Guidance on the AML/CFT framework which applies to Financial Services Businesses and Prescribed Businesses

Guidance on the AML/CFT framework which applies to Financial Services Businesses and Prescribed Businesses

1. The Guernsey authorities are committed to ensuring that money launderers, terrorists, those financing terrorism and other criminals, cannot launder the proceeds of crime through Guernsey, or otherwise use Guernsey's finance sector. The Guernsey Financial Services Commission (the Commission) endorses the Financial Action Task Force on Money Laundering's (FATF's) Forty Recommendations on Money Laundering and the IX Special Recommendations on Terrorist Financing. The Commission also considers that the EU and its approach to regulation will grow in importance and influence and as a consequence, the Commission has concluded that it will be important for the Bailiwick to demonstrate equivalence with the EU's AML/CFT standards as well as the international AML/CFT standards of the FATF.

2. Recommendation 20 of the FATF's Recommendations requires that where a jurisdiction has identified "non-financial businesses" which are at risk of being misused for money laundering or terrorist financing that such businesses be bought into the AML/CFT framework of that jurisdiction.

3. The 3rd EU Money Laundering Directive applies to auditors, external accountants and tax advisors whether they are legal or natural persons acting in the exercise of their professional activities.

4. Currently, the Drug Trafficking (Bailiwick of Guernsey) Law, 2000, the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 and the Disclosure (Bailiwick of Guernsey) Law, 2007 applies to all firms and individuals within the Bailiwick. This legislation contains offences if firms and individuals do not make a disclosure to the Financial Intelligence Service (FIS), (Guernsey's Financial Intelligence Unit) where they have knowledge or suspicion of money laundering or terrorist financing or if they have reasonable grounds for knowing or suspecting money laundering or terrorist financing. Copies of the documents which must be used when making a disclosure of suspicion to the FIS can be found on its website at www.guernseyfis.org. Firms and their staff are legally protected from breaking any obligation of confidentiality when making disclosures to the FIS. The legislation also includes tipping off offences whereby it is an offence to disclose information or any other matter which is likely to prejudice an investigation by law enforcement.

5. The Commission is currently consulting on proposed changes to Schedules 1 and 2 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 ("1999 Law"), and Schedule 1 to the Registration of Non-Regulated Financial Services businesses (Bailiwick of Guernsey) Law, 2008 ("2008 Law").

6. The proposed changes to Schedule 1 to the 1999 Law and the 2008 Law will bring postage stamp dealers and bullion dealers, into the AML/CFT framework. Such businesses will be required to register with the Commission and comply with the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007 ("2007 Regulations") and the rules in the Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing.

7. These changes arise from threat and risk assessments presented to the Bailiwick of Guernsey AML/CFT Advisory Committee, on the risk of money laundering with regard to the use of postage stamps, there is concern about their potential nature as investment products and their portability because of their small size. In addition, the volume of bullion being transported across the Bailiwick's borders has raised concern about the money laundering risk to the Bailiwick arising from the buying and selling of bullion – the AML/CFT Advisory Committee has recommended the inclusion of stamp dealers and bullion dealers in Schedule 1 to the 1999 Law and Schedule 1 to the 2008 Law as a response to these concerns.

8. The proposed changes to Schedule 2 to the 1999 Law will bring firms of accountants which are currently not registered with the Commission and firms (including sole practitioners) of insolvency practitioners, auditors and tax advisers, into the AML/CFT framework. Such businesses will be required to register with the Commission and comply with the Criminal Justice (Proceeds of Crime) (Legal Professionals, Accountants and Estate Agents) (Bailiwick of Guernsey) Regulations 2008 ("2008 Regulations") and the rules in the Handbook for Legal Professionals, Accountants and Estate Agents on Countering Financial Crime and Terrorist Financing.

9. Sections 24-29 of Schedule 1 to the 1999 Law and Regulation 16 of the 2008 Regulations contain exemption provisions. Any business who meets all of the exemption provisions in the relevant section is not required to register with the Commission or comply with the Regulations and the rules in the Handbooks.

10. The Commission is conscious that the requirements of the regulations and the rules will appear to be rather complex and onerous, especially to firms which have not previously been subject to any form of AML/CFT regulation or supervision. In order to assist such firms, the following paragraphs provide a simplified overview of the requirements of the regulations and the rules in the Handbooks. However, whilst this information and guidance paper has been prepared to provide an overview, it is not intended to provide detailed guidance on the requirements of all the regulations and the rules.

11. Descriptions of money laundering and terrorist financing, together with some examples are attached in appendix 1.

A Risk-Based Approach

12. The main theme which runs through the Regulations and Handbooks is a risk-based approach. This allows each firm to have flexibility on managing and mitigating the risk of money laundering and terrorist financing, taking into account its size and the nature and complexity of its operations.

13. A risk-based approach serves to balance the cost burden placed on individual businesses and on their customers/clients with a realistic assessment of the threat of the business being used in connection with money laundering or terrorist financing. It focuses the effort where it is needed and has most impact.

14. To assist the overall objective to prevent the abuse of businesses, a risk-based approach:

- recognises that the ML/FT threat to a financial services/prescribed business varies across its customers/clients, countries/territories, products/services and delivery channels;

- allows the Board and senior management (i.e. those charged with the management of the financial services/prescribed business), to apply their own approach to the policies, procedures and controls of the business in particular circumstances and to differentiate between their customers/clients in a way that matches the risk in their particular business;

- promotes the prioritisation of effort and activity by reference to the likelihood of money laundering or terrorist financing taking place and helps to produce a more cost-effective system;

- reflects experience and proportionality through the tailoring of effort and activity to risk; and

- allows a business to apply ML/FT counter measures sensibly and to consider all relevant factors.

Corporate Governance and Compliance – Information

15. References to "the Board" in the 2007 and 2008 Regulations and the rules in the Handbooks should be read as meaning the senior management, (those charged with the management of the financial services/prescribed business where the business is not a company, but is, for example, a firm or partnership).

Corporate Governance and Compliance – Guidance

16. The Board has responsibility for compliance with the regulations and the rules. In particular it is the Board which is responsible for the policy on reviewing compliance, including the consideration of the appropriateness and effectiveness of compliance and the review of compliance at appropriate intervals.

17. Although the Board may wish to delegate some or all of its duties it retains responsibility for overall compliance with AML/CFT requirements.

Business Risk Assessment – Guidance

18. A risk-based approach starts with the identification and assessment of the risk that has to be managed and requires a business to assess the risks of how it might be involved in ML/FT taking into account its customers/clients, products and services and the ways in which it provides those services. The Board and senior management (i.e. those charged with the management of the financial services/prescribed business), are in the best position to evaluate all potential risks.

19. A business should ask itself what is the threat of it being used for money laundering or terrorist financing and consider what risk is posed/mitigated by its customers/clients, taking into account:

- their geographical origin (e.g. are customers/clients locally resident or are they based in a jurisdiction where drug trafficking, bribery and corruption are widely considered to be prevalent;

- the complexity of their legal and transaction structures;

- the way they were introduced to the financial services/prescribed business; and

- the unwillingness of customers/clients who are not individuals to give the names of their underlying owners and principals.

20. A business should also consider what risk is posed/mitigated by the products or services offered. Such as:

- whether the value of a transaction is particularly high; and

- whether payments to third parties are allowed.

21. Since 1999 the Commission has, from time to time, issued Business from Sensitive Sources Notices, Instructions, Advisory Notices and Warnings. These Instructions, Notices and Warnings highlight potential risks arising from particular sources of business and require special attention and a greater degree of caution to be exercised when taking on business from or undertaking transactions connected with the countries or territories specified in the Instructions, Notices and Warnings. By visiting the Commission's website on a regular basis a financial services/prescribed business will be able to apprise itself of the available information, and make itself aware of any potential risks and problems associated with taking on politically sensitive and other customers/clients from countries or territories where drug trafficking, bribery and corruption are widely considered to be prevalent.

22. Consideration of the risks identified in paragraphs 18 and 19, together with information such as that provided by the Commission in its Instructions and Business from Sensitive Sources Notices, will be a useful framework for the process whereby, having assessed the risk to its business, appropriate policies, procedures and controls on the countering of ML/FT can be considered and put in place.

Policies, Procedures and Controls – Information

23. An effective framework for countering ML/FT requires businesses to have a range of policies, procedures and controls in place relating to:

- risk assessment and mitigation

- undertaking customer/client due diligence (CDD);

- monitoring customer/client activity and ongoing CDD;

- reporting suspected money laundering and terrorist financing activity;

- staff screening and training;

- record keeping; and

- ensuring compliance with legislation and rules, corporate responsibility and related requirements.

CDD Procedures – Information

24. Paragraphs 18 to 22 deal with the risk to the business. There is also the risk of each individual customer/client to be considered. Sound CDD procedures are vital because they:

    - provide the basis for identifying, assessing, mitigating and managing risk;

    - help to protect the financial services/prescribed business by reducing the likelihood of it becoming a vehicle for, or a victim of, financial crime and terrorist financing;

    - help the financial services/prescribed business take comfort that the customers/clients and other parties included in a business relationship are who they say they are, and that it is appropriate to provide them with the product or service required; and

    - help the financial services/prescribed business understand the purpose and intended nature of the relationship and therefore to identify, during the course of a relationship, factors which are unusual and which may lead to knowing or suspecting or having reasonable grounds for knowing or suspecting that customers/clients or other parties may be carrying out ML/FT.

CDD Procedures – Guidance

25. Knowing your customer/client and understanding their intentions in respect of the proposed relationship will allow you to assess the level of CDD documentation and information required to adequately manage and mitigate any ML/FT risks.

26. Having customer/client take-on policies, procedures and controls in place which provide scope to identify and verify identity to a depth appropriate to the assessed risk of the business relationship will impose the least necessary burden on customers/clients and not constrain access to services. The general rules is that the full range of CDD measures as identified in Chapter 4 of the Handbooks, including the requirement to identify and verify the identity of the customer/client, beneficial owners and any underlying principals must be applied.

27. Nevertheless, there are circumstances where the risk of money laundering or terrorist financing has been assessed as being low (for example, a locally resident retail customer purchasing a low risk product where the purpose and intended nature of the business relationship or occasional transaction is clearly understood and where no aspect of the business relationship or occasional transaction is considered to carry a high risk of money laundering or terrorist financing), or where information is publicly

available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances a business may consider applying simplified or reduced CDD measures when identifying and verifying the identity of the customer/client, beneficial owners and underlying principals.

Politically Exposed Persons – Information

28. Additionally, and more importantly, appropriate and effective CDD procedures will ensure that any customers/clients who may be politically exposed persons (PEPs) (see the definition in appendix 2) will be identified and the risks of establishing relationships with such persons can be managed and mitigated.

29. In order to determine whether a customer/client or another party to the relationship is a PEP, internet websites such as Google or Yahoo are a useful tool. Additionally, the Handbooks provide links to other relevant websites and there are a number of available commercial databases.

Monitoring and Scrutiny of Transactions – Information

30. Understanding the purpose and intended nature of the relationship allows for the monitoring of business relationships and the application of scrutiny of unusual, complex or high risk transactions or activity so that ML/FT may be identified and prevented. An unusual transaction or activity may be in a form that is inconsistent with the expected pattern of activity within a particular business relationship, or with the normal business activities for the type of product or service that is being delivered.

Staff Training – Information

31. One of the most important tools available to assist in the prevention and detection of ML/FT is to have staff (including partners etc) who are alert to the potential risks and who are appropriately trained.

Staff Training – Guidance

32. Whilst there is no single or definitive way to conduct staff training for AML/CFT purposes, the critical requirement is that staff training is adequate and relevant to those being trained and the training messages should reflect good practice. The training should equip staff in respect of their responsibilities and cover:

- the CDD requirements and the requirements for the reporting of suspicion;
- the criminal and regulatory sanctions in place for failing to report information in accordance with policies, procedures and controls;
- the identity and responsibilities of the MLRO;
- the principal vulnerabilities of the products and services offered by the firm; and
- new developments, including information on current money laundering and terrorist financing techniques, methods, trends and typologies.

33. The guiding principle of all AML/CFT training should be to encourage employees, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the firm against the risk of money laundering and terrorist financing.

Record Keeping – Information

34. Record keeping is an essential component necessary to assist in any financial investigation and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated by the appropriate authorities.

Record Keeping – Guidance

35. Appropriate and effective policies, procedures and controls in respect of the keeping of records will require copies of documents to be kept in a readily retrievable form so as to be available on a timely basis and will include:

- identification and verification of identity documents and information which have been collected under the CDD procedures;
- customer/client files, account files, business correspondence and information relating to the business relationship;
- all suspicion reports; and
- training records.

36. CDD information and suspicion reports should be kept for a period of 5 years after the business relationship has ceased or from the completion date of a transaction where no relationship has been established (e.g. when a property has been purchased or sold). Transaction documents should be retained for 5 years from the date the transaction was completed.

APPENDIX 1 - MONEY LAUNDERING AND FINANCING OF TERRORISM TECHNIQUES

What is Money Laundering?

Deception is the heart of money laundering: at its most basic level money laundering is deception by attempting to make assets appear to have been obtained through legal means with legally-earned funds or to be owned by third parties who have no relationship to the true owner.

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. From the perspective of the criminal, it is no use making a profit from criminal activities if that profit cannot be put to use. A proportion of the profit will often be re-invested into further criminal ventures, but criminals will often wish to use the rest for other purposes. If this activity is to be achieved without being detected the money must be 'laundered'. Money laundering can be described as the processing of criminal proceeds to disguise their illegal origin. Criminals seek to put their proceeds of crime into a state in which it appears to have an entirely respectable origin. If this act is carried out successfully it allows criminals to maintain control over their proceeds and ultimately to provide a legitimate cover for their source of income. Where criminals are allowed to use the proceeds of crime, the ability to launder such proceeds makes crime more attractive.

However, this does not mean that all criminals need to resort to elaborate schemes in order to create the perception of legitimacy of the source and ownership of their assets. Small-time criminals rarely do; they deal in cash and avoid financial institutions as much as possible. Even with regard to larger criminal activities the need to launder money will vary from jurisdiction to jurisdiction.

The money laundering process is generally made up of three stages:

- The placement stage where illegitimate funds find their way into the financial system via payment into legitimate accounts. For example, depositing cash in banks which ask no questions, using business entities that are cash intensive in nature to commingle funds, buying precious metals/diamonds, or artwork/stamp collections;

- The layering stage which is used to disguise the audit trail between the funds and the original point of entry into the financial system. This is achieved by moving the funds around so that the origins of the money become obscured. For example, by transferring funds across borders, purchasing investment bonds, gambling at the race track or at casinos, and making use of foreign financial centres;

- The integration stage where funds are reintroduced as legitimate wealth to fund further activities or to acquire assets.

What is Financing of Terrorism?

For terrorists, the acquisition of funds is not an end in itself but a means of committing a terrorist attack. With terrorist financing, it does not matter whether the transmitted funds come from a legal or illegal source. Indeed, terrorist financing frequently involves funds that,

prior to being remitted, are unconnected to any illegal activity. Examples have occurred when legitimate funds have been donated to charities that, sometimes unknown to the donors, are actually fronts for terrorist organisations.

Tracking terrorist financial transactions arising from legitimate sources is more difficult than following the money trails of the proceeds of crime because of the often relatively small amount of funds required for terrorist actions and the range of legitimate sources and uses of funds. While many organised crime groups are adept at concealing their wealth and cash flows for long periods of time, their involvement in the physical trade of illicit drugs, arms, and other commodities, often exposes the revenues and expenditures connected to these illegal dealings. In contrast, terrorist attacks are in many cases comparatively inexpensive, and their financing is often overshadowed by the larger financial resources allocated for the group's political and social activities, making it more difficult to uncover the illicit nexus.

Identifying and disrupting the mechanisms through which terrorism is financed are key elements in the overall efforts to combat terrorism. As well as reducing the financial flows to terrorists and disrupting their activities, action to counter terrorist financing can provide vital information on terrorists and their networks, which in turn improves law enforcement agencies' ability to undertake successful investigations.

Red Flags

Precious metals, and in particular gold, offer the advantage of having a high intrinsic value in a relatively compact form. Gold can be bought and sold for currency with little difficulty in most areas of the world. Furthermore, it holds its value regardless of the form it takes – whether, for example, in bullion or as a finished piece of jewellery – it is thus often sought after as a way of facilitating the transfer of wealth. 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, that is, the high intrinsic value, convertibility, and potential anonymity in transfers. It is used both as a source of illegal funds to be laundered (through smuggling or illegal trade in gold) and as an actual vehicle for laundering (through the outright purchase of gold with illegal funds). Most laundering involving gold are linked to illegal narcotics trafficking, organised crime activities and illegal trade in goods and merchandise.

Case Studies

The following case studies demonstrate how financial products and services can be used to launder the proceeds of crime or to finance terrorism.

Money Laundering

Example 1: Retail gold purchases serves as direct method of money laundering

In the first and simplest case study, the money launderer or often someone acting on his behalf simply purchases gold from a retail merchant with funds that were generated directly by an illegal activity.

A foreign national used the services of a bureau de change to buy 265 ingots of gold with a total value of about USD 2,440,000, paid in cash. These transactions took place over a period of 18 months. The buyer, who did not have a bank account, alternated temporary jobs with periods of unemployment, suggesting that he was acting on behalf of a third party, whether a natural or legal person, who was probably involved in drug trafficking. The facts were forwarded to the prosecutor for investigation.

Example 2: Gold purchases facilitate money laundering

An asset management company was responsible for managing the bank portfolios of two individuals active in gold purchases in Africa. The purchased African gold was then sold to a gold working company in Country F, which in turn forwarded its payments to the accounts of the sellers. Debits were regularly made from these accounts to accounts in another European country. Desiring to verify the use of the funds, the asset management company requested its clients to provide a description of the channels used for making the payments for the gold in Africa. The information received permitted the company to identify an intermediary residing in Europe who was responsible for paying the suppliers in Country F. The individual in question was described as being closely associated with a corrupt regime in Africa.

Based on this information, the asset management company reported the case to the FIU and proceeded to block the accounts. Information exchanged with foreign counterparts permitted the linking of this illegal trade with an ongoing foreign investigation, which targeted the same individual for arms trafficking. The case was transmitted to the office of the public prosecutor which worked with the foreign authorities to dismantle these operations.

Example 3: Gold processing company used as a cover for money laundering

The money laundering organisation used a company processing and working gold to introduce cash from the sale of cannabis in Country R into the banking system of Country P. Moreover, the money launderers used a system that had been designed to make payments relating to cigarette smuggling and defraud Country P by applying for value added tax (VAT) refunds for non-existent operations.

The organisation had a person operating in Country R who collected bags full of sterling and other European currencies at restaurants and hotels near airports. The money came from the sale of cannabis in various European countries. The money was transported by air to Country P and declared in customs as payment for gold the company in Country P had sold to a company in Country R. The various currencies were paid into bank accounts in a city in Country P, certifying the origin of the money by means of the customs declaration completed at the border. These sales of gold by the company in Country P to the company in Country R were fictitious, although they were documented by false invoices. Subsequently the gold was supposedly sold to a company in a nearby offshore location, which issued a false letter of receipt.

The fictitious gold sales made it possible to transport money in cash from Country R to Country P where it was deposited in banks. Furthermore, it enabled the money launderers to apply for a refund on the VAT supposedly paid. In order for this mechanism to work the money launderers operated a gold working company which bought gold ingots from the largest metal wholesaler in Country P. Part of the gold was used to manufacture gold wire and shipped to Country F, where it was delivered to a finishing company that melted it back

down and sold it, paying by bank transfer to the same banks in Country P. Another portion of the gold sold by the company was diverted onto the black market where it was sold without VAT and therefore at an advantageous price for its buyers.

To complete the circuit, given that the initial gold purchase from the wholesaler had not been subject to VAT, the organisation set up a group of companies run by front men who issued false invoices for the sale of gold on which VAT was applied. The system used also enabled the organisation to change funds into the local currency and introduce them into the banking system. This money was used to pay transport costs and bribes relating to cigarette smuggling. The vehicles travelled through Country P but never reached their cities of destination in the neighbouring region.

Example 4 – Money laundering through temporary bank accounts

An investigation revealed that the proceeds of a value added tax evasion scheme were laundered through a series of bank accounts established for short term purposes. The launderer transferred the proceeds to a bank and requested that the funds be placed in an account for a short period because he had not decided in which account to place them. A few days later, he instructed the bank to return the money in cash or by cheque. The transaction was not registered in the books of the launderer. Investigators also discovered that the launderer used each bank account for more than one transaction. Afterwards, he sometimes asked the bank to transfer the funds to other accounts at the same bank or another bank, which had been opened on behalf of companies controlled by the launderer. False invoices for fictitious deliveries to these companies were used to justify the transfers.

Example 5 – A PEP launders his proceeds of corruption

A politician and government official in Country M arranged for his wife and children to receive the benefits of payments for infrastructure projects ranging from public swimming pools to power stations which he had supported on receipt of substantial payments.

Trusts and companies were established in a number of tax neutral countries for each of the family members.

A large proportion of the family's wealth – some of which was inherited – was administered by a bank in Country M. The bank had made introductions to the service providers in the tax neutral countries. In addition, the politician entered into business ventures in other jurisdictions, particularly Country L, a European country with a sophisticated finance sector. In all his transactions in foreign countries the politician portrayed himself as a businessman.

As a change in government in Country M became likely the politician asked the local bank to arrange for the administration of much of the family's portfolio to be moved to a bank in Country L. It was only when newspaper reports of the corrupt practices in Country M enabled the bank in Country L to make enquiries and to draw a link between the politician in Country M and the assets it administered that a disclosure report was made to the Financial Intelligence Unit (FIU).

Example 6 – Payments are structured via a money remitter to avoid detection

Over a four year period, Mr A and his uncle operated a money remittance service known as Company S and conducted their business as an agent of a larger money remitting business that was suspected of being used to finance terrorism. An investigation was initiated in relation to Company S based on a disclosure report.

The investigation showed that over the four year period, Mr A's business had received over US$4 million in cash from individuals wishing to transmit money to various countries. When Mr A's business received the cash from customers, it was deposited into multiple accounts at various branches of banks in Country G. In order to avoid the automatic financial reporting requirements in effect in Country G, Mr A and others always deposited the cash with the banks in sums of less than US$10,000, sometimes making multiple deposits of less than US$10,000 in a single day.

Mr A was charged and pleaded guilty to a conspiracy to structure currency transactions in order to evade financial reporting requirements.

Terrorist Financing

Example 1 – Terrorist use Gold to Move Value

During the invasion of Afghanistan in 2001, it was widely reported that the Taliban and members of al-Qaeda smuggled their money out of the country via Pakistan using couriers that handled bars of gold. In Karachi, couriers and hawala dealers transferred the money to the Gulf Region, where once again it was converted to gold bullion. It has been estimated that during one three-week period in late November to early December 2001, al-Qaeda transferred USD 10 million in cash and gold out of Afghanistan.

An al-Qaeda manual found by British forces in Afghanistan in December 2001 included not only chapters on how to build explosives and clean weapons, but on how to smuggle gold on small boats or conceal it on the body.

Gold is often used by hawala brokers to balance their books. Hawala dealers also routinely have gold, rather than currency, placed around the globe. Terrorists may store their assets in gold because its value is easy to determine and remains relatively consistent over time. There is always a market for gold given its cultural significance in many countries.

Example 2 – Auditor uncovers NPO being used for terrorist financing

Mr J is an auditor at accountancy firm ZZZ. For some years he has been responsible for the audit of the financial statements of firm b, a manufacturer of specialist hand tools for the oil and gas industries.

Firm B decides to seek advice on splitting its business into two separate companies under a holding company. It asks for help from the senior commercial adviser of firm ZZZ. The adviser feels that he must consider the accounts of firm b closely in order to provide the best commercial (including tax) advice. Close analysis of Mr J's papers and the account and other information provided by firm ZZZ, reveals the unusual timing of a series of large payments to a non-profit organisation (NPO) in a distant jurisdiction known to have civil strife, terrorist

activity and to be a centre of drug production. It is not clear why firm B is supporting the NPO. The adviser is informed that the manufacturer supports the NPO as it is based in a gas producing country and that the NPO supported the families of victims of an accident which had taken lace while representatives of the firm had been in the country. Upon investigation, the commercial adviser becomes suspicious that the payments made to the NPO are helping to fund the terrorist activity.

It transpired that several of the senior representatives of the firm were engaged in terrorist financing.

Example 3 – An individual's account activity and inclusion on an official list show possible link to terrorist activity

An individual residing in Country A had a demand deposit account and a savings account at a bank in Country B. The bank that maintained the accounts noticed the gradual withdrawal of funds from the accounts and decided to monitor the accounts more closely. The suspicions of the bank were subsequently reinforced when a name very similar to that of the account holder appeared in an official list of persons and/of entities suspected of involvement in terrorism. The bank immediately made a report to the FIU.

The FIU analysed the financial movements relating to the accounts of the individual using records requested from the bank. Both of the accounts had been opened by the individual in 1990 and had been fed mostly by cash deposits.

The individual made a sizeable transfer from his savings account to his demand deposit account. These funds were used to pay for a single premium life insurance policy and to purchase certificates of deposit. The individual made several more large transfers from his savings account to his demand deposit account. These funds were transferred abroad to persons and companies located in neighbouring countries and in other regions. The individual then sold the certificates of deposit and transferred the profits to the accounts of companies based in Asia and to that of a company established in his country of origin.

The FIU made enquiries internationally. The anti-money laundering unit in the individual's country of origin communicated information related to suspicious operations carried out by the individual and by the companies that received the transfers. This enabled the FIU to draw links between the individual, the companies and money laundering and terrorist financing.

Example 4 – Loans for hotels for individuals with suspected terrorist links revealed by a disclosure report

The FIU in Country D received a disclosure report from a domestic bank regarding an account held by an individual residing in a neighbouring country. The individual managed European-based companies and had filed two loan applications on their behalf with the reporting institution. These loan applications amounted to several million US dollars and were ostensibly intended for the purchase of luxury hotels in Country D. The bank did not grant any of the loans.

The analysis by the FIU revealed that the funds for the purchase of the hotels were to be channelled through the accounts of the companies represented by the individual. One of the companies making the purchase of these hotels would then have been taken over by an

individual from another country. This second person represented a group of enterprises whose activities focused on the hotel and leisure sectors, and he appeared to be the ultimate intended buyer of the hotels. On the basis of the analysis by the FIU, it appeared that the subject of the disclosure report was acting as a front for the ultimate intended buyer. The latter individual, as well as his family, were suspected of being linked to terrorism.

APPENDIX 2

"politically exposed person" means -

(i) a person who has, or has had at any time, a prominent public function or who has been elected or appointed to such a function in a country or territory other than the Bailiwick including, without limitation -

(A) heads of state or heads of government,

(B) senior politicians and other important officials of political parties,

(C) senior government officials,

(D) senior members of the judiciary,

(E) senior military officers, and

(F) senior executives of state owned body corporates,

(ii) an immediate family member of such a person including, without limitation, a spouse, partner, parent, child, sibling, parent-in-law or grandchild of such a person and in this subparagraph **"partner"** means a person who is considered by the law of the country or territory in which the relevant public function is held as being equivalent to a spouse, or

(iii) a close associate of such a person, including, without limitation -

(A) a person who is widely known to maintain a close business relationship with such a person, or

(B) a person who is in a position to conduct substantial financial transactions on behalf of such a person.