, often with relatively large sums as payments and in some instances by cash payments from third parties. A large number of identified scenarios involve the use of lost or stolen cards by third parties. Another method is to use cash advances from credit card accounts to purchase cashier's cheques or to wire funds to foreign destinations. On some occasions, cash advances are deposited into savings or current accounts. It is intended that this typology will be examined as part of a future FATF typologies exercise.

2. Alternative Remittance Systems/Value Transfer Systems

Alternative remittance systems (also called underground or parallel banking, informal money or value transfer systems) are almost always associated with ethnic groups from Africa, China or Asia, and commonly involve the transfer of value between countries, but outside the legitimate banking system. The 'broker', which may be set up as a financial institution such as a remittance company, or may be an ordinary shop selling goods, has an arrangement with a correspondent business in another country. The two businesses have customers that want funds in the other country, and after taking their commission the two brokers will match the amounts wanted by their customers and balance their books by transferring an amount between them for the time period, e.g. once a month. The details of the customers who will receive the funds, which are usually minimal, are faxed between the brokers, and the customers obtain their funds from the broker at the end of the transaction.

Often there is no physical movement of currency and there is a lack of formality with regard to verification and record-keeping. The normal *modus operandi* is that money transfer takes place by coded information passed through chitties, couriers, letters or fax, followed by a telephone confirmation. Almost any document which carries an identifiable number can be used for the purpose. Because there is no recognisable audit trail the launderer's chance of remaining undetected or avoiding confiscation is significantly increased.

The systems are referred to by different names depending upon the community being served, e.g. *Hawala* (an Urdu word meaning reference), *Hundi* (a Hindi word meaning

trust), *Chiti* banking (referring to the way in which the system operates), *Chop Shop* banking (China) and *Poey Kuan* (Thailand).

There is evidence that terrorists use traditional methods of money transmission such as *Hawala* to move funds between jurisdictions. Such transactions often involve transfers from the UK through a third country, further obscuring the ultimate destination of the funds (see also *Typology No. 9 – Terrorist Financing*).

3. Investment Banking and the Securities Sector

At some stage of the laundering process, the successful launderer may wish to invest the proceeds. This investment may be by way of a stockbroker or a portfolio management service from an investment bank or directly with a securities house.

All types of securities, commodities, futures and options can be used as a means of money laundering. The wholesale market is attractive due to the ease and speed with which products can be purchased, sold, converted between currencies and transferred from one jurisdiction to another. A further attraction is the availability of bearer products and the large size of transaction. The high net worth individual or corporate launderer may not draw as much attention when washing large sums as they would in a more conventional banking operation.

Cash-based transactions

The use of cash within the securities sector is relatively rare and many market operators are generally restricted or prohibited from accepting cash. Consequently, the use of the securities sector for laundering purposes is primarily part of the layering and integration stages. However, from time to time cash can be introduced through the sector, particularly where brokers break rules to accept cash, often for increased commissions. Another way within some countries is to accept cash for use in margin trading. In an effort to turn a quick profit, settlement within the margin trading market is often left until the last minute and cash then becomes the popular means of settlement.

‘Pump and Dump’ schemes

Market manipulation through the artificial inflation of a stock based on misleading information (a ‘pump and dump’ scheme) is also used to generate fraudulent proceeds. 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 typical ‘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 criminal proceeds to purchase these large blocks of stock. The shares are usually obtained at an extremely low price, and after the perpetrators have accumulated large stock holdings in the company, they may utilise unscrupulous brokers to promote the securities to their clients.

Misleading information is released into the public domain to promote the company and its business operations although the company will often have no legitimate operations. In order to create the appearance of market demand, the perpetrators of the securities fraud may divide transactions among several brokers and/or channel transactions through multiple jurisdictions. When the shares reach a peak price, the perpetrators sell off their shareholding 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, firstly the launderer, by selling his/her stock in the company has layered the illicit funds they originally invested; and, secondly, as a perpetrator of a securities fraud, they have generated additional illicit proceeds that require laundering.

4. Insurance and Personal Investment Products

Life policies and other personal investment products, and general insurance are attractive to the launderer. Life policies and personal investment products can often be purchased with cash, especially through small intermediaries. A useful ploy for the launderer is to purchase with cash followed by early cancellation or surrender of the policy.

In many jurisdictions life insurance policies are viewed as another form of investment, and it is this investment aspect that increases the vulnerabilities of the products. Because the insurance sector within many jurisdictions tends to view itself as lower risk for money laundering, the insurance broker may often prove to be one of the weakest links in an anti-money laundering strategy.

General insurance policies can also be an attractive laundering technique: putting an expensive asset on cover, paying a large premium by bank transfer, followed by early cancellation of cover asking for the refund remittance to be made to another bank in another country.

5. Internet and Electronic Financial Services

The number of financial institutions providing financial services on the internet is growing considerably with an increasing range of services becoming available (savings/deposit accounts, full cheque accounts, electronic fund transfers, stockbroking, insurance, etc.).

Delivery of financial services over the internet has been, in essence, a development from banking services and stockbroking services delivered by telephone. The challenge to the service provider and the attraction to the launderer is the absence of face-to-face contact.

Technology has provided the opportunity for more credit and financial institutions to offer electronic money. This may be by way of a card-based electronic purse. While

the size/value of such 'purses' is restricted by regulatory requirement, the opportunity to purchase such electronic money for cash and then to use it to purchase assets, albeit modest, or obtain a refund by cheque, provides an opportunity for structured placement.

There are currently few case studies of money laundering through online financial services but whether this is due to a true lack of cases or the inability to detect such activity is not clear.

Companies trading and other business activities

Companies, partnerships and sole trader businesses are used as a cover for money laundering. Cash-based businesses provide a cover for cash deposits into a bank account and the payment of suppliers, both domestically and internationally, provides a ready excuse for transfers of all sizes. Criminals may also pay an inflated price for stock in order to obtain control of a company and then use the company to inject the criminal proceeds along with the legitimate earnings, or use legitimately earned company profits to fund further criminal activity.

International trade

International trade in goods and services can be used either as a cover for money laundering or as the laundering mechanism itself. Import/export activities and transactions are commonly used; a trader may pay a large sum of money (from the proceeds of illegal activity) for goods which are worthless and are subsequently thrown away or sold on cheaply. Alternatively, illegal proceeds can be used to buy high-value assets such as luxury cars, aeroplanes or boats which are then exported to narcotics-producing countries.

The launderer's priority is to make the transactions look normal. To achieve this the launderer will utilise all the normal trade finance services offered by the banks to legitimate import/export businesses.

Shell corporations

The shell corporation is a tool which appears to be widely used in both the banking and non-banking sectors. Often purchased 'off the shelf' from lawyers, accountants or secretarial companies, it remains a convenient vehicle to launder money. It conceals the identity of the beneficial owner of the funds, the company records are often more difficult for law enforcement to access because they are offshore or held by professionals who claim secrecy, and the professionals who run the company act on instructions remotely and anonymously. These companies are used at the placement stage to receive deposits of cash which are then often sent to another country or at the integration stage to purchase real estate. They have also been the vehicle for the actual predicate offence of bankruptcy fraud on many occasions.

6. The Gold and Diamond Markets

The gold market

Precious metals, and in particular, gold, offer the advantage of having a high intrinsic value in a relatively compact form. For some societies, gold carries an important cultural or religious significance that adds to the demand for the metal in certain regions of the world. The advantages that gold provides are also attractive to the money launderer, in particular its high intrinsic value, convertibility and potential anonymity in transfers. Most laundering schemes involving gold are linked to drugs trafficking, organised crime activities and illegal trade in merchandise and goods. The gold itself may be the proceeds of crime that needs to be laundered if, for example, it has been stolen or smuggled by creating a system of false invoicing.

Another more complex technique uses the gold or precious metal purchases and sales as a cover for the laundering operation.

The diamond market

Illegal trade in diamonds has become an important factor in armed conflict in certain areas of the world, and terrorist groups are believed to be using diamonds from these regions to finance their activities. The ease with which diamonds can be hidden and transported, and the very high value per gram for some stones, make diamonds particularly vulnerable to illegal diversion from the legitimate channels for the exploitation and profit of criminals. As with gold, the simplest typology involving diamonds consists of direct purchase of the diamonds with criminal proceeds. Other common typologies using diamond trading activity include retail foreign exchange transactions, the purchase of gaming chips at casinos, forged or fraudulent invoicing, and the commingling of legitimate and illicit proceeds in the accounts of diamond trading companies.

It is believed that between 5 and 10 per cent of diamonds produced annually in one particular region are lost due to theft or pilferage which then form part of the illicit diamond market. Some of the illicit diamonds are known to provide income to purchase illicit arms and consequently these diamonds have been termed 'blood' diamonds.

7. Lawyers, Accountants and Other Intermediaries

Lawyers and accountants can become involved in money laundering through their role in setting up corporate and trust structures and when acting as directors or trustees. In addition, the client account can provide the launderer with a totally hidden route into a bank account. In some jurisdictions legislation may forbid the bank being provided with information relating to the identity of the client and the source of funds. Lawyers, accountants and other financial advisers can also be a useful means of laundering money through the sale of personal investment products (see *Typology No. 3*).

8. Terrorist Financing

There are two primary sources of financing for terrorist activities. The first method involves obtaining financial support from states or structures with large enough organisations to be able to collect and then make the funds available to the terrorist organisation. It is believed that this so-called state-sponsored terrorism has declined in recent years and has been superseded by backing from other sources.

The second method of raising funds for terrorist organisations is to obtain them directly from various ‘revenue-generating’ activities. These activities may include criminal acts; in this way they may appear similar to ordinary criminal organisations. Unlike such organisations, however, terrorist groups may also derive a portion of their revenues from legitimately-earned income. How much of a role legal monies play in the support of terrorism seems to vary according to the terrorist group and whether its source of funds is in the same geographic location as its terrorist acts.

‘Legal’ sources of terrorist financing

The ideological rationale for some terrorist movements means that individual terrorists or terrorist groups may sometimes rely on legally-generated sources of income. As mentioned above, this is a key difference between terrorist groups and traditional criminal organisations. Some of the specific fundraising methods include:

- Collection of membership dues and or subscriptions;
- Sale of publications;
- Speaking tours, cultural and social events;
- Door-to-door solicitation within the community;
- Appeals to wealthy members of the community; and
- Donations of a portion of their personal earnings.

Donations

It is common practice within the Islamic community to donate a ‘zakat’, one tenth of one’s income, to charity. There should be no assumption that such donations bear a relation to terrorist funding. However, donations continue to be a lucrative source of funds from private individuals, rogue states and the sale of publications. Such donations are often made on an irregular basis. There is also growing evidence that large donations made by wealthy individuals in the Middle East to charitable organisations that have connections with terrorist organisations are more associated with Mafia-style protection payments. The donation ensures that the donor’s business interests remain untouched.

‘Illegal’ sources of terrorist financing

Criminality provides a much more consistent revenue stream. Terrorist organisations will choose activities that carry low risks and generate large returns. Major sources of income are:

- ***Kidnap and extortion***

This form of money raising continues to be one of the most prolific and highly profitable. Monies are usually raised from within the community of which the terrorists are an integral part. Eventually extortion becomes a built-in cost of running a business within the community and the payment of ransom demands to free family members becomes an everyday occurrence.

- ***Smuggling***

Smuggling across a border has become one of the most profitable ventures open to terrorist organisations. Smuggling requires a co-ordinated, organised structure, with a distribution network to sell the smuggled goods. It then offers high returns for low risks. Criminal partners will also benefit from their involvement, but there are considerable amounts made available for the terrorist organisation.

The profits can then be channelled via couriers to another jurisdiction. The money enters the banking system by the use of front companies or short-term shell companies that disappear after three months. Specialised bureaux de change may also be created, whose sole purpose is to facilitate the laundering of proceeds of the smuggling.

Another method of integrating the proceeds into the banking system has recently been detected. Monies are given by the smuggler to legitimate businesses who are not associated with the smuggling operation. These monies are then paid into the banking system as part of a company’s normal turnover. Provided the individuals are not greedy, detection is extremely difficult. Monies are then sent via different financial institutions and jurisdictions, including FATF blacklisted countries. The transfer of monies through different jurisdictions causes one of the principal problems of tracing the asset trail. Different legislative laws and procedures prevent quick and effective investigation. This only aids the criminal/terrorist enterprise rather than law enforcement.

- ***Fraud including credit card fraud***

Stockpiling of cheque-books for later misuse is a new variation on the theme of fraudulent misuse of accounts and credit cards.

- ***Misuse of non-profit organisations and charities fraud***

Non-profit organisations (NPOs) are established in a wide variety of legal forms and are subject to varying degrees of control by the jurisdictions in which they are located. Given their diversity, the FATF has adopted a definition of NPOs which is based on their function rather than on their legal form, i.e. ‘any legal entity that engages in the raising or disbursing of funds for charitable, religious, cultural, educational, social, fraternal or

humanitarian purposes, or for the purposes of carrying out some other types of good works’.

The potential misuse of NPOs by terrorist groups can take many forms. One possibility is the establishment of an NPO with a stated charitable purpose, but which actually exists only to channel funds to a terrorist organisation. Another possibility is that an NPO with a humanitarian or charitable purpose is infiltrated by the terrorists and their supporters, often without the knowledge of the donors or the members of staff or management. Still another possibility is for the organisation to serve as the intermediary or cover for the movement of funds, usually on an international basis. In some cases, the NPO support function could extend to the movement and logistical support of the terrorists themselves.

Reporting suggests that not all charitable or goodwill institutions are regulated to this extent. In particular, charities do not always publish full accounts of the projects which their fundraising has helped to finance.

There are known cases of charities being used to raise funds for terrorist purposes. One investigation arose as a consequence of a suspicious transaction report. A bank disclosed that an individual who allegedly was earning a salary of £12,000 per annum had a turnover in the account of £250,000. A financial investigation revealed that the individual did not exist and that the account, fraudulently obtained, was linked to a Middle East charity. A fraud was being perpetrated for the purpose of raising funds for a terrorist organisation. Donations were paid into an account and the additional charitable payment was being claimed back from the government. The donation was then returned to the donor. This fraud resulted in over £800,000 being fraudulently obtained.

- ***Drug trafficking***

Drugs can be a highly profitable source of funds and are used by some groups to finance other activities. Many terrorist groups are not directly involved in the importation or distribution of the drugs but exact a levy for the drug suppliers to operate within a certain area or community.

Such extortion, often known as protection money, is far less risky than being responsible for organising the supply and distribution of the drugs. The supply of controlled narcotic substances is a high priority for virtually all law enforcement agencies throughout the world and large resources are dedicated to investigation.

Laundering through the financial system

While terrorist groups may support themselves with funding from illicit sources and legitimate sources, there appears to be little difference in the methods used by terrorist groups or criminal organisations to launder their funds, i.e. to hide or obscure the link between the source of the funds and their eventual destinations or purpose.

Bank accounts have been used in the following ways to launder terrorist funds.

- ***Legitimate accounts***

It has been observed that individuals may run a number of accounts with several banks. It is not unusual for the accounts with one bank to be used for domestic purposes, while accounts based at another are for 'business purposes'. Into the former a salary or benefits may be paid, while the latter will benefit from money transfers and cheque payments. Substantial value to the investigation can be obtained from the audit trail associated with those money movements, particularly when linked to additional intelligence.

- ***Dormant accounts***

On occasions, dormant accounts are used by terrorists to establish a legend upon which additional frauds are perpetrated. Facilities can be accessed which include the obtaining of bank loans, the payments of which will invariably not be met.

Dormant accounts are also used to receive monies from support members abroad. Once again, the terrorist uses a number of banks, holding an account in each of them. Two of the accounts might contain a minimal sum, believed to be for two purposes: (a) in order to keep it open; and (b) to ensure that undue attention is not drawn to it. At a strategic time, a transfer is received into the account to enable the purchase of terrorist material. The sum is eroded by the daily removal of the maximum cash amount from automatic teller machines. This continues until the entire transfer sum has been removed, which might take several months. The location of such withdrawals can prove to be of great assistance to the investigation.

- ***Telegraphic transfers***

This can be effected by the use of banks or wire companies. Certain wire transfer companies appear to be used in preference to others. Enquiries to date suggest that those based in retail outlets containing video cameras are used to a much lesser extent than those where the wire transfer is franchised to a small, more localised unit. However, the use of these facilities is also determined by the ease of both sending and receiving the money. Indeed, certain companies do not even request documentation, requiring only the use of a pre-agreed question and answer prior to release of the transferred sum.

- ***Money service businesses and alternative remittance systems***

Given that many sources of terrorist funding (extortion and drug trafficking, for example) generate a high volume of cash, terrorists often channel funds through bureaux, money changers and other dealers in foreign currency to finance their operations abroad. Money may pass through several jurisdictions before reaching its final destination. UK firms that carry out such business under FSA or Customs supervision should be aware of the risks in this area. Use of the informal money or transfer value system e.g. *hawala*, *hundi*, *fei-chien* and the black market *peso* exchange have also been detected in relation to terrorist financing activity.

9. Correspondent Banking

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 having performed all the necessary due diligence and continuous monitoring of its own customers' account activity.

An additional risk incurred by the correspondent bank is that 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.

A further risk is the existence of sub-respondents through which a respondent bank may itself be offering correspondent banking facilities to other credit institutions. One FATF member stated that some banks offering correspondent facilities may not be asking their respondents about the extent to which the latter offers such facilities to other institutions. This oversight has meant in certain cases that the correspondent bank is even further removed from knowing the identities or business activities of these sub-respondents, or even the types of financial services they provide.

There are also increased difficulties in monitoring the individual transactions involved in large volume correspondent accounts since the bank is usually not in contact with the originator or the beneficiary of such transactions.

10. Corruption, PEPs and Private Banking

Examples of senior government officials involved in corruption and other types of proceeds generating crime are no longer rare occurrences. In the past few years several high-visibility corruption cases involving 'politically exposed persons' and the laundering of vast amounts of criminal proceeds through various FATF jurisdictions have been detected and investigated.

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 that the beneficial ownership remains hidden.