2004 (Revised 2007) GUIDANCE NOTES ON

THE DETECTION AND PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING ACTIVITIES

For Commercial Banks, Merchant Banks, Building Societies, Credit Unions, Cambios, Bureau de Change and Money Transfer and Remittance Agents and Agencies

Initial Re- Issue August 2004
1st Update February 2005
2nd Update March 2005
3rd Update June 2005
4th Update March 2007

TABLE OF CONTENTS

SECTION I - INTRODUCTION

OBJECTIVE

1. The objective of these Guidance Notes is to provide guidance to the financial institutions that are subject to the supervision of the Bank of Jamaica as regards the responsibilities of these institutions under the Money Laundering Act (MLA)[1], Money Laundering Regulations (MLR) and the Terrorism Prevention Act as well as outline the best practices in the areas of Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) techniques. Failure to comply with these Notes could expose the financial institution to prosecution under the Money Laundering Act or Regulations, or to prosecution under the Terrorism Prevention Act as well as to regulatory action by the Bank of Jamaica.

   These Guidance Notes last revised in June 2005, were originally issued to the industry in August 2004 subsequent to initial circulation in this form in January and April of 2004. They therefore replaced the ones previously issued in August 2000 and the very first ones issued in July 1995. A detailed schedule of the revisions made to the AML Guidance Notes since August 2000 is attached at Appendix VA.

APPLICABILITY OF THESE GUIDANCE NOTES

2. These Guidance Notes govern the anti-money laundering and combating the financing of terrorism activities of the following institutions which carry on activities within Jamaica:
   - commercial banks licensed under the Banking Act,
   - financial institutions (merchant banks) licensed under the Financial Institutions Act,
   - building societies licensed under the Building Societies Act,
   - cambios and bureaus de change licensed under the Bank of Jamaica Act and
   - money transfer and remittance agents and agencies[2] licensed under the BOJ Act,

[1] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA.

[2] As of January 15, 2002 Money Transfer and Remittance Agents and Agencies were designated financial institutions for the purposes of the Money Laundering Act by virtue of Ministerial Order. Further, on 12 February 2004, the BOJ Act was amended to formally establish the regulatory regime for money transfer and remittance agents and agencies and the requisite Operational Directions for these persons was issued on July 5, 2005. These entities now fall fully under the licensing and regulatory jurisdiction of the Bank of Jamaica.

- cooperative societies that operate as credit unions (to be licensed under the Bank of Jamaica (Credit Union) Regulations), as well as
- any other financial institution that falls under the jurisdiction of the Bank of Jamaica, and are collectively referred to herein as "Financial Institutions".

3. Financial institutions are required to advise their overseas branches/overseas subsidiaries of the provisions of the Jamaican AML/CFT laws together with the provisions of any applicable Guidance Notes insofar as the dealings of such subsidiaries or branches with the local institution will be affected by these laws and Guidance Notes.

4. Financial institutions are required to assess the AML/CFT regime existing in any jurisdiction in which its branches and/or subsidiaries operate and are required to ensure that branches apply the requirements of the Jamaican law, and that subsidiaries apply the requirements of Jamaican law, where the AML/CFT requirements in the jurisdiction in which they operate fall short of the requirements obtaining in Jamaica[3]. A failure to carry out this requirement may be considered to be a failure to manage group risks and will result in the Bank of Jamaica taking regulatory action, including where necessary sanctions against the institution, as provided by law.

5. Branches (where applicable) are considered not to be legally distinct from their head office and therefore are subject to Jamaican laws. A clear exception would be in cases where the branch operates in an overseas jurisdiction and is required to comply with the AML/CFT laws in that jurisdiction and these requirements meet or exceed the standards required by Jamaican laws.

5A. Foreign subsidiaries and foreign branches of local financial institutions must inform their local parent companies and local head offices if they are not in a position to observe appropriate AML/CFT measures where compliance therewith will contravene the laws of the overseas jurisdiction/(s) in which these subsidiaries reside. In such circumstances the local head office /parent company **must** accordingly advise the Bank of Jamaica which will then make a determination on the required course of

[3] See FATF Recommendation 22

action which may also include the regulatory requirement of closure of the relevant overseas branch or subsidiary.

LEGAL STATUS OF THESE GUIDANCE NOTES

6. It should be noted that, under Regulation 3(3) of the Money Laundering Regulations, 1998 (MLR)[4], **a court will give consideration to the supervisory or regulatory guidance issued by the Competent Authority which has jurisdiction over an entity which is charged with an offence under that Regulation.** It should also be noted that section 18(4) of the Terrorism Prevention Act requires entities to consult with the Competent Authority for the purpose of carrying out its obligations to establish regulatory controls to enable them to fulfil their counter-financing of terrorism duties. **In the Bank's view, a court would have regard to these Guidance Notes to determine the appropriateness of the AML and CFT[5] measures adopted by the financial institution. The Attorney General's Chambers has also issued an opinion on the importance and effect of this clause which confirms that MLR 3(3) makes compliance with these Guidance Notes compulsory**.

7. The Bank of Jamaica (which is also the Competent Authority[6] for the financial institutions named in these Guidance Notes for the purposes of the MLA) will also consider an institution's breach of its statutory obligations under the Money Laundering Act (MLA) the Regulations there-under, and the Terrorism Prevention Act, and non-adherence to these Guidance Notes to constitute unsafe or unsound practices for the purposes of Section 25(1) of the Banking and Financial Institutions Acts and the BOJ (Building Societies) Regulations Part D of the First Schedule Paragraph 2 and the related Regulation 68 (See also footnote 3 below).

8. Additionally, recent amendments to the financial legislation include, among other things, express provision that non-compliance with the Money Laundering Act[7], the Regulations thereunder, the Terrorism Prevention Act and any other statute which imposes obligations on financial institutions could result in the suspension or

[4] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA.
[5] Regulations under the TPA are being developed.
[6] Ministerial designation of the BOJ as the competent authority under the TPA is being prepared and will shortly be brought into effect.
[7] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA.

revocation of that financial institution's licence.[8] All financial institutions should be aware that the Bank of Jamaica's on site examinations will continue to include an assessment of the institutions' AML/CFT systems. Deficiencies in the systems, which place the institution in breach of its obligations under the governing statute(s) will render the entity subject to regulatory sanctions and will be reported to the Designated Authority. In the case of Money Transfer and Remittance Agents and Agencies, non-compliance with their statutory AML obligations and their AML/CFT obligations hereunder will render such persons liable to regulatory action by the Bank of Jamaica[9].

9. The law to address terrorism and terrorist financing activities is in effect.[10]. This therefore means that any transactions performed for terrorists or terrorist related persons or purposes, or facilitated by any financial institution for terrorists or terrorist related persons or purposes, constitutes an offence under the Terrorism Prevention Act for which stringent penalties are applicable.

10. Similar powers to take regulatory action for AML/CFT breaches will also be incorporated into the regulatory laws covering credit unions when these come into effect. Additionally, credit unions should be aware that their level of compliance with the Anti-Money Laundering and Anti-Terrorism laws and these Guidance Notes will form a part of the review and assessment process for licence applications when the licensing regime for credit unions is commenced.

11. Financial Institutions are therefore required to take all necessary steps to ensure full compliance, and should also note that revisions have been effected to the laws which allow for the imposition of more stringent regulatory sanctions, including the suspension and/or revocation of licences, for non-compliance. (See paragraph 8). **The Bank of Jamaica will be obliged, in any case where it discovers a breach of any**

[8] See the Banking Amendment Act, 2004 Clause 4(a)(iii)
See the Financial Institutions Act, 2004 Clause 4(a)(iii)
See the BOJ (Building Societies) Regulations, 2004 First Schedule Part D Paragraph 2(b)(iii)

[9] See the BOJ Operating Directions for Money Transfer and Remittance Agents and Agencies (direction 9.2). The move to regulate money remitters is informed by FATF Recommendation 23 which requires that countries ensure that financial institutions are fully and effectively regulated.

[10] The Terrorism Prevention Act was passed in April 2005 and the Appointed Day Notice for this Act signed by the Minister in June 2005, gazetted and has been fully in force since then.

laws to which these Guidance Notes relate, to make a report to the Designated Authority for the appropriate action, including prosecution.

These Guidance Notes will be reviewed periodically and amended as deemed necessary, to ensure their continued usefulness, efficacy, relevance and adherence to international best practice standards.

SECTION II - BACKGROUND

MONEY LAUNDERING

12. The term 'money laundering' refers to all procedures, methods, and transactions designed to change the identity of illegally obtained money so that it appears to have originated from a legitimate source.

13. It is recognized that cash lends anonymity to, and is therefore the normal medium of exchange for many forms of criminal activities, in particular, drug and arms trafficking as well as criminal activities involving fraud, dishonesty and corruption. The extent and impact of these criminal activities globally have required countries to make concerted efforts to defend their institutions, financial systems, economies and citizens by criminalizing the proceeds of these crimes. Thus, in the context of these Guidance Notes money laundering refers to the criminalizing of the proceeds[11] from the commission of any offence under the Dangerous Drugs Act, or the Firearms Act or any offence involving fraud, dishonesty or corruption.

14. One of the most critical features of any AML regime is the protection of the financial system. Thus apart from ensuring that they do not commit the offence of money-laundering, financial institutions are placed under further statutory obligations to ensure that they take active, effective and ongoing steps to prevent and detect money laundering[12].

TERRORIST FINANCING

15. Terrorist financing refers to the accommodating or facilitating of financial transactions that may be directly or indirectly related to terrorists, terrorist activities and/ or terrorist organizations. Once the financial institution knows or suspects or should reasonably suspect that an individual/group is associated with any terrorist activity or group, a financial institution (in carrying out a transaction for or with that individual/group), may be considered to be facilitating terrorist activity whether or not

[11] See FATF Recommendation 1.
[12] See MLA s. 7

the institution knows the specific nature of the activity facilitated, or whether any terrorist activity was actually carried out. (Refer to Section IV – "Know Your Customer Policy").

16. Financial institutions should also be aware, that business relationships with terrorists and terrorist organizations (as referred to in Paragraph (15) above) can expose the entity to significant legal, operational and reputation risks. These risks increase exponentially if the person or organization involved is later shown to have benefited from a lack of effective monitoring or wilful blindness of the financial institution, and thus was able to carry out, support or facilitate acts of terrorism.

17. Any financial institution that carries out transactions, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organizations, or that the transaction is directly or indirectly linked to, or likely to be used in, terrorist activity, may be committing a criminal offence under the laws of many jurisdictions and such an offence in many instances may exist regardless of whether the assets involved in the transaction were the proceeds of the criminal activity or were derived from lawful activity but intended for use in support of terrorism. Additionally, some states have included in their legislation provisions intended to extend their local criminal jurisdiction beyond state borders. This is grounded on the premise that a person who commits a terrorist offence in a jurisdiction other than his own jurisdiction, can in fact be prosecuted by the local jurisdiction for the commission of a terrorism offence, so long as such offence if committed in the local jurisdiction would have been a terrorism offence.

The United Nations Resolution 1373 and the Financial Action Task Force's (FATF) Special Recommendations on CFT require that states must have the ability to provide mutual assistance to each other whether through the exchange of information, or facilitating the freezing and forfeiture of assets used to aid the commission of a terrorist offence in another jurisdiction. In Jamaica the Mutual Assistance (Criminal Matters) Act of 1995 and The Sharing of Forfeited Property Act of 1999 permit Jamaica to extend assistance to other countries that are in the process of prosecuting, or enforcing judgments or forfeiture proceedings for drug offences and revenue offences. The Authorities have indicated an intention to amend these Acts to permit

and extend their application to terrorist offences. It is also intended that the Extradition Act will be amended to extend its application to terrorist offences.

Similar provisions have been included in the Terrorism Prevention Act. The Terrorism Prevention Act also provides that for the purpose of conferring jurisdiction, any offence committed outside of Jamaica will be deemed to have been committed in Jamaica where the offender may be domiciled for the time being, if such offence, when committed in Jamaica, would have been a terrorism offence.

18. The detection of funds linked to terrorist activities may be very difficult owing to the fact that terrorists or terrorist organizations often obtain financial support from legal sources. Other factors contributing to the difficulty of detection may also be the size and nature of transactions as these can be non-complex and in very small amounts.

19. A key issue for financial institutions therefore is for them to be able to identify any unusual and/or suspicious transaction that merits additional scrutiny and to record and report such transactions accordingly. In this regard, financial institutions should pay particular attention to: -

i. The nature of the transaction itself;
ii. The parties involved in the transaction; and
iii. The pattern of transactions or activities on an account over time.

Appendix I, which provides examples of suspicious transactions that could be evidence of money laundering and/ or terrorist financing has been further expanded to include certain elements of varying transactions which could indicate that the funds involved relate directly or indirectly to money laundering or terrorist financing. The list is not exhaustive and entities should be alert to evolving money laundering and/or terrorist financing techniques, patterns and typologies.

SECTION III - LEGISLATIVE AND REGULATORY FRAMEWORK

{The following summaries do not constitute a legal interpretation of the sections of the Acts or Regulations referred to, and appropriate legal advice must be sought thereon}.

GOVERNING LEGISLATION

The Money Laundering Act, 1996 ("MLA")[13]

20. The main features of this Act are as follows:

(i) **Section 3** of the MLA, creates an offence where a person: -

(a) engages in a transaction[14] that involves property which is derived from the commission of a specified offence[15] ; or

(b) acquires, possesses, uses, conceals, disguises, disposes of, brings into Jamaica, any such property; or

(c) converts or transfers that property or removes it from Jamaica,

if that person knows at the time of the transaction referred to at (a) or at the time he does any of the acts referred to at (b) or (c), that the property is derived or realized directly or indirectly from the commission of a specified offence.

(ii) **Section 5** makes it an offence if a person conspires with another to commit, aid, abet, counsel, or procure the commission of an offence under Section 3.

(iii) **Section 6** further requires a financial institution to report all cash transactions involving the "prescribed amount" (which has been set at the Jamaican or other currency equivalent of **US$50,000.00**)[16], to the Designated Authority. By virtue of the Money Laundering (Designated Authority) Order, 2003 under the MLA the Designated Authority is now the Chief Technical Director of the Financial Investigations Division of the Ministry of Finance and Planning for the purposes of the MLA. In the case of Cambios, the owners and managers

[13] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA
[14] "Transaction" includes receiving or making a gift.
[15] Specified offences are as listed in the Schedule of the Money Laundering Act
[16] The new limit proposed under the pending amendments to the AML framework is US$15,000.00.

are under an obligation to report transactions amounting to and exceeding **US$8,000.00**[17] or its equivalent in Jamaican or other currency to the Designated Authority. Cash transaction reporting requirements are not applicable to cash transactions carried out by a Ministry, Department of Government, statutory body or authority; a company in which the Government or an agency of Government is in a position to influence the policy of the company; an Embassy, High Commission, consular office or organization to which the Diplomatic Immunities and Privileges Act apply or any organization in relation to which an order is made under Section 3(2) of the Technical Assistance (Immunities and Privileges) Act.

(iv) **Section 6A** allows the Minister to grant exemptions from the threshold reporting requirement, to financial institutions which apply for such exemption, in relation to established customers (defined as customers with whom the institution has done business for at least 12 months). The Minister may also exempt a specific transaction or series of transactions. Such Ministerial exemptions would be considered in circumstances where:

(a) the transaction or series of transactions involve the deposit into or withdrawal of monies held by such an established customer from an account in a financial institution;

(b) the customer carries on: -

(1) a retail business, not including the sale of motor vehicles, vessels, farm machinery or aircraft; or

(2) a business declared by the Minister by order to be an entertainment business or a hospitality business for the purposes of this Act;

(c) the account through which the transactions are conducted is maintained for the purpose of such business; and critically,

(d) the amount of money involved is not over and above an amount that is reasonably commensurate to the lawful activities of the customer.

[17] The proposed amendments to the AML framework include a proposed threshold reporting limit for remittance companies of US$5,000 or the equivalent thereof in any other currency.

(v) **Section 6B** stipulates that a financial institution is under **a duty to pay special attention, to all complex, unusual or large transactions, or unusual patterns of transactions, which appear inconsistent with the normal transactions of a particular customer.** This section further creates a duty on the part of the financial institution to report to the Designated Authority **on its own initiative**, **or in response to a request made to it by the Designated Authority**, **any transaction that the institution has reasonable cause to suspect involves property obtained from the commission of a specified offence**.

(vi) **Section 6C** further makes it an offence to disclose information relating to actions or proposed actions of the Designated Authority relating to money-laundering, unless such disclosure is made to an attorney-at-law for the purpose of obtaining legal advice, facilitating the investigation, or any proceedings which might be conducted following the investigation. The penalty for breach of this section is imprisonment for two years or a fine of not more than J$2 million or both.

(vii) **Section 8** relates to the power of the Designated Authority to apply to a Judge in Chambers for a Monitoring Order[18]. This order directs a financial institution to give to a Constable named by the Designated Authority in the application, information and such documents as the Designated Authority may specify in the application, other than items subject to legal privilege[19]. A financial institution that is notified of a monitoring order and knowingly

[18] Section 8 of the MLA refers to a monitoring order as an order directing a financial institution to give such information and documents as the DPP requires in his application for this order. The order requires a financial institution to produce documents and/or information obtained by or that are under the control of the financial institution about transactions conducted through accounts held by a particular person with the financial institution.

[19] Legal privilege according to (Gilbert Law Summaries Dictionary of Legal Terms), is a person's privilege to refuse to disclose and to prevent others from disclosing anything said in confidence to that person's Attorney. Legal privilege applies to –

(i) matters that come within the ordinary scope of professional employment of an attorney and which are received in the attorney's professional capacity, either from a client or on the client's account, and for the client's benefit in the transaction of the client's business; or

(ii) communications from the client received by the attorney in the course of employment with the client and which relate to matters which the attorney becomes aware only through the professional relationship with the client. (See The Queen v. Cox and Railton – (1884) QBD 153 C.A..

contravenes the order, or provides false or misleading information or documents in purported compliance with the order, is guilty of an offence and is liable on summary conviction in a Resident Magistrate's Court to a fine not exceeding J$1mn. In these circumstances, the financial institution is under a duty not to disclose the existence or operation of the monitoring order to any other person except an officer of the institution for the purpose of compliance with the order, or an attorney-at-law for the purpose of obtaining advice or representation. Licensees experiencing some difficulty reconciling this aspect of the law with the regulator's entitlement to full access of their records should note that the situation at this point is that under the MLA the above obligation stands. However under the financial legislation governing financial institutions' operations the regulator may have access to the records including those indicating the existence of a monitoring order and the customer to whom it relates. The regulator however will not insist on taking copies of records of this nature, but will only exercise the access to the records sufficient to satisfy the regulator that a licensee is complying with its statutory obligations under the MLA.

The Money Laundering Regulations, 1998 ("MLR")[20]

21. These Regulations outline the operational procedures that must be maintained by financial institutions particularly when contemplating the commencement of a business relationship or one-off transaction. The MLR require financial institutions to establish and maintain appropriate procedures in relation to **identification**, **record-keeping (minimum 5 years retention period)**, **internal controls**, **communication**, and **training of employees**. These Guidance Notes outline in detail the requirements of the Supervisory Authority in fulfilling the requirements of the Regulations.

[20] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA

The Terrorism Prevention Act, 2005 ("TPA")

22A The Act outlines the following as financing offences:-

(i) Directly or indirectly, wilfully and without lawful justification or excuse collecting property, providing or inviting a person to provide, or make available property or other related services, -

(a) intending that they be used, or knowing that they will be used in whole or in part -

1. for the purpose of facilitating or carrying out terrorist activity;
2. for the benefit of any entity known to be committing or facilitating any terrorist activity;

(b) knowing, that in whole or in part, they will be used by or will benefit a terrorist group. **(section 4)**

(ii) Facilitating or carrying out a terrorist activity by-

(a) using property directly or indirectly, in whole or in part; or

(b) possessing property intending that it be so used or knowing that it will be so used directly or indirectly in whole or in part.
(section 5)

(iii) (a) Dealing directly or indirectly in or with any property that is owned or controlled by or on behalf of a terrorist group;

(b) Entering into or facilitating, directly or indirectly, any transaction in respect of property owned or controlled by or on behalf of a terrorist group;

(c) Providing any financial or other related services in respect of that property for the benefit of or at the direction of a terrorist group;

(d) Converting any such property or taking any steps to conceal or disguise the fact that the property is owned or controlled by or on behalf of a terrorist group. **(Section 6)**

22B. The TPA states that a person who commits any of these offences is liable on conviction in the case of an individual, to life imprisonment, and in the case of a body corporate, to a fine.

22C. The TPA also requires that: -

- Financial institutions determine on a continuous basis whether they are in possession or control of property owned or controlled by or on behalf of a listed entity. A listed entity is one which the Designated Authority has reasonable grounds to believe has knowingly committed or participated in the commission of a terrorism offence; or is knowingly acting on behalf of, at the direction of or in association with such an entity; **(section 15)**

- Financial institutions report all suspicious transactions to the Designated Authority[21], which is stated to be the Director of Public Prosecutions (DPP) or such other person as the Minister may designate by Order. In March 2006, the Minister designated the Chief Technical Director (CTD) of the Financial Investigations Division (FID) as the Designated Authority; **(section 15)**

- Financial institutions should ensure that high standards of employee integrity are maintained, and that employees are trained on a continuous basis regarding their responsibilities under the Act; **(section 18)**

- Financial institutions should establish and implement programmes, policies, procedures and controls for enabling them to fulfil their duties under the Terrorism Prevention Act. Towards this end, financial

[21] Section 16 of the TPA speaks to the DPP being the Designated Authority or the Minister's designate. In March 2006 the Minister designated the CTD of the FID the Designated Authority for the purposes of reporting obligations and other specific obligations outlined at sections 15-18 of the TPA.

institutions must designate a compliance officer at management level and arrange for independent audits to ensure that their compliance programmes are effectively implemented. **(section 18)**

22D. The TPA states that a person who commits any of these offences at sections 15, 16 or 18 of the Act) is liable on conviction in the case of an individual, to a fine not exceeding J$1 million dollars, and in the case of a body corporate, to a fine not exceeding J3$ million dollars.

22E. **Section 17** makes it an offence to disclose information relating to actions or proposed actions of the Designated Authority relating to an investigation being conducted or about to be conducted in relation to a terrorism offence, unless such disclosure is made to an attorney-at-law for the purpose of obtaining legal advice, facilitating the investigation, or any proceedings which might be conducted following the investigation. The TPA states that a person who breaches this section is liable on conviction to imprisonment for a term not exceeding two years and/or a fine of not more than J$2 million or both in the case of an individual and in the case of a body corporate, to a fine not exceeding J6$million dollars.

22. F. **Section 19** relates to the power of the Designated Authority to apply to a Judge in Chambers for a Monitoring Order[22]. This order directs a financial institution to give to a Constable named by the Designated Authority in the application, information and such documents as the Designated Authority may specify in the application other than items subject to legal privilege. A financial institution that is notified of a monitoring order and knowingly contravenes the order, or provides false or misleading information or documents in purported compliance with the order, is guilty of an offence and is liable on summary conviction in a Resident Magistrate's Court to a fine not exceeding J$1million in the case of an individual, and in the case of a body corporate, to a fine not exceeding J$3 million.

[22] Section 8 of the MLA refers to a monitoring order as an order directing a financial institution to give such information and documents as the DPP requires in his application for this order. The order requires a financial institution to produce documents and/or information obtained by or that are under the control of the financial institution about transactions conducted through accounts held by a particular person with the financial institution.

22. G. The TPA also defines 'terrorism offence' and 'terrorist activity' to include conspiracies, or attempting to commit, aiding, abetting, procuring or counselling activities. (See definition of terrorist offence and terrorist activities – **section 2**)

22. H. **Regulations Under the Terrorism Prevention Act (TPA)**

Section 47 of the TPA allows for Regulations to be made for giving effect to the provisions of this Act. Regulations under the TPA are subject to Affirmative Resolution. The Terrorism Prevention (Reporting Entities) Regulations are being drafted. Under these Regulations, Reporting Entities, include the financial institutions to which these Guidance Notes apply. These Regulations will outline the operational procedures that must be maintained by financial institutions particularly when contemplating the commencement of a business relationship or one-off transaction. As such these regulations will therefore largely mirror the MLR and will therefore require financial institutions to establish and maintain appropriate procedures in relation to identification, record-keeping (minimum 5 years retention period), internal controls, communication, and training of employees. These Regulations will also prescribe the requisite Declaration Forms for transactions which the reporting entity knows or suspects is one that constitutes a terrorism offence; and for the quarterly reports as to whether or not the reporting entity is holding property etc. in respect of a listed entity.

TRANSITIONAL GUIDANCE

In the interim however, where an institution finds itself in the position where circumstances exist that require a report to be made under the TPA, that is to say:

- the institution is in possession of property for a listed entity; or
- the institution is in possession of property for a person included on the UN consolidated listing of individuals and entities pertaining to Al-Qaida pursuant to United Nations Counter-Terrorism Security Council Resolution 1267 (1999) – Afghanistan; or
- the institution is of the view that a transaction conducted or being conducted or about to be conducted constitutes a transaction of the kind described at section 16 of the TPA (ie. unusual, complex etc.),

the institution should proceed to obtain expert legal advice as to the extent of its possible liabilities or exposure and as to the available courses of action to effectively minimize this risk and where it is determined that this can be done without legal

repercussions, the institution should consider making the necessary reports to the Designated Authority[23] in writing and in a form as similar as possible to the reporting formats currently used for reports made under the MLA.

22. I. **SPECIFIC GUIDANCE REGARDING TREATMENT OF LISTED ENTITIES**

Prior to the passage of the TPA, financial institutions have been required to determine whether they were in possession of property for persons on the U.N. lists of terrorists or persons linked with terrorists. The Guidance provided by the Bank of Jamaica was for the institution to flag such accounts where these were in the names of persons included on the above referred U.N. lists, and to obtain expert legal advice as to the extent of their possible liabilities or exposure and as to the available courses of action to effectively minimize this risk. Where it is determined that this could be done without legal repercussions, the institution should consider reporting the matter to both the Bank of Jamaica and the Financial Investigations Division (FID). Now that the TPA is passed and until the Regulations thereunder come into effect, then the method of proceeding in the circumstances described at paragraph 22H above ("Transitional Guidance") will remain the same, **with the additional requirement that institutions do not facilitate or offer any financial services to such persons.** The TPA states that unless a financial institution is acting in accordance with the direction of the Designated Authority, the institution will be committing an offence under either section 4, 5, or 6 of the TPA and will be charged and prosecuted accordingly.

Institutions should note that once a person has been designated a 'listed entity", the fact of this designation will be published by the DPP in a daily newspaper in circulation in the Island. (See section 14(5) of the TPA)

22I(A). In the following cases where financial institutions find that they are in possession of property for: -

(i) persons affiliated with listed entities; (i.e. the customer is a director, or shareholder of a company that is connected with the listed entity.

[23] By virtue of Ministerial Order dated March 2006 the designated authority under the Act was amended from the DPP to the Chief Technical Director of the FID.

{Connected/affiliated in this case has the same meaning as defined in the BA and FIA} or the customer includes the listed entity as one of its trading partners; customers; investors; consultants; etc.)

(ii) persons for which the names are very similar to those appearing on the list of listed entities (i.e. constituting a 97% match – in the case of individuals Christian/first names and Surnames match but Middle names are different; Full names match but the customer is female whereas the person on the listed entity list is identified as male – in the case of incorporated/unincorporated entities the names are sufficiently similar to consider that entity a related entity; or the name constitutes the English version of the name on the listed entity list);

(iii) persons whose business documentation reflect that commercial activities are conducted in territories that are generally featured as "generators or producers of terrorists"; or "sympathetic to terrorists" as indicated in official advisories from the U.N.; FATF; Ministry of Foreign Affairs and Foreign Trade; Designated Authorities (viz AML/CFT typologies); or the Competent Authority;

It is likely that the view might be formed that transactions/accounts with such persons may not be at the stage of being regarded as suspicious but do in fact raise questions. These accounts or transactions should be flagged for closer scrutiny and enhanced due diligence checks. For example if scenario (ii) circumstances should exist, the institution should consider taking steps to ascertain date of birth information; customer gender and possibly have the customer come in to the bank with a view to updating the KYC information on file. Scenario (iii) circumstances may require the institution to link with a sister agency such as the bankers association within the jurisdiction from which the documentation originated with a view to ascertaining guidance on how checks can be done to satisfy the institution of the bona fides of the documentation. Where the business relationship is continued or the transaction is conducted, the account or transaction should be subject to **full KYC banking standards and additionally reported to the Designated Authority without delay**. (See also paragraph 92B)

22.I. (B) Because of the severe implications that can arise from a financial institution being viewed as one that is holding property or providing financial services to a terrorist or a person so affiliated, (i.e. prosecution; loss of correspondent banking relationships; reputation risk, etc.,) it is imperative that reports made to the Designated Authority by the institution regarding 'listed entities' should be followed up preferably by specifically assigned senior officers (i.e. the compliance officer himself/herself or his/her highly ranked designate such that at anytime an institution is called on, it is in a position to provide more information than merely that "the matter was reported to the Designated Authority". The institution should be able to show from its records that the account or transaction was followed up and continuously analyzed and the point at which a determination was made to:

- close the account;
- end the business relationship;
- terminate the transaction;
- scale down services;
- refuse to undertake transactions above or under a certain amount;
- refuse to undertake new business with the customer;
- refuse to accept introduced business from that customer

Steps of this nature must also be clearly evident from the institution's records, as they will be indicative of a financial institution vigorously acting to protect itself and the integrity of the overall system. Such steps may ultimately be the determining factor in whether an institution is viewed as "complicit in its dealings with the customer; and whether it is negligent or is recklessly aiding and abetting the customer/(s) in question. **In complying with their obligations under the TPA in this regard, financial institutions should consult closely with their respective legal advisors.**

The Drug Offences (Forfeiture of Proceeds) Act,[24] 1994 (DOFPA)

23. **Section 3** of the DOFPA provides for the forfeiture of the property of persons convicted for contravention of the Dangerous Drugs Act and the Money Laundering Act. Forfeiture will take place where the property is derived from activities, which are

[24] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the DOFPA.

illegal under these statutes. The DOFPA also provides for the levying of pecuniary penalties on convicted parties.

24. **Sections 20, 28 and 38** grant powers to the Designated Authority[25] as well as the Police to obtain search warrants, restraint orders and production orders respectively. Additionally, provision is made for the payment to the Crown by a person convicted under the provisions of the DOFPA, of an amount, which is equal to the value of the benefit received from the activities found to be in contravention of these Acts (Section 14).

25. **Sections 46 and 47** require a financial institution to retain all records and documents pertaining to all transactions carried out by it, for a minimum period of five (5) years.

26. **Section 44** empowers the Designated Authority to apply for and serve a monitoring order on a financial institution, and to direct the disclosure of information concerning the **transactions** of a customer. In these circumstances, the financial institution is under a duty not to disclose the existence or operation of the monitoring order to any other person **except an officer of the institution for the purpose of compliance with the order, or an attorney-at-law for the purpose of obtaining advice or representation**. Licensees experiencing some difficulty reconciling this aspect of the law with the regulator's entitlement to full access of their records should note that the situation at this point is that under the MLA the above obligation stands. However under the financial legislation governing financial institutions' operations the regulator may have access to the records including those indicating the existence of a monitoring order and the customer to whom it relates. The regulator however will not insist on taking copies of records of this nature, but will only exercise the access to the records sufficient to satisfy the regulator that a licensee is complying with its statutory obligations under the DOFPA.

[25] The Designated Authority under the MLA is the FID. The Designated Authority under the DOFPRA is the DPP.

The Dangerous Drugs Act, 1948

27. This Act makes it a criminal offence for any person to import, export, cultivate, manufacture, use, sell, transport or otherwise deal in opium, ganja, cocaine, morphine, or any derivatives thereof.

The Firearms Act, 1967

28. This Act deals with the regulation and licensing of the sale, purchase, acquisition, ownership and other dealings with regard to firearms.

Offences Relating to Fraud, Dishonesty, and Corruption

29. There are several statutes relating to these offences. Some examples are the Larceny Act, the Corruption Prevention Act, and certain offences under the Companies Act.

INTERNATIONAL REGULATORY REQUIREMENTS

30. In October 2001, the Basel Committee on Banking Supervision issued Customer Due Diligence best practice standards ("CDD") as the minimum standards to be adopted by banking institutions in all countries. These standards have the full endorsement of the Jamaican Supervisory Authority and are attached as Appendix II.

31. The United Nations (U.N.) International Convention for the Suppression of the Financing of Terrorism 1999 established three main obligations for member states of the United Nations as follows:-

- First, states must establish the offence of the financing of terrorist acts in their national legislation;

- Second, states must engage in wide-ranging cooperation with other states and provide them with legal assistance in the matters covered by the Convention; and

- Third, states must enact certain requirements concerning the role of financial institutions in the detection and reporting of evidence of the financing of terrorist acts.

Jamaica became a signatory to the U.N. International Convention for the Suppression of the Financing of Terrorism 1999 on November 10, 2000. On September 16, 2005 Jamaica deposited with the U.N., instruments of accession to /ratification of this Convention.

U.N. Resolution 1373 (2001) on threats to international peace and security caused by terrorist acts, also mandates all member states of the United Nations to take action against individuals, groups, organizations and their assets. As a consequence of the United Nation's characterization of acts of terrorism as threats to international peace and security, the United Nations is entitled to take, if necessary, the collective measures ("sanctions") under Chapter VII of the United Nations Charter. [26] **To this end the Ministry of Foreign Affairs and Foreign Trade receives from time to time, an updated listing of individuals and entities which the UN has added to its consolidated list pertaining to Al-Qaida pursuant to United Nations Counter-Terrorism Security Council Resolution 1267 (1999) – Afghanistan. This listing once provided to the Bank of Jamaica has been forwarded to all BOJ regulated institutions for the necessary and comprehensive checks to be made to ascertain whether the books and records of the institutions reflect evidence of any accounts or transactions in the names of or on behalf of the listed individuals or entities, and for the necessary action to be taken as outlined in paragraph 22(I) of these Guidance Notes. However, once the reporting formats under the "listed entity regime" have been finalized and brought into effect by the Regulations under the TPA, then it is likely that this process will subsumed under the listed entity regime and all such lists circulated by the UN will be forwarded to the DPP for the purpose of being addressed pursuant to the listed entity regime. Licensees may, notwithstanding the foregoing, wish to apprise themselves directly from the United Nations web site and in that case may take note that the complete list and updates may be regularly accessed through the United Nations website as below:**

[26] Suppressing the Financing of Terrorism – A Handbook for Legislative Drafting Chapter on U.N. Security Council Resolutions on Terrorism Financing - Page 15 – (Prepared by the IMF)

URL:http://www.un.org/docs/sc/committees/1267/1267listeng.htm

31A. The Jamaican authorities are also guided by the Forty Plus Nine[27] Recommendations of the Financial Action Task Force (FATF) on the Detection and Prevention of Money Laundering and Terrorist Financing and the Nineteen Recommendations of the Caribbean Financial Action Task Force (CFATF). The ninth special recommendation speaks to the matter of 'Cash Couriers' and their increasing prominence in money laundering and terrorist financing activities. Special Recommendation 9 therefore requires countries to have in place measures to detect the physical cross-border movement of funds, and the requisite enforcement powers for the restraint and eventual confiscation of currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or in respect of which false declarations are made.

These Recommendations (FATF and CFATF) set out the internationally and regionally accepted principles relating to the appropriate measures to combat money-laundering and terrorist financing. Appendices III and IV respectively set out the provisions of these Recommendations.

Although not falling within the ambit of international best practice, financial institutions should also be aware of the USA Patriot Act (see paragraph 33), as well as the USA Foreign Narcotics Designation Kingpin Act and Regulations (Drug Kingpin Act) (see paragraph 33B), both of which can exert a direct and adverse impact on their correspondent banking operations and their holding of assets overseas.

32. In conjunction with these Guidance Notes, financial institutions should be guided by the above standards, principles and recommendations in establishing policies, programs and procedures to prevent and detect money laundering and in combating the financing of terrorist activities.

[27] The FATF 40 + 8 Recommendations were increased to FATF 40+9 Recommendations in October 2004.

33. Statutes Which May Impact Licensees Doing Business in the USA

33A. The USA Patriot Act. The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001" - the Patriot Act - was passed by the US Congress in direct response to the September 11 terrorist attacks and became effective on 26 October 2001. This legislation has, among other things, expanded the money laundering laws of the United States and has placed more stringent procedural requirements on financial institutions. Of specific importance to Jamaican financial institutions is the additional authority that has been vested in the US Secretary of the Treasury to regulate the activities of US financial institutions and in particular their relations with foreign individuals and entities. All banks and other financial institutions operating in Jamaica that have established correspondent accounts or any other business relationship with banks in the USA should therefore be aware of the provisions of this Act, including those highlighted below: -

- Provisions which permit the US Authorities to forfeit funds held by foreign banks in correspondent accounts held with banks situated in the USA. (S. 319)[28]

- Provisions that will allow the US authorities to seize correspondent accounts held in US financial institutions for foreign banks which are in turn holding forfeitable assets. (s. 317 and s. 319)[29]
- Provisions prohibiting US financial institutions from establishing, maintaining and administering or managing correspondent accounts with foreign banks that have no physical presence in any jurisdiction (i.e. shell banks), with certain limited exceptions; (s. 313)[30]
- Provisions requiring US financial institutions to take "reasonable steps" to ensure that accounts for foreign financial institutions are not used to indirectly provide banking services to shell banks; (s. 313)[31]

[28] Reference taken from "Current Developments in Monetary and Financial Law – Chp. 19, pages 349-352.

[29] Reference taken from "Current Developments in Monetary and Financial Law – Cap 19 – pages 349-352.

[30] Same as above

[31] Same as above

- Provisions which grant the Treasury and the US Attorney General power to issue a subpoena or summons to any foreign financial institutions with a correspondent account in the US and to request records relating to the account. A financial institution that has a correspondent account for a foreign financial institution must maintain certain delineated records in the US relating to that foreign financial institution; (s. 319 (b))[32]
- Provisions which grant the Treasury and the US Attorney General power to direct a financial institution to terminate its relationship with a foreign correspondent financial institution that has failed to comply with a subpoena or summons. The directive must be by written notice and non-complying financial institutions are subject to civil penalties of up to US$10,000 per day; (s. 319 (b))[33]

33B. **The USA Drug Kingpin Act** [34]

The Foreign Narcotics Designation Kingpin Act and Regulations - Drug Kingpin Act – The purpose of the Kingpin Act is to deny significant foreign narcotics traffickers, their related businesses, and their operatives, access to the U.S. financial system and all trade and transactions involving U.S. companies and individuals. The Kingpin Act authorizes the President to take these actions when he determines that a foreign narcotics trafficker presents a threat to the national security, foreign policy, or economy of the United States.

The Kingpin Act requires that the Departments of Treasury, Justice, State, and Defense, and the Central Intelligence Agency, coordinate on the identification of proposed kingpins for designation by the President. Although not required by statute, the Department of Homeland Security also is included in the process. By June 1 each year, the Act calls for the President to report to specified congressional committees those "foreign persons [he] determines are appropriate for sanctions" and stating his intent to impose sanctions upon those foreign persons pursuant to the Act. While this

[32] Same as above
[33] Reference taken from "Current Developments in Monetary and Financial Law – Cap 19 – pages 349-352.

[34] This update on the Drug Kingpin Act is taken from White House Press Release Office of the Press Secretary - June 1, 2004 - **Fact Sheet: Overview of the Foreign Narcotics Kingpin Designation Act**

is a recurring annual requirement, the President may designate significant foreign narcotics traffickers at any time.

Under the Kingpin Act, the President may designate foreign entities as well as foreign individuals as kingpins. A foreign person is defined as "any citizen or national of a foreign state or any entity not organized under the laws of the United States, but does not include a foreign state."

The long-term effectiveness of the Kingpin Act is enhanced by the Department of the Treasury's authority (in consultation with appropriate government agencies and departments) to make derivative designations of foreign individuals and entities providing specified types of support or assistance to designated traffickers. This authority broadens the scope of application of the economic sanctions against designated kingpins to include their businesses and operatives. To date, the President has announced 48 Kingpins and the Department of the Treasury has announced a total of 66 derivative designations, 14 entities and 52 individuals, pursuant to section 805(b) of the Kingpin Act. These entities and individuals are subject to the same sanctions that apply to kingpins. In addition, designated individuals and immediate family members who have knowingly benefited from the designated individuals' illicit activity will be denied visas to the United States under 8 U.S.C. section 1182(a)(2)(C).

The Kingpin Act provides for criminal penalties of up to 10 years imprisonment for individuals and up to a US$10 million fine for violations, as well as a maximum of 30 years imprisonment and/or a US$5 million fine for officers, directors or agents of entities who knowingly participate in violations. The Kingpin Act also provides for civil penalties of up to US$1 million.

Designations - A complete list of individuals and entities designated can be found at:

http://www.treasury.gov/offices/enforcement/ofac/

USA Economic Sanctions Programmes[35]

As of March 2004, the Office of Foreign Assets Control of the US Department of the Treasury OFAC[36] administered and enforced comprehensive sanctions programs involving four countries: Cuba, Iran, Libya, and Sudan. Unless authorized by OFAC, no U.S. person or company can do business with individuals, companies, or government institutions in those countries, or persons or entities acting for or on behalf of those countries. OFAC also enforced sanctions regimes regarding the following: the Western Balkans, Burma (Myanmar), diamond trading, Iraq, narcotics trafficking, North Korea, the proliferation of weapons of mass destruction, terrorism, and Zimbabwe. To read about the specifics of each sanctions program, please visit: www.treas.gov/ofac.

Specially Designated Nationals (SDN) and Blocked Persons[37]

OFAC has identified and officially "designated" numerous foreign agents and front organizations, as well as terrorists, terrorist organizations, and narcotics traffickers, on its SDN list, which contains over 5,000 variations on names of individuals, governmental entities, companies, and merchant vessels located around the world.

All U.S. persons (including individuals and organizations) are responsible for ensuring that they do not undertake a business dealing with an individual or entity on the SDN list. U.S. persons
are:

- All U.S. citizens and permanent residents,

- All persons located in the United States,

[35] The update on the US Economic Sanctions Programmes is taken from the Foreign Assets Control Regulations For The Credit Reporting Industry at the following web site address- http://**www**.ustreas.gov/offices/enforcement/ofac/regulations/credit.txt

[36] "OFAC administers and enforces economic and trade sanctions based on US foreign policy and US national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific (US) legislation, to impose controls on transactions and freeze foreign assets under US jurisdiction" (Source - US Department of The Treasury web-site)

[37] The update on the US Economic Sanctions Programmes is taken from the Foreign Assets Control Regulations For The Credit Reporting Industry at the following web site address- http://**www**.ustreas.gov/offices/enforcement/ofac/regulations/credit.txt

- Overseas branches of U.S. companies, and

- In the case of the Cuba and North Korea programs, non-U.S. subsidiaries of U.S. companies.

Penalties for Non-compliance

Depending on the program involved, criminal violations of the statutes administered by OFAC can result in penalties ranging from US$50,000 to US$10,000,000 and/or up to 30 years imprisonment for wilful violations. OFAC also has authority to impose civil penalties of up to USUS$1,075,000 per violation depending on the sanctions program.

DOMESTIC REGULATORY REQUIREMENTS

34. The domestic legal requirements outlined above at paragraphs 20 - 29 clearly indicate that financial institutions must establish and implement programmes, policies, procedures and controls for the purpose of preventing and detecting money laundering [38]and terrorist financing[39] activities.

35. Financial institutions are placed under a legal and regulatory obligation not to facilitate money laundering and terrorist financing activities. Arising from this obligation, there must be full awareness of: -

(i) the nature of the money-laundering and terrorist financing threats;

(ii) the local laws relating to money-laundering, particularly the potential liability of institutions and employees for failure to comply fully;

(iii) the local standards/principles established to prevent and detect terrorist financing activities as well as related international standards, protocols, laws and regulations (e.g. the FATF 40+9, UN Resolution 1373 and the USA Patriot Act and the Foreign Narcotics Kingpin Designation Act);

(iv) the requisite systems for customer identification and verification, including special procedures for non-face to face transactions, high risk customers,

[38] See MLA section 7 and MLR regulation 3
[39] See TPA section 18

'Politically Exposed Persons' (PEPs), and transactions with overseas counterparts;

(v) the requisite systems for the recording and reporting of unusual and suspicious transactions and transactions that exceed the statutory thresholds; including the role of the compliance officer;

(vi) the requisite programmes for ensuring employee integrity and awareness through effective screening and due diligence prior to hiring and continued relevant training post hiring, and continued screening of employees post hiring (viz. job performance; adherence to internal policies and procedures including codes of conduct and AML/CFT requirements).

36. Each financial institution must establish clearly defined policies and operational procedures in regard to the matters itemized at (i) to (vi) above, which must be properly documented in the form of a manual for distribution among all relevant staff. The management of the financial institution should review this manual at least on an annual basis and make appropriate revisions and enhancements when necessary. The Board should **review and ratify** the manual and all subsequent revisions and the overall effectiveness of the company's AML/CFT systems including those of its subsidiaries and branches whether located in Jamaica or overseas.

37. The policies and programmes contained in this manual must at a minimum, include the following:

(i) the establishment of procedures to ensure high standards of integrity for employees at all levels including senior and executive management levels;

(ii) the development of a system to evaluate the personal employment history and financial history of all employees at all levels including senior and executive management levels. Financial institutions are expected to establish specific procedures for such evaluation at the point of hiring, although ongoing evaluation would also be expected throughout the period of employment;

(iii) the establishment of programmes for the training of employees on a continuing basis, and for instructing all employees as to their responsibilities in respect of the law, regulatory guidance and 'best practice' standards;

(iv) the establishment of comprehensive customer due diligence policies and procedures, incorporating adequate customer acceptance policies and a multi-

tiered customer identification programme that involves more extensive and rigorous due diligence for high risk customers/accounts, as well as transactions with non face-to-face and overseas customers and counter-parties;

(v) designation of an officer of the institution at the management level to be the institution's Compliance Officer, responsible for ensuring the effective implementation of the policies, programmes, procedures and controls including the reporting of threshold and suspicious transactions to the appropriate authorities;

(vi) full co-operation and consultation with the relevant authorities, primarily the Designated Authority and the Competent Authority, for the purpose of carrying out the institution's obligations under law and best practice standards;

(vii) procedures for analysis of clients' transactions to ascertain trends and to recognize indicators of unusual and/or suspicious activity over time, e.g. multiple small transactions aggregating to a specified limit in a month, or annually;

(viii) arrangements for regular and timely internal and external audit reviews in order to ensure that there is adherence to the documented policy;

(ix) provision for the heightened scrutiny of certain categories of customers and types of transactions when necessary, as well as the continuous review of existing practices and procedures in this area as part of the general internal/external audit and control processes.

38. The procedures must include methods for:

(i) customer identification and verification **prior** to the commencement of business relationships and on an ongoing basis thereafter, using reliable independent source documents, data or information;

(ii) documenting and maintaining records of transactions;

(iii) recognizing suspicious transactions and recording these as well as threshold transactions, with appropriate channels for reporting;

(iv) ensuring compliance with relevant legislation, and co-operation with enforcement authorities;

(v) internal audit checks to ensure compliance with policies and procedures relating to money laundering and terrorist financing;

(vi) the training of staff in the operation and implementation of procedures and controls relating to money laundering and terrorist financing and their obligations under the law;

(vii) communication of group policies and procedures on the detection and prevention of money laundering and terrorist financing, and the monitoring of compliance by all subsidiaries and branches whether located in Jamaica or overseas.

39. Financial institutions are required to adopt a consolidated approach to the establishment and implementation of policies and procedures, which would cover the activities of all local and foreign branches, subsidiaries[40] and other entities within the group, that fall under the MLA and the TPA.

[40] See FATF Recommendation 22

SECTION IV - "KNOW YOUR CUSTOMER" (KYC) POLICIES AND PROCEDURES

SECTION IV. A. – GUIDANCE FOR COMMERCIAL BANKS, MERCHANT BANKS, BUILDING SOCIETIES AND CREDIT UNIONS

Introduction

40. Central to an effective anti-money laundering and anti-terrorist financing programme is the formulation and implementation of comprehensive, rigorous and thorough customer due diligence or "Know-Your-Customer" polices and procedures. **KYC policies and procedures should however, not only be geared toward the timely prevention and detection of money laundering and terrorism financing activities, but must also form a fundamental part of the licensee's overall risk management and internal control systems**. This is essential, as inadequate KYC standards can result in undue risk exposures, particularly as they relate to reputational, operational, legal and concentration risks.

41. The following section is intended to inform financial institutions as to general areas that have been determined by the Supervisory Authority as forming a critical part of each institution's overall KYC policies and procedures. The provisions indicated here are not exhaustive, and are not intended to be all encompassing.

42. With regards to all customers and for effective risk management, financial institutions should administer and monitor their customer due diligence processes on a consolidated and global basis, where applicable.[41] This will require, inter alia, the capacity to aggregate and monitor significant balances and transactions for the under-mentioned customers.

(i) Customers with multiple accounts/transactions at the entity - either within a particular branch or among several branches situated within the local and foreign jurisdiction; and

(ii) Customers with multiple accounts/transactions at several entities

[41] Operationally, this may only be possible in a fully regulated group or for financial institutions falling under the MLA, down to its subsidiaries.

within the financial group.

This is required whether the accounts are held on balance sheet, or off-balance sheet as assets under management, [42] or on a fiduciary basis.

43. **KYC policies and procedures must contain a clear statement of management's overall expectations and establish specific lines of responsibilities not only at the point of the institution's first contact with the customer, but throughout the business relationship. Policies and procedures should be properly documented and clearly communicated to all relevant staff.**

44. At a minimum, KYC policies and procedures should address: -

- Processes that must be followed to ensure proper identification of customers (including parties who may have a beneficial interest in the transaction or account) and those that may be acting on their behalf **prior to** the commencement of the business relationship, and the appropriate documentation requirements to satisfactorily establish a customer's identity and to verify the information received in this regard;
- Processes for the identification and verification of the nature and purpose of a customer's business in order for the financial institution to have a basis for determining whether a transaction is unusual or suspicious, or fits the norm expected of such a business;
- Procedures for the recording and regular review of customer identification and transaction information/records to ensure that the information is current and comprehensive[43], as well as the retention of such information for a minimum of five years after the transaction was initiated/attempted or had actually taken place, or the business relationship has been terminated;
- Procedures clearly indicating the application of KYC due diligence which take account of the level of risk posed to the institution by transacting business with the particular customer; (i.e. individuals opening standard savings accounts obviously funded primarily by salary; pension payments etc. vis-à-vis

[42] Reference herein to assets under management is only to the extent that deposit taking institutions have their own assets under proprietary management Otherwise, asset management on behalf of customers is not an activity that can legally be undertaken by deposit-taking institutions.
[43] See also MLR Regulation 8

corporate accounts opened via pooled arrangements involving multiple parties or accounts opened for PEPs and other high risk customers.)

- Measures to deal with special areas of operations such as high risk clients (i.e. correspondent banking, counter-parties/clients residing in countries with inadequate anti-money laundering and anti-terrorism financing measures, as well as making assessments of any person or legal entity connected with a financial transaction that could pose reputational or other risks to the financial institution).

General Requirements for Customer Due Diligence[44]

45. A business relationship or one-off transaction must not be established or continued until the identity of the customer is satisfactorily determined[45]. Where a potential customer refuses to produce any requested information, the relationship **must not** commence or the transaction **should not** proceed. Any business relationship that has already commenced should be legally terminated (unless otherwise advised by law enforcement authorities) if the customer fails to provide requested follow-up information or if any other verification problems arise which cannot be resolved. (See also paragraph 106 for additional guidance in this regard). In seeking to terminate the relationship, financial institutions should be careful not to "tip off" customers or potential customers where a suspicion has been formed by the financial institution that an offence is being attempted or has been or is being committed.

45A. Financial Institutions should consider including in their contracts with customers, provisions that will allow them to legally terminate arrangements where the financial institutions form the view that criminal activity is taking place and that continuing the relationship could lead to legal or reputational risks to the institution due to the suspected criminal activity.

46. Financial Institutions should undertake regular reviews[46] of all existing client identification records to ensure that they remain up-to-date and relevant and remain subject to customer due diligence processes. Where no comprehensive review has

[44] See MLR Regulation 4, CDD Para 22 to 59, and FATF Recommendations 5-9.
[45] See MLR regulation 3(1) and CDD para. 22
[46] See CDD para. 24

been done since the coming into effect of the MLA and Regulations and the BOJ Guidance Notes, then the institution should immediately implement a retrospective review of all pre-existing accounts/customers to ensure that full KYC identification details are on file. Under normal circumstances these reviews should be done should be done **at least** every five years from the date of the commencement of the relationship and at minimum five-year increments thereafter.

The documentation establishing the relationship with the financial institution should also be reviewed for continued relevance and updated where necessary. Documentation used in establishing the relationship with the financial institution should also include the requirement for customer notification to the institution of any change in identification information.

The foregoing KYC reviews would also be necessary under the following circumstances: -

- Upon the execution of a significant transaction;
- Upon material changes to customer documentation standards;
- When there is material change in the manner in which the account is operated;
- When, during the course of the business relationship, doubt arises regarding the true identity of the client or the beneficial owner of the account;
- When there is any change in the ownership or control of a corporate customer;
- Where the financial institution becomes aware at anytime that it lacks sufficient information about an existing customer.

If during the course of the updating exercise or anytime after the business relationship has commenced the financial institution discovers that the information on file is not accurate, or is no longer applicable and the correct or updated information is not available or cannot be obtained for any reason, then the financial institution must take steps to terminate the relationship and should consider referring the matter to the Designated Authority. The financial institution should conduct the necessary analysis and review of the account to inform its consideration of whether the matter should be referred to the Designated Authority and records of the conduct and results of this exercise should be in writing and available on request, to the Competent Authority/BOJ, and the Designated Authority as well as the auditors of that institution.

In such cases those accounts should be legally terminated unless direction/request to the contrary is received from the Designated Authority or other law enforcement authorities.

Identification of Natural Persons (whether resident in the jurisdiction or not)

47. The following information should be obtained from all prospective customers:

(a) true name and names used;

(b) correct permanent address, including postal address;

(c) date of birth;

(d) nationality;

(e) at least two (2) referees;

(f) source of funds, and source of wealth, where considered appropriate;

(g) contact numbers (work; home; cellular)

Institutions may also require the submission of a photograph of the customer for their records.

48. Institutions should be aware that the best identification documents are those that are the most difficult to obtain illicitly. Positive identification should be obtained from documents issued by reputable sources[47] which include:

(a) valid driver's licence (bearing a photograph), issued by the authorities in the country in which the person is resident.

(b) current valid passport;

(c) current valid voter's identification card with a photograph;

(d) TRN (if different from the Drivers licence number) in addition to any one of the identification documents described at (a) – (c) if there is doubt or uncertainty about the veracity or accuracy of the details in the identifications described at (a) – (c).

48A. In cases where the customer/applicant for business is unable to produce the identification described at paragraph 48 above, the financial institution will need to analyse the situation to determine whether it should exercise its discretion to facilitate the transaction on the basis of alternative forms of identification. The acceptable forms

[47] See CDD 22

of alternative identification can be seen at Paragraph 66, Section IV (B) of these Guidance Notes. This exception is only feasible in the following cases:-

(i) one-off customers who have not established any business relationship with the financial institution or its affiliates; and

(ii) the business transacted does not exceed US$250.00 or the equivalent figure in any other currency; and

(iii) who would not meet the definition of 'repeat customer' (i.e. for the purposes of this Guidance, a repeat customer is a person who transacts business with the financial institution or any of its branches, subsidiaries or other affiliates more than once within a three month period.)

It is not anticipated that a significant portion of the customer base of a financial institution will fall into this category. Consequently, a financial institution that seeks to rely on this exception as the normal acceptable form of identification outside of the parameters indicated above, will be deemed to be acting contrary to its KYC obligations and will expose itself to regulatory action (see paragraph 7).

Where an account is to be opened, the customer must be in a position to provide the financial institution with one or more of the identification documents described at (a) – (c) of paragraph 48 above.

Verification of KYC Details

49. The name and permanent address and employment/business details of a customer should be verified by an independent source, other than those provided by the customer, as per the following examples:

(a) Requesting sight of a current utility bill for the customer's place of residence (for example, electricity, telephone, and water) or cable receipt in the name of the customer;

(b) Checking a local telephone directory and calling the number for verification purposes;

(c) Checking the Voters List[48];

[48] Checking with the Post Office which has listings according to constituency or purchasing the CD Rom from the Electoral Office of Jamaica. The latter option is only useful if the institution is in possession of the

(d) Spot check visits to the home address or work place (where practical i.e. where the home or work place of the customer is in relatively close proximity to the financial institution);

(e) Independent confirmation of national identifications with the relevant Government Authorities e.g. (confirming drivers licences with the records of the Collectorate; confirming Voters ID with the relevant Electoral Office of Jamaica (see footnote 48 below);

(f) Confirming customer's stated place of employment independently with the employer; confirming customer's salary scale by obtaining general information from the employer of the salary scale and benefits applicable to the level indicated by the customer;

(g) Cross-checking KYC details with other financial institutions or businesses that the customer indicates financial business is transacted with for instance (the issuing bank in the case of cheque transactions; the insurance company from which the funds are indicated as being obtained, the cambio from which the foreign currency was received, or the remittance company through whom the funds were sent.); (See also paragraph 71A below);

(h) Cross-checking KYC details for one account holder with the other holder of the account and vice-versa;

(i) Cross-checking KYC details provided with other affiliated companies within the corporate group with whom the customer has also done business. (In so doing financial institutions will need to be guided by the respective Agreements with the customer which should ideally reflect that the customer's consent has been obtained to do this type of check.)

(NB. Reference to the customer also includes reference to the Applicant for business).

Identification of Bodies Corporate

50. Financial Institutions should be vigilant when dealing with corporate vehicles as they may be used as a method of ensuring anonymity. In all cases the financial institutions

customer's voter identification number as this number is needed to access the customer's details from the CD ROM. The information cannot be accessed otherwise from the Electoral Office of Jamaica.

should fully understand the structure of the prospective corporate client, the source of funds and the beneficial owners and controllers[49]. This should be the case whether the corporate client is locally incorporated or a foreign company. Financial Institutions should also ensure that they obtain the following documents or their equivalents in respect of new accounts or new transactions for companies, other bodies corporate or partnerships formed in Jamaica or overseas.

(a) Certificate of Incorporation or certificate of registration;

(b) Articles of Incorporation[50]; or Partnership Deed;

(c) Directors' Resolution authorizing company's management to engage in transactions;

(d) Financial Institutions mandate, signed application form, or an account opening authority containing specimen signatures;

(e) A financial statement of the business (audited, or in the case of companies incorporated and in operation for under eighteen months, in-house statements);

(f) A description of the customer's principal line of business and major suppliers (if applicable);

(g) List of names, addresses and nationalities of principal owners, directors, beneficiaries and management officers, including evidence of the identity of the natural persons, that is to say, the individuals that ultimately own or control the corporate vehicle;

(h) Group/Corporate structure, where applicable.

The financial institution should also determine and document the source of funds and the source of wealth being placed with the financial institution.

51. Special care should be taken by financial institutions in dealing with unincorporated bodies. The legal relationship should only be established with the principal officers or principal representatives of the body, and information on these persons, the purpose of the account and intended nature of the business relationship must be obtained. In this regard, Appendix VI provides extracts from the FATF's 2003/4 AML and CFT typologies exercise covering, inter alia, non-profit organizations.

[49] See CDD Para 33

[50] Under the new Companies Act, 2004 the requirement of Memorandum of Association has been discontinued, however, Memorandum and Articles of Association would still be relevant for the purpose of these Guidance Notes until these documentation have been updated pursuant to the new Companies Act.

52. Where the corporate customer is a part of a group of companies, the financial institution should ensure that it is fully aware of the ultimate beneficial owners/controllers of the company and that it is aware of any group arrangements or affiliates that could present a reputational risk to the financial institution. When there is doubt concerning the identity of a company, its controllers, directors, shareholders or ultimate beneficial owners/shareholders, a search should be conducted at the Registrar of Companies and/or a credit reference agency and/or the trade or professional regulatory body or other appropriate source.

Identification of Natural Persons Resident Overseas

53. The identification requirements for natural persons resident in Jamaica also apply to natural persons resident outside of Jamaica. Financial Institutions are required to obtain the same identification documentation or their equivalents for prospective customers resident outside of Jamaica. Deposit taking financial institutions should also ascertain why a non-resident client has chosen to open an account in the local jurisdiction[51].

Particular attention should be paid to the place of origin of identity and other documents provided in such circumstances, and the background against which they are produced, bearing in mind that standards of control vary between countries. A financial institution may have to request certified copies of documents, notarised by a foreign official, such as a notary public, or county clerk in addition to making appropriate enquiries with overseas credit reference agencies or similar bodies.

54. Institutions should also exercise particular care when dealing with overseas counter-parties or financial institutions acting for overseas clients, where to the local financial institution's knowledge, the overseas counter-party or representative financial institution is not subject to AML/CFT laws and regulatory arrangements at least as stringent as the Jamaican provisions. Additionally, financial institutions should carefully scrutinize any transaction proposed to be carried out with any client, counter-party or banking institution situated in a jurisdiction with weak or non-existent AML and CFT programmes or with a known history of involvement in drug production, drug trafficking, corruption, money laundering or terrorist financing or renowned for

[51] See CDD Para 23

industry sensitive activities such as the production and transportation of arms. Financial institutions should seek to keep abreast of steps being taken by such jurisdictions to effectively deal with such problems.

Identification of Overseas Bodies Corporate

55. The requirements for the customer due diligence for domestic corporate customers are also applicable to overseas corporate bodies with which a financial institution does business. Comparable documents to those listed in paragraph (50) should be obtained, when opening accounts for companies or any bodies corporate or, partnerships incorporated outside of Jamaica.

56. Particular attention should be paid to the place of origin of such documents, and the background against which they are produced, bearing in mind that standards of control vary between countries. A financial institution may have to request certified copies of documents, notarised by a foreign official, such as a notary public, or county clerk in addition to making appropriate enquiries with overseas credit reference agencies or similar bodies.

57. Financial institutions should also seek to determine and document the source of funds/wealth being placed with the financial institution or being used for any proposed transaction.

58. Financial institutions should **not** establish business relationships with foreign entities with bearer shares[52]. Financial institutions should also exercise a high level of caution when establishing business relationships with foreign companies that have nominee shareholders. If the ultimate beneficiary/ies or beneficial shareholders/s cannot be reliably established or there are no reliable measures in place to monitor any changes in the ownership structure, the relationship should **not** be commenced, or where a business relationship has already been established, this relationship should be legally terminated.

[52] See CDD Para. 34

SECTION IV. B. - SPECIFIC GUIDANCE FOR CAMBIOS, (EXCHANGE BUREAUX) AND MONEY TRANSFER AND REMITTANCE AGENTS AND AGENCIES (REMITTANCE COMPANIES)

59. This section of the Guidance Notes deals with the identification procedures that cambios and remittance companies are required to undertake before proceeding with a transaction or before establishing a business relationship. It is understood and accepted that the nature of the relationship between cambios, remittance companies and their respective customers can be fundamentally different from that established between banks and other regulated financial institutions and their customers. Cambios are entities, which are permitted with the approval of the Bank of Jamaica, to only buy and sell foreign currency. Remittance companies are entities which facilitate the movement of funds from one person to another person (whether intra-island or across national borders) by way of remitting the funds from one remittance company to the next location of its remittance arm which bears proximity to the destined location of the intended recipient outlined in the customer's instructions. The customer profile of cambios and remittance companies will therefore fall largely within the following categories: -

(i). Customers[53] conducting one-off transactions;

(ii). Customers constituting new arrivals to the country (i.e. tourists / visitors)

(iii). Repeat customers which for the purposes of these Guidance Notes means the following:-

- Repeat customers, for the purpose of cambio transactions, are defined as "Persons who conduct a US$250[54] and over transaction or its equivalent in other currencies, more than once in a three (3) month period".

- Repeat customers, for the purpose of outbound remittance transactions, are defined as "Persons who transact business with a Primary Agent (and/or the sub-agent/(s) thereof) more than once

[53] Customers – both individual and corporate
[54] Or the equivalent of US$250 in any other currency.

within a three (3) month period irrespective of the transaction amount".

Based on the customer profile of these entities there may be practical difficulties with enforcing the same level of KYC procedures in relation to the customers described above particularly in relation to (i) and (ii).

60. According to the MLR, an 'applicant for business' means a person seeking to form a business relationship **or carry out a one-off transaction** with a financial institution. Guidance Notes 45 - 55 require an institution to obtain adequate customer identification and ensure that the contract permits the institution to withdraw from arrangements where the view is formed that criminal activity is or may be taking place or that there are reputational risks that could arise due to the suspected criminal activity. **These requirements are fully applicable to cambios and remittance companies.** However, considering the possible customer profile of cambio and remittance businesses, it might not in all cases be practicable or feasible for the same financial institutions standards as regards establishing KYC procedures to be fully applicable to all cambios and remittance company transactions. Consequently, cambios and remittance companies will be subject to identification verification requirements, which are more compatible with the nature of the customer/entity relationship generated by such businesses.

KYC Guidance

61. All applicants for business with a cambio or remittance company, must be required to submit the information at Paragraphs 47(a), (b), and (c) of these Guidance Notes for all transactions in the case of persons doing business with remittance companies and for all transactions reaching or exceeding US$250.00[55] in the case of persons doing business with cambios. In ensuring that there is compliance with this requirement, cambios and remittance companies are not expected to apply the exact verification procedures outlined in Guidance Note 49 in relation to customers. However, cambios and remittance companies must employ alternative

[55] Or the equivalent of US$250 in any other currency.

verification processes more suited to their operations in order to satisfy themselves of the veracity of the information provided and of the authenticity and validity of the identification tendered. (Techniques to be employed may include but not be limited to checking the signature of the applicant for business with the signature on any transaction instrument or documentation offered by the customer; ensuring that identifications tendered do not appear to be forged documents or documents that have been tampered with; that the picture in the identification used is consistent with the features of the person tendering the identification; questioning the customer for confirmation details where this becomes necessary in the circumstances and clearing all cheque transactions before proceeding to act upon such instruments.) (See also paragraph 49(e) above).

62. Where the applicant for business is a corporate customer seeking to act through an agent/bearer (whether employed or contracted, and which is usually the case), the cambio or remittance company must enforce the identification requirements at 48 (a) – (c) of the Guidance Notes in relation to the agent/bearer. Additionally, the agent/bearer must submit a copy of the corporate customer's certificate of incorporation and a letter from the corporate customer on the corporate customer's official letterhead and bearing the signature of an authorized officer.[56] The letter should clearly indicate the business to be transacted, that the agent/bearer is acting on the corporate customer's behalf for this matter and that the person signing to the letter is authorized so to do. Where in relation to the corporate customer it appears to the cambio or remittance company conducting the transaction that the agent/bearer is not the usual agent/bearer, or the letter from the corporate customer is in any way defective, (eg. it is not on official letterhead; there have been alterations or amendments to the contents of the letter, and/or these amendments are not signed in verification clearly by the author of the letter; or the letter itself is not signed) business should either not be transacted at all, or should be delayed until the corporate customer is contacted by the cambio or remittance company and asked to confirm in writing or issue renewed written instructions and the confirmation or renewed instruction is in fact received. In ensuring that there is compliance with KYC requirements in relation to corporate customers, cambios and remittance companies are not expected to apply

[56] For the purpose of these Guidance Notes "authorized officer" would mean a manager /senior officer of the company, and as such the letter should clearly indicate the name and position of the "authorized officer".

the exact verification procedures outlined in Guidance Note 50(b)(c) or (h) in relation to corporate customers. However, cambios and remittance companies must employ alternative verification processes more suited to their operations in order to satisfy themselves of the veracity of the information provided and of the genuineness of the information provided by or on behalf of corporate customers. (In this regard see also the last paragraph of Guidance Note 63).

63. The above notwithstanding, it should be noted that:

(i) For any transaction above US$1,000.00 or the equivalent amount in any other currency:

(a) all applicants for business with a cambio or remittance company must submit information at paragraph 47(f) (information on source of funds) in addition to the information required at paragraph 47(a), (b) and (c), or at paragraph 50 (where it speaks to source of funds), in addition to the information required at paragraph 50(a), (c), (d), (f), and (g) in relation to corporate customers.; and

(b) Identifications tendered must be photocopied and the photocopies retained in the cambio / remittance company's records. In the case of remittance companies this requirement is only applicable to outbound transactions.

(ii) All repeat customers must submit information at paragraph 47(f) or paragraph 50 (where it speaks to source of funds) in addition to the information required at paragraph 47(a), (b) and (c), or at paragraph 50(a), (c), (d), (f), and (g) and identification documentation for such persons must be photocopied and the photocopies retained in the cambio/remittance company's records. In the case of remittance companies this requirement to photocopy identification documentation is only applicable to outbound transactions.

The requirement at paragraph 63(i) is not applicable to Authorized Foreign Exchange Dealers and Cambios (who are the 'applicants for business' with a cambio or remittance company) unless the transaction is "red-flagged" for closer scrutiny as discussed in paragraph 69 herein or the transaction amounts to a suspicious or unusual transaction.

The requirements of paragraph 50 (c), (d), (f), and (g) will be satisfied by cambios if the corporate customer completes and submits to the cambio with which business is to be transacted, the Corporate Profile Form developed by the Cambio Association of Jamaica in consultation with the Bank of Jamaica. (The applicable form is attached as - Appendix II A. The minimum financial information that cambios should obtain from corporate customers are:-

(a) Total Capital as at the end of the last financial year for the customer;

(b) Total Assets as at the end of the last financial year for the customer;

(c) Total Liabilities as at the end of the last financial year for the Customer;

(d) Change of Directors/Principals/significant shareholders signing officers/ since the completion of the last corporate profile form;

(e) Main business to be carried out/services to be offered by the customer;

(f) Whether the customer is in possession of any special authorizations under the BOJ Act Part IVA pertaining to foreign exchange activities. (Details of the authorization and duration thereof to be provided if the customer indicates such authorization exists);

(g) Purpose of FX activities the company can be expected to conduct with the cambio, i.e. -

  (i) Bill payments for services rendered by overseas based parties; or for items purchased from overseas for the customer's own use;

  (ii) Importation of commercial goods;

  (iii) Own account investment activities;

  (iv) Other- details to be provided as to what the activity entails - in outlining the purpose of the FX activities to be conducted a general estimation of the frequency with which the company expects to be conducting or actually conducted these activities for the relevant period to be included e.g. daily; weekly; fortnightly; monthly; bi-monthly; quarterly; bi-yearly; annually; occasionally; or as the need arises.)

64. Full banking KYC standards are applicable for significant transactions. For the purposes of these Guidance Notes, a "significant transaction" in relation to any business being done with a cambio or remittance company means any transaction amounting to or exceeding US$8,000 (in the case of business done with cambios) and

US$5,000 (in the case of business done with remittance companies) or the equivalent thereof in any other currency.

Establishing Appropriate Identification

65. The "appropriateness test" of the identification obtained is that, from the records prepared and retained by the cambios or remittance companies, one should be able to compile a complete picture of the customer and of the business that customer transacted with the cambio or remittance company.

66. The type of identification tendered must be a valid Passport, Drivers Licence, or National Identification.

If an applicant for business has none of these forms of identification with him/her, then the Cambio or remittance company may accept:-

(a) a customer's worker's identification (with a picture) from a known employer in addition to the customer's TRN; or a birth certificate accompanied by a Declaration of Identification and a photograph both of which (i.e. the Declaration and the photograph) must be signed by a Justice of the Peace (JP), a Minister of Religion or an Attorney-at-Law confirming the identity of the customer; or

(b) a customer's client card (where the client card was issued to that customer by the specific cambio or remittance company itself). Where however client cards are the sole source of identification relied on, the cambio's records or the records of the remittance company must contain a photocopy of the customer's official identification as well as corroboration of the customer's address and source of funds and these records will need to be updated from time to time (see paragraph 46 above).

(c) In the case of Remittance Companies when conducting inbound transactions only, a valid school ID where the student is enrolled in a secondary or tertiary institution may be accepted where the student

identified as the recipient, is maintained through remittances sent by overseas parents or guardians responsible for him/her. The ID must have the following features:

- A photograph of the student
- Signature of ID holder (student)
- ID Number
- Expiry date of ID
- Name of the relevant academic institution (high/secondary school or tertiary institution)
- Signature of principal/bursar/vice-principal of the relevant academic institution.

The foregoing is applicable only to individuals under the age of 18 years as persons over 18 years of age will have attained the age of majority[57] and will have achieved the age limit to qualify for obtaining other forms of identification i.e. Drivers Licence; Voters I.D. etc.. Additionally, the point must be made that this paragraph is meant to facilitate the specific circumstances of remittances from persons (parents/guardians) living overseas to their children /dependants (between the ages of 10 and 17 years of age) in Jamaica for school and living expenses.

67. The identification reference number must be clearly and accurately recorded on the document evidencing the transaction with the customer; (where the identification tendered is a birth certificate and J.P's Declaration, the Declaration should be collected from the customer and retained by the cambio/remittance company and the reference number on the Birth Certificate clearly indicated on the document evidencing the transaction and the Declaration stapled to the document evidencing the transaction.)

68. The customer's **complete** residential address must be recorded. Therefore short addresses such as May Pen P.O. or Post District PA; will **not** be acceptable. The address must be sufficient for the customer to be contacted by mail or by hand (i.e. bearer) and (should the need arise) by telephone. If a business place is being given as

[57] See The Law Reform (Age of Majority) Act, 1979, sections 3 and 6

the official address of contact (where the applicant for business is a corporate customer) then the name of the business should also be given and the full business address stated. Descriptions such as "business place" will not be acceptable. If there is any uncertainty about the address, a contact number must be obtained from the customer.

69. Suspicious Transactions. Note that where a transaction appears to be suspicious, the transaction should not be conducted. Transactions that are not at the stage of being regarded as suspicious but appear to be unusual and therefore raise questions, or are flagged for closer scrutiny and which in that case are still conducted, should be subject to **full KYC banking standards and reported to the Designated Authority without delay**. (See also paragraph 92B).

70. The ability to discontinue transactions or terminate business relationships.

As cambios and remittance companies will not be opening or operating on-going accounts for customers, it may be unlikely that prolonged business relationships such as those established with customers by other financial institutions, (banks, insurance companies, unit trusts, mutual funds, securities dealers, cooperative societies), will be established in the case of cambios and remittance companies. Cambios and remittance companies must nonetheless seek to employ procedures that make it **abundantly clear** that they can refuse to do business with a customer and this is probably best achieved by a bold notice to this effect being displayed perhaps by the window of the teller. In the case of persons who have obtained client cards, the documentation issued with the card or the card itself should make it abundantly clear that the card privileges and the card can be withdrawn at anytime without notice where the cambio or remittance company believes that its discretion in this regard needs to be exercised.

SECTION IV. C. – HEIGHTENED IDENTIFICATION AND KYC REQUIREMENTS IN SPECIAL CASES

71. Heightened identification and KYC requirements must be invoked in the following cases:-

- Verification of KYC post commencement of the business relationship;
- Introduced business;
- Trust Accounts;
- Accounts opened by Professional Intermediaries;
- High Risk Customers (private banking clients; transferring clients; politically exposed persons (PEPS); non-face-to-face customers; Transactions via emerging technology; correspondent banking; payable through accounts; customers from countries with inadequate AML/CFT frameworks; transactions undertaken for occasional customers; transactions undertaken by non-customers; custody arrangements; wire transfers and other electronic funds transfer activities).

Verification of KYC Post Commencement of Business Relationship

71. A. MLR 4 and 8(2) both speak to situations in which satisfactory evidence of a customer's identification can be obtained as soon as is reasonably practicable after contact is first made between that person and an applicant for business. Before proceeding in this manner a financial institution must be in a position to provide documentary evidence of the evaluation it undertook to satisfy itself that it could proceed with the transaction. This includes evidence of considerations which at a minimum should include-

- The nature of the proposed business relationship;
- The nature of the transaction/(s) contemplated;
- The geographical location of the parties;
- Practicality of proceeding viz. entering into commitments; or facilitating transactions before confirmation of the identification is obtained;

- Assessment of the risks to the institution if it proceeds without confirmation of the customer's identification.

Confirmation of KYC with the assistance of other financial institutions

71. B. (See also paragraph 49G above). In some cases, a financial institution may require the customer to issue instructions to another financial institution with whom he/she has dealings and which institution is able to provide appropriate KYC verification for the customer in question. A financial institution may therefore need to approach another on a non-competitive basis, specifically for the purpose of verifying identity. Where this is the case, it is expected that members of the industry will formulate industry agreements and protocols on these matters, within the specific constraints of the law. Where KYC verification is pursued through this option and the information is still not forthcoming from the institution from whom the assistance is requested, then unless the information is obtained:

- the transaction should not proceed; or
- where commenced in circumstances where it was deemed reasonable to proceed ahead of the verification, the transaction should not be completed; or
- where the relationship is already formed (eg. an account is opened ahead of verification) then no other service, facility or transaction should be provided or conducted with, on behalf of, or in relation to this customer;

unless and until the appropriate KYC verification information has been received. The financial institution must ensure that it is legally in a position to terminate the account/transaction or sever the business relationship where the verification of KYC details cannot be obtained. (See also paragraph 45A above).

In order to facilitate compliance with the law by all financial institutions, it is therefore critical that institutions respond in a timely manner to each other's requests for assistance with the verification of KYC information.

Introduced Business[58]

72. In circumstances where business is being introduced by individuals or companies, **the ultimate responsibility is on the recipient financial institutions to know the referred customer and his/her business**. Financial institutions should therefore not place excessive reliance on the identification procedures that they expect the introducers to have performed. Financial institutions must carefully assess the fitness and propriety of introducers as well as the customer identification and due diligence standards that the introducers maintain, using the following criteria: -

(i) Introducers should adhere to minimum "Know Your Customer" standards as identified within these Guidelines;

(ii) Financial institutions must be able to verify the due diligence procedures undertaken by the introducer at any stage and the reliability of the systems put in place to verify the identity, financial history and KYC details of the customer;

(iii) Notwithstanding any reliance on an introducer's representations, a financial institution should ensure that it procures and reviews all the relevant identification data and other documentation pertaining to the customer's identification, financial history and other KYC data. This information must also be available for review by the Supervisory Authority;

Whenever possible, the prospective customer should be interviewed.

Where it has been determined that the referenced identification standards are unsatisfactory or weak, then the licensee must conduct its own customer due diligence assessment.

Trust Accounts[59]

73. Subject to paragraph 74 below, where an account is being opened by a trustee pursuant to trust arrangements, the identity of **all** parties and beneficiaries to the transaction must be ascertained and recorded in keeping with the account opening procedures

58 See MLR regulation 7, FATF Recommendation 9 and CDD Paragraphs 35 and 36

59 See MLR regulation 6 and CDD paragraph 32

identified in these Guidance Notes. Specifically, this would include identification of the trustees, settlors and grantors, the beneficiaries of the trust account, source of funds or wealth from which the proceeds of the trust are derived and the purpose and details (i.e. terms) of the trust arrangement.

Accounts opened by Professional Intermediaries[60]

74. Professional intermediaries include pension funds, unit trusts and other fund managers, as well as lawyers, securities dealers and stock brokers managing single or pooled accounts held on deposit or in escrow for clients.

If the financial institution determines that an account is being held on behalf of a single client, the identity of the client **must** be ascertained. Where pooled accounts are maintained the licensee may rely on the professional intermediary's due diligence process and not look through to the ultimate beneficiary/ies, but **only** if the following conditions obtain:

I. The intermediary engages in sound due diligence processes (which, at a minimum are consistent with the standards outlined in these Guidance Notes) and/or is subject to similar regulation for the detection and prevention of money laundering and terrorist financing activities;

II. The financial institution is able to verify the reliability and effectiveness of the intermediary's customer due diligence and anti-money laundering and terrorist financing policies, systems and processes at any stage. This requirement should ideally be included among the terms and conditions agreed by both parties in the operation of the relevant account;

III. The intermediary has the necessary systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries, which systems do not include the use of "payable through accounts"(see paragraph 86);

[60] See MLR regulation 6, FATF Recommendation 9 and CDD Paragraph 36-39

IV. The intermediary is operationally and legally able to provide the required information (i.e. identity; source of funds/wealth etc.) on each of the interim and ultimate beneficiaries to the financial institutions**;**

V. The information provided to the financial institutions must also be available to the Supervisory Authority for review pursuant to the execution of supervisory duties. [Licensees should note that it is also intended that such information should also be accessible to the Designated Authority under the MLA and law enforcement agents carrying out criminal investigations. This is one of the amendments to the AML framework that is now being contemplated].

Note that Appendix VI provides extracts from the FATF report on the 2003/4 typologies exercise covering, inter alia, professional intermediaries or gate-keepers. Appendix VII provides extracts from the FATF report on the misuse of corporate vehicles including trust and company service providers.

High Risk Customers[61] (Paragraphs 75 - 93)

75. Financial institutions should develop graduated "know your customer" policies and procedures for higher-risk customers that go beyond the basic information-gathering requirements for average/low risk clients. This would include a detailed description of the types of customers that are likely to pose a higher than average risk to a financial institution based on assessment of certain factors including customers' background, country of origin, important public or high profile position/(s) held, linked accounts, business activities or other risk indicators.

76. Accounts for high-risk customers must not be opened unless senior management approval is obtained. Further, financial institutions should ensure that there are adequate management information systems to provide timely and comprehensive management reports to facilitate effective monitoring of high-risk client accounts by senior management. At a minimum, the under-mentioned categories of clients and situations should be subject to enhanced due diligence policies.

[61] See CDD paragraph 6 and 20

(i) Private Banking Clients[62]

77. In particular, institutions that offer private banking services for high net worth individuals must ensure that enhanced due diligence policies and procedures are developed and clearly documented in the overall KYC policy to govern this area of operations. Senior management with ultimate responsibility for private banking operations should ensure that the personal circumstances, income sources and wealth of private banking clients are known and verified as far as possible, and should also be alert to sources of legitimate third party information. Whilst it is appreciated that efforts must be made to protect the confidentiality of private banking customers and their businesses, these accounts must be available for review by the Supervisory Authority, the Designated Authority, and the financial institution's internal compliance officers and internal auditors. The approval of private banking relationships must be obtained from at least one senior level officer, other than the private banking officer/relationship manager.

(ii) Transferring Clients[63]

78. Where accounts are transferred from another financial institution, enhanced KYC standards should be applied especially if the licensee has any reason to believe that the account holder has been refused banking facilities by the other financial institution.

(iii) Politically Exposed Persons (PEPs)[64]

79. PEPS are individuals in foreign jurisdictions (or the local jurisdiction) who are or have been entrusted with prominent public functions. This includes heads of state or of government, senior politicians, senior government, judicial or security force officials (whether elected or not), senior executives and their immediate family[65].

Financial institutions should not establish business relationships with PEPs if the financial institutions know or have reason to suspect that the funds derive from corruption or misuse of public assets. Senior management with ultimate responsibility

[62] CDD Paragraph 5
[63] See CDD Para 29
[64] See FATF Recommendation 6 and CDD Para 6
[65] Parent, siblings, spouse, children and in-laws as well as close associates i.e. persons known to maintain unusually close relationship with PEPS also included in requirement for enhanced scrutiny.

for banking operations should ensure that the personal circumstances, income sources and wealth of PEPS are known and verified as far as possible, and should also be alert to sources of legitimate third party information. Whilst it is appreciated that efforts must be made to protect the confidentiality of PEPS and their businesses, these accounts must be available for review by the Supervisory Authority, the Designated Authority, and the financial institution's internal compliance officers and internal auditors. The approval of business relationships involving PEPS must be obtained from at least one senior level officer, other than the banking officer/relationship manager. To mitigate the significant legal and reputational risk exposures that financial Institutions face from establishing and maintaining business relationships with PEPS, the following procedures should be followed prior to the commencement of such relationships: -

- Obtain all the relevant client identification information as would be required for any other client prior to establishing the business relationship. Additionally, the decision to open an account for a PEP must be taken at the senior management level;
- Information gathering forms/procedures should be structured to reasonably allow the financial institution to ascertain whether a client is a PEP, and to identify persons and companies/business concerns clearly related to or connected with the PEP. The financial institution should also access publicly available information to assist in the determination as to whether or not an individual is a PEP;
- Investigate and determine the income sources prior to opening account. Reference to income sources includes - source of funds; source of wealth and asset holdings; confirmation of the general salary and entitlements for public positions akin to the one held by the customer in question – (General information on local PEPS may be available from the Public Services Commission in Jamaica. General information on local PEPS can also be viewed from the Jamaica Parliamentarian's Salaries Review Commission Report accessible on the website of the Ministry of Finance and Planning. This report details the basic salary and allowances (travelling, subsistence, housing, and utilities) of parliamentarians. Comparable information may be available on similar national websites for foreign PEPS.

Following the commencement of banking relationships, there should be:

- Regular review of customer identification records to ensure they are kept current ; and
- Ongoing monitoring of PEP accounts.

The abovementioned procedures should also be followed for the **existing** client base to ensure that all current PEPs have been so identified and remain subject to enhanced customer due diligence processes. Please also refer to Appendix VI, which contains extracts from the FATF 2003/4 AML/CFT typologies exercise covering, inter alia, politically exposed persons.

Non Face-to-Face Customers

80. Financial institutions should avoid the practice of opening new accounts via post, unless higher standards of scrutiny are applied. In the case of electronic banking accounts opened via the Internet or similar technology, these should be subject to more rigorous identification and verification standards including independent verification by a reputable third party. MLR regulation 8 touches on the matter.

Emerging Technology[66]

81. Additionally, licensees should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks. At a minimum, licensees should follow the procedures outlined below to assist in the identification and verification of non-face-to-face customers:

- Documents presented should be certified by the relevant and appropriate authority;
- Customers should submit additional documents to verify identity;
- Independent and if possible, face to face contact should be made with the customer by the licensee;
- Where third party introduction is being facilitated, this must be subject to the licensee ensuring that the introducer meets the criteria outlined in paragraph 72 above;

[66] See FATF Recommendation 8 and CDD paragraph 46

- There should be the requirement that, if possible, the first payment be made through a financial institution which has similar customer due diligence standards.

Appendix VIII provides extracts from the FATF report on new payment methods (i.e. retail electronic payment systems; electronic purses; internet payment services etc.) and how such facilities can be used to facilitate money laundering.

Correspondent Banking[67]

82. Correspondent banking refers to the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Financial institutions must apply appropriate levels of due diligence to such accounts by gathering sufficient information from and performing enhanced due diligence processes on correspondent banks prior to setting up correspondent accounts. This should, at a minimum include:

- Obtaining authenticated/certified copies of Certificates of Incorporation and Articles of Association (and any other company documents to show Registration of the institution within its identified jurisdiction of residence) ;
- Obtaining authenticated/certified copies of banking licences or similar authorization documents, as well as any additional licences needed to deal in foreign exchange;
- Determining the supervisory authority which has oversight responsibility for the respondent bank;
- Determining the ownership of the financial institution;
- Obtaining details of respondent bank's board and management composition;
- Determining the location and major activities of the financial institution;
- Obtaining details regarding the group structure within which the respondent bank may fall, as well as any subsidiaries it may have;
- Obtaining proof of its years of operation, along with access to its audited financial statements (5 years if possible);
- Information as to its external auditors;

[67] See FATF Recommendation 7 and CDD paragraphs 49-52

- Ascertaining whether the bank has established and implemented sound customer due diligence, anti-money laundering and anti-terrorism financing policies and strategies and appointed a Compliance Officer (at management level), inclusive of obtaining a copy of its AML/CFT policy and guidelines;
- Ascertaining whether the correspondent bank has in the previous seven (7) years (from the date of the commencement of the business relationship or negotiations thereof), been the subject of or is currently subject to any regulatory action or any AML/CFT prosecutions or investigations. A primary source from which this information can be sought and ascertained include the Banking Regulatory Authority for the jurisdiction in which the correspondent bank is resident. Information may also be available from the Regulatory Authority's website;
- Ascertaining that the foreign correspondent banks do not permit their accounts to be used by shell banks;
- Establishing the purpose of the correspondent account;
- Documenting the respective responsibilities of each institution in the operation of the correspondent account;
- Identifying any third parties that may use the correspondent banking services; and
- Ensuring that the approval of senior management is obtained for the account to be opened.

82. A. While Jamaica currently does not provide correspondent banking services to foreign banks, financial institutions should note that in the event that correspondent banking services are provided to foreign respondent banks then the financial institution will need to bear in mind the requirements of these Guidance Notes particularly those outlined at paragraph 82 above. Additionally, financial institutions will need to satisfy themselves that the foreign respondent banks do not permit their accounts to be used by shell banks. In this regard financial institutions should pay attention to the following indicators:-

- whether the respondent bank permits "payable through accounts". This would be one likely way in which shell banks could take advantage of respondent banks;

- the respondent bank's inability or reluctance to provide ultimate beneficiary/customer information in relation to pooled arrangements or collective investment schemes or aggregate accounts whereby only the KYC on the agent of the beneficiaries of the pooled arrangement, collective investment scheme or aggregate account will be or can be provided by the respondent bank;

- the country in which the foreign respondent bank resides (see Paragraph 54 and 87-88). Jurisdictions with secrecy laws that prohibit the release of any KYC information or which laws present an obstacle to the KYC due diligence process pose a particular problem in this regard.

Record- Keeping Regarding Correspondent Banks

83. Financial institutions should also be aware that Section 319(B) of the USA Patriot Act requires that financial institutions maintain records of the owners and the US agents of foreign respondent banks. Subsection (k) also authorizes the relevant authorities in the USA to issue a summons or subpoena to any foreign financial institution that maintains a correspondent account in the USA and to request records relating to such account, including records maintained outside the USA relating to the deposit of funds into the foreign bank. If a foreign bank fails to comply with or contests the summons or subpoena, any financial institution with which the foreign bank maintains a correspondent account **must** terminate the account upon receipt of notice from the authorities.

Shell Banks[68]

84. FATF recommendation 18 states that countries should refuse to enter into or continue a correspondent banking relationship with a shell bank and further recommends that countries not approve or accept the establishment or continued operation of shell banks. Financial institutions will therefore need to ensure that the required due diligence procedures are undertaken (see paragraph 82) to ensure that correspondent relationships are **not established or continued with shell banks.**

[68] See FATF Recommendation 18

85. Shell banks are defined as banks that have no physical presence in the jurisdiction in which they are registered. To be deemed as having a "physical presence", a bank or financial institution should: -

- Be physically located (i.e. "brick and mortar" presence) at a fixed address in the country in which it has been licensed to do banking business. This fixed address must therefore be other than a post office box or electronic address;
- Employ at least one or more individuals on a full-time basis at the above-named location;
- Maintain operating records relating to its banking activities at its fixed address;
- Be subject to inspection by the banking authority by which it has been licensed.

To this end financial institutions will also need to be particularly mindful of the requirements of the USA Patriot Act, which effected several changes to the anti-money laundering and terrorist financing provisions of that country's Bank Secrecy Act. (Refer to Paragraph 33).

Payable-Through Accounts

86. Banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf. An example of this would be a payable-through account[69]. The glossary to the FATF revised 40 Recommendations states that "Payable-through accounts refer to correspondent accounts that are used directly by third parties to transact business on their own behalf". In this regard, banks must be guided by the criteria established for introduced business, as outlined in paragraph (72).

{NB. The USA PATRIOT Act Section 311 (1) BANK DEFINITIONS (C) contains the following definition for a PAYABLE-THROUGH ACCOUNT- "The term `payable-through account' means an account, including a transaction account (as defined in section 19(B)(1)(C) of the Federal Reserve Act), opened at a depository institution by a foreign financial institution by means of which the foreign financial institution permits its customers to engage, either directly or through a sub-account, in banking activities usually in connection with the business of banking in the United States.". Section 19(B)1(C) of The Federal Reserve Act - The term "transaction account" means a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. Such term includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts}.

[69] See Basel CDD, paragraph 52.

Countries with Inadequate AML/CFT Frameworks[70]

87. Financial institutions must exercise added care when dealing with clients residing in countries with weak or non-existent laws and regulations to detect and prevent money laundering and terrorist financing. Such high-risk countries should be clearly outlined in the financial institution's policy manual and updated whenever necessary. As a general guide in identifying these jurisdictions, financial institutions may refer, on a continual basis, to the FATF's list of countries, which have been identified as "non-cooperative" in the fight against money laundering (NCCT). This may be accessed at the FATF's website **http://www1.oecd.org/fatf/NCCT_en.htm**. The Bank of Jamaica will also periodically update its licensees with significant information on this issue, based on advisories received from the CFATF and the FATF.

88. The commencement of business relationships with clients residing in high-risk countries must have the prior approval of senior management. Any suspicious transactions originating from such countries must be investigated, the findings established in writing and immediately reported to the Designated Authority.

Transactions Undertaken For Occasional Customers[71]

89. Where a financial institution undertakes these transactions, satisfactory evidence of identity must be obtained failing which, the transaction should be terminated. The non-account holder must produce positive evidence of identity as set out in paragraphs (47 through 50) above, and all copies, reference numbers and other relevant details relating to the transaction should be recorded and retained by the financial institution for a minimum period of not less than five (5) years.

Transactions by Non-Customers

90. Funds deposited into an existing account by persons whose names do not appear on the mandate for that account, should be handled with particular care. In cases where such transactions are not routine, they should be treated in the same way as transactions with non-account holders. (See paragraph 89 above)

[70] See FATF Recommendation 21
[71] See MLR Regulation 3

Custody Arrangements

91. A financial institution must take certain precautionary measures in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, there must be strict adherence to the identification procedures set out in these Guidance Notes and the relevant statutes.

Wire Transfers and Other Electronic Funds Transfer Activities[72]

92. According to the interpretative note to FATF Special Recommendation 7 – the terms 'wire transfer' and 'funds transfer' refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means, with a view to making an amount of money available to a beneficiary person at another financial institution. The following information should be obtained and retained for the statutory period when conducting any/all electronic fund transfers (wire transfers, remittances etc): -

- The identity of the originator/remitting customer (including name, address and account number (in the absence of an account number, a unique reference number must be included) whether or not the originator is a customer of the licensee; (Note that according to the interpretative note to FATF Special Recommendation 7, (paragraph 2(e), the originator is an account holder, or where there is no account, the person that places the order with the financial institution to perform the wire or funds transfer);
- The identity of the ultimate recipient/beneficiary, where practical (including name, address and account number (in the absence of an account number, a unique reference number must be included);
- Related messages/instructions that accompany transfers.

In establishing the identity of the originator/remitting customer and the ultimate recipient/beneficiary, a financial institution should take reasonable measures to understand the ownership and control structure of the person conducting the

[72] See FATF Recommendation 5 and FATF Special Recommendation 7 on Terrorist Financing

transaction including the purpose and intended nature of the business relationship. Verification of the identity of the originator/customer /beneficial owner should:-

(i) be done before the establishment of the business relationship or before conducting any one off (i.e. occasional) transactions with customers in accordance with regulation 3(1) of the Money Laundering Regulations;

(ii) be applied to existing customers and at appropriate times {(i.e. when significant transactions are being conducted; when transactions which do not appear consistent with the nature or pattern of transactions normally carried out by the customer are conducted; when transactions are conducted after long periods of inactivity of the account or when transactions are conducted via use of the reference number (as the case may be)}. Please note that these circumstances are not exhaustive and financial institutions are therefore expected to maintain a reasonable level of diligence and monitoring in conducting wire transfers or any other kind of funds transfers.

All information related to the identity of customers and the transactions conducted should be retained for a minimum of five (5) years from the date on which the relevant financial business was terminated. (Please also be guided by paragraphs 95 and 96 of these Guidance Notes. Please also refer to following Appendices which provides extracts from reports of FATF Typologies Exercises:

- Appendix VI which provides extracts from the report on the FATF 2003/4 AML/CFT Typologies Exercise covering, inter alia, wire transfers;
- Appendix VIII which provides extracts from the FATF report on new payment methods and how these can be used to further money laundering activities;
- Appendix IX which provides extracts from the FATF report on Trade-Based money laundering and includes case studies which include the use of wire transfers to facilitate this type of money laundering.

92. A. The Guidance in paragraph 92 is applicable to both domestic and cross border wire transfers and electronic funds transfers.

92. B. Specific SRVII Guidance

(i) Batch transfers- Unless the receiving or intermediary financial institution has the technical capability to immediately access from its records, the requisite originator and beneficiary details as set out in paragraph 92, batch transfers should not be accepted in the course of wire transfers or any other electronic funds transfers regardless of whether such transactions qualify as 'routine' or 'non-routine' transactions.

(ii) Transfers not accompanied by the complete originator information –These transfers should not be processed by the receiving or intermediary financial institution unless and until the complete originator information is available. Where a transfer of this nature is identified, it should be immediately red flagged for either termination or as one not to be acted on, until the requisite information is received. To this end it is the responsibility of financial institutions to ensure that they are legally in a position to terminate the transaction, or to delay acting on the transaction until the requisite information has been received. Where the decision is taken to terminate the transaction, financial institutions should be guided by the appropriate guidance in these Guidance Notes (particularly paragraphs 45, 45A and 106A). In the interest of good customer relations, financial institutions should pursue methods of making their customers aware from the outset that all wire and electronic funds transfers must be accompanied by the complete originator details as the absence of this information can cause the transaction to be delayed or terminated.

(iii) The guidance in (i) and (ii) are also equally applicable to financial institutions conducting outgoing domestic transfers and outgoing cross border transfers.

(iv) Where the receiving or intermediary financial institution finds that there is an ongoing situation of consistent or the frequent receipt of transfers of the nature described in (ii) above, it should consider terminating its business relationship with the financial institution from which such transfers are consistently or frequently received (i.e. the sending or ordering financial institution). In so doing financial institutions should be guided by paragraphs 45, 45A and 106A.

92. C. Financial institutions are also reminded of paragraph 7 in observing their obligations in this regard.

92. D. Financial institutions should note that Regulators are required to specifically review whether institutions are in compliance with **Special Recommendation VII and to this end; the BOJ's regular exams will continue to incorporate a review as to whether this is being appropriately implemented.**

Anonymous Accounts/ Accounts In Fictitious Names/Numbered Accounts

93. **This Guidance Note speaks to an issue that goes to the heart of KYC procedures. A financial institution must not in the course of business carried on by it, permit any person with whom it forms a business relationship, to conduct any transaction with it by means of an anonymous account, an account held in a fictitious name[73] or an account identified only by a numbered account;**

- **For the purposes of these Guidance Notes an anonymous account includes an account for which there is no name, by which the account holder can be identified;**

- **A numbered account refers to an account that is identifiable solely by reference to the number or series of numbers assigned to that account[74];**

-

- **For the purposes of these Guidance Notes an account held in a fictitious name includes an account name which when subjected to customer due diligence identification and verification procedures, does not constitute the true name of the account holder or of the Principal on whose behalf the transaction is being**

[73] See FATF Recommendation 4 and 5 and CDD Paragraph 30
[74] See MLR 11(2)

done, or of the beneficiary of the legal arrangement through which the transaction is being conducted.

SECTION IV. D. RECORD KEEPING

94. Once a business relationship has been formed, the financial institution should maintain records of client identification and transactions performed[75]. Clear standards must be outlined within the policy manual pertaining to record keeping including the minimum five-year retention period from the termination of the business relationship.

95. Client identification files should contain account numbers and full customer identification information, account opening forms, copies of identification documents, business correspondence and other relevant details. Transaction records must be maintained in such a form that would allow for reconstruction of individual transactions, to provide audit trails and if necessary, evidence for prosecution of criminal activity. At a minimum, this would therefore include the date and nature of the transaction and the amounts and types of currency used, if any.

96. The Money Laundering Regulations require a financial institution to maintain customer identification records for a minimum period of five (5) years[76] after the termination of the business relationship. Similarly, records relating to transactions carried out by each customer must be maintained for at least five (5) years after the transactions have been completed.

97. The DOFPA also places a financial institution under a duty to retain all records and documents pertaining to all transactions carried out by it for a minimum period of five (5) years. Retention may be by way of original documents, stored on microfiche, or in computerized form. Institutions which store original documents in a computerized form should bear in mind the requirements of the Evidence Act as regards the admissibility of documents via computer evidence.

[75] See CDD paragraph 26 and FATF Recommendation 10.
[76] See FATF Recommendation 10

98. In circumstances where the records relate to on-going investigations by the law enforcement authorities, or to transactions that have been the subject of a disclosure order, they should be retained beyond the five-year minimum period and until it has been confirmed by the Designated Authority that the case has been concluded and further retention is unnecessary.

In this regard, institutions that have made suspicious transaction reports to the Designated Authority must make it a point of duty to follow up with the Designated Authority for guidance on how future business with the accounts/ account holders in question must be conducted. For these purposes institutions are cautioned to make every effort to also retain copies of all reports made to the Designated Authority for at least the minimum five-year period.

SECTION V – TRANSACTION MONITORING AND REPORTING

REPORTING OBLIGATIONS AND THE APPOINTMENT OF COMPLIANCE OFFICERS

99. **Appointment of Compliance Officers**[77]. A financial institution must designate an officer of the institution who performs management functions as its "Compliance Officer", to be responsible for ensuring the effective implementation of the established policies, programmes, procedures and controls to prevent and detect money laundering and terrorist financing activities in accordance with the relevant statutes, the BOJ Guidance Notes and the licensee's own policies and procedures. That officer should be responsible for reporting to the Designated Authority, all such activities as required by the relevant statutes and the Guidance Notes, and should be in a position to provide advice and guidance to the staff of that institution, on the identification of suspicious transactions (See Appendix III - List of the Basic Duties and Responsibilities of the Compliance Officer).

100. In this regard, the licensee's policy manual should require the preparation and submission of a comprehensive report by the Compliance Officer to the Board of Directors at least on an annual basis. This report should, at a minimum include an overview and evaluation of the overall effectiveness of the entity's AML/CFT framework, as well as the effectiveness of AML/CFT measures implemented under each of the various operational areas and/or product and service types. This would include details such as: -

- The entity's compliance with relevant legislation and BOJ's Guidance Notes;
- Number and frequency of threshold and suspicious transactions/activities detected and reported to the FID;
- Any significant and/or unusual trends in evidence arising from a review of transactions detected and reported (e.g. trends in relation to specific branches, geographic areas – local and/or overseas, or types of transactions);

[77] See MLA section 7(3)

- Report on the entity's compliance in relation to customer due diligence standards as set out in the Guidance Notes as well as the entity's own policy;

- Report on the entity's success/level of compliance in updating its customer records for pre-existing customers;

- Report on the findings of the annual AML/CFT audits undertaken by the institution's external and internal auditors, and findings emanating from reviews by BOJ examiners;

- Steps that have been taken to effectively address AML/CFT weaknesses identified by the BOJ Examiners, the entity's external as well as internal auditors and/or compliance unit;

- Detailed assessment of effectiveness of monitoring of high-risk customers and information as to any challenges posed by that area of the entity's operations;

- Update on programmes employed over the reporting period for ensuring employee awareness and integrity - including training programmes for staff, and the effectiveness of such programmes;

- Update on the institution's overall relationship with the Designated Authority and general guidance received from that quarter;

- Advice on any proposed/impending legislative/regulatory changes as regards AML/CFT, with an assessment of how the institution will be impacted and advice as to how necessary operational changes will be implemented to ensure continuing adherence by the institution.

This report will be subject to review by the Supervisory Authority.

RECOGNITION AND REPORTING OF UNUSUAL/SUSPICIOUS TRANSACTIONS

101. A suspicious transaction will often be inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account. Hence, general knowledge of the nature of the industry/sector in which the customer operates and the nature and pattern of the customer's own business is the first element in recognizing an unusual transaction, or series of transactions.

101. A. Section 6.B (1) of the MLA[78] states that:-

*"A financial institution shall, in relation to each customer, **pay special attention** to all complex, unusual or large business transactions, or unusual patterns of transactions whether completed or not, which appear to the financial institution to be inconsistent with the normal transactions carried out by that customer with the institution."*

Section 16 of the TPA states that:-

*"An entity shall, in relation to each customer, **pay special attention** to all complex, unusual or large business transactions, or unusual patterns of transactions whether completed or not, which appear to the entity to be inconsistent with the normal transactions carried out by that customer with the entity."*

The term *"pay special attention to"* as used in MLA section 6B(1) and as used in Section 16 of the TPA should be interpreted to mean the examination of the background and purpose of these types of transactions, the formal recording of the institution's findings and the retention of these findings for a period not less than five (5) years. As regards the obligation for retention of records, institutions should also be guided by paragraphs 94 – 98 of these Guidance Notes.

Financial Institutions must also be in a position to make their findings in this regard available to the Bank of Jamaica, especially in regard to the Bank of Jamaica's on- site examinations which will continue to include an assessment of institutions' AML/CFT systems. Such findings should also be available to the auditors of the financial institution.

[78] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA.

Financial institutions are reminded that an institution's failure or inability to comply in this regard will constitute unsafe or unsound practices in accordance with the Banking Act/ Financial Institutions Act or BOJ (Building Societies) Regulations (as the case may be). (See paragraph 7 of these Guidance Notes). Failure in that regard will also be considered a breach of that institution's statutory obligations under the Money Laundering Act (MLA)[79], the Regulations issued there-under and the Terrorism Prevention Act. Deficiencies in the systems, which place the institution in breach of its obligations under the governing statutes will be reported to the Designated Authority.

102. There are certain categories of activities that are suspicious by their very nature, and should alert a financial institution as to the possibility that a customer is seeking to conduct illegal activities at/through the institution. Examples of such suspicious conduct and activities are outlined in Appendix I. This listing is not intended to be exhaustive, and only provides examples of the most basic ways by which money may be laundered and should act as a catalyst for prompting enquiries about the source of funds. Financial institutions should also keep themselves informed as to the constantly evolving methods (i.e. typologies) of money laundering. Financial institutions should note that under the MLA, predicate offences include "any offence involving fraud, dishonesty or corruption". (See the MLA[80] Schedule 1- paragraph 5) This means that STRs should also be made in cases where there is suspicion that the transaction being conducted is facilitating theft of funds; funds received through insider trading activities; funds diverted to avoid the payment of taxes or to otherwise deprive the Government of revenues; funds comprising bribes or diversion of public funds and so forth.

103. Financial institutions should have adequate systems in place to ensure the timely, ongoing detection and reporting of unusual, suspicious and threshold transactions and bring these to the attention of the relevant authorities.

[79] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA.
[80] See footnote 79 above

Suspicion-Based and Threshold Reporting Procedures

104. The reception point for disclosures under the MLA (whether these are suspicion-based reports or reports of transactions at or above threshold limits) is the Designated Authority. The Division in the Ministry of Finance, which has responsibility for matters related to anti-money-laundering and combating the financing of terrorism is the Financial Investigations Division (FID). An obligation to report to the Compliance Officer transactions which breach the provisions of the MLA or MLR is placed on the person who first notes the breach of threshold limits or suspects that a transaction involves property derived from illegal activities. The obligation will then lie with the Compliance Officer to file the necessary report to the Designated Authority. Similarly under the TPA there is an obligation to report unusual, complex etc transactions. There is also an obligation to make quarterly reports as to whether the institution is in possession of property for a listed entity. Financial institutions also need to ensure that the requisite Money Laundering Reporting Forms are properly completed to facilitate the investigatory process that may be undertaken as a consequence of the report. As regards reporting obligations under the TPA, until the required reporting format is settled by the issue of the Regulations under the TPA, the guidance at paragraph 22H above entitled "Transitional Guidance" should be consulted.

105. Financial institutions should establish systems that require all suspicious and threshold transactions to be brought to the attention of supervisory management (branch or departmental manager). Each case must then be reviewed at that level to determine whether the suspicion is justified, and in the absence of factual information to negate the suspicion, the Compliance Officer should be informed, who must then immediately submit a report to the Designated Authority. The specific steps that must be followed for the reporting of such transactions must be clearly outlined in the policy manual and communicated to all relevant personnel. The following must also be noted: -

(a) The MLR provides for the use of a standard reporting format[81], which must be adopted. Reporting formats under the TPA will be effected with the passage of the Regulations under the TPA. Until the required reporting format is settled

[81] See MLR regulation 12

by the issue of the Regulations under the TPA, the guidance at paragraph 22H above entitled "Transitional Guidance" should be consulted and adhered to;

(b) Once a suspicious transaction report is acknowledged by the Designated Authority, that office may give written consent for the continued operation of the customer's account;

(c) The Designated Authority may also apply for appropriate Monitoring Orders, and deal with other legal processes necessary to carry out further investigations. The reporting institution concerned will be advised in circumstances where a monitoring order has been obtained. Institutions are expected at all times to co-operate with the law enforcement authorities;

(d) Access to disclosed information is restricted to the investigating officers of the Designated Authority and the prosecuting personnel;

(e) **A financial institution is under strict obligations not to disclose to any person, the fact that it has made a report to the Designated Authority and must comply with all directions given to it by the Designated Authority.** Directors and employees of a financial institution, which report a suspicious or threshold transaction are exempt from any criminal, civil or administrative liability for breach of any restriction on disclosure of information imposed by contract, or by any legislative, or administrative requirement.

106. A financial institution should decline to do any business (including opening an account) with a potential customer if there are serious doubts about the bona fides of the individual or criminal involvement is suspected. Where criminal involvement is suspected, the financial institution should however, seek to retain copies of relevant identification or other documents, which may have been presented, and should consider reporting the offer of suspicious funds to the Designated Authority (Refer to FATF Recommendation 5). Where a business relationship has already commenced and the customer fails to provide requested follow-up information, the relationship should be legally terminated unless otherwise advised by the law enforcement authorities. (See paragraph 45.) In seeking to terminate the relationship, financial institutions should be careful not to "tip off" customers or potential customers where a suspicion has been formed by the financial institution that an offence is being attempted or has been or is being committed. Financial institutions should also be mindful of paragraph 105(e) above in relation to tipping off a customer that a report has

been made to the Designated Authority or that an investigation is being conducted. Under the MLA[82] and TPA[83] the latter unauthorised disclosure amounts to an offence.

106A. Where an institution forms the suspicion that criminal activity is taking place after a business relationship is established with a customer, the institution should seek to legally terminate arrangements where it is of the view that continuing the relationship could lead to legal or reputational risks due to the suspected criminal activity. (See paragraph 45(A). See also paragraph 69 for guidance on transactions that though not suspicious, raise questions or are flagged for closer scrutiny and which in that case are still conducted.)

Monitoring Orders

107. The Designated Authority may apply for a "Monitoring Order"[84] directing a financial institution to disclose information, and/or a "Production Order"[85] directing a financial institution to produce documents, concerning transactions conducted through an account held with that institution.

108. A financial institution must not disclose the existence of a monitoring order to any person, except to:

- an officer or agent of the institution, solely for the purpose of ensuring that the order is complied with; or,

- an attorney-at-law for the purpose of obtaining legal advice or representation in relation to the order.

In these circumstances, the financial institution is under a duty not to disclose the existence or operation of the monitoring order to any other person except an officer of the institution for the purpose of compliance with the order, or an attorney-at-law for the purpose of obtaining advice or representation. Licensees experiencing some difficulty reconciling this aspect of the law with the regulator's entitlement to full access of their records should note that the situation now is that under the MLA the above obligation stands. However under the financial legislation the regulator may

[82] See section 6C. (NB Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA.)
[83] See section 17
[84] See MLA section 8 and DOFPA section 44
[85] See DOFPA section 38

have access to the records including those indicating the existence of a monitoring order and the customer to whom it relates. The regulator however will not insist on taking copies of records of this nature, but will only exercise the access to the records sufficient to satisfy the regulator that a licensee is complying with its statutory obligations under the MLA.

SECTION VI - EMPLOYEE INTEGRITY AND AWARENESS

INTRODUCTION

109. The success of the AML and CFT programme depends to a large extent on the integrity of employees, and as such, financial institutions should establish and implement appropriate policies and procedures[86] to ensure that employees are "fit and proper" persons.

110. To this end, potential employees should be subject to a comprehensive screening process, which should involve a thorough investigation of the potential employee's background, honesty, competence and integrity.

111. Financial institutions should also institute processes geared towards ensuring the continued maintenance of a high level of integrity and competence among staff. These may include: -

(i) Establishment of a Code of Ethics to guide employee conduct;

(ii) Regular review of employee's performance and adherence to internal policies and procedures including codes of conduct and AML/CFT requirements;

(iii) Imposition of appropriate disciplinary actions for breaches of the institution's AML and CFT policies; and

(iv) Close scrutiny and investigation of employees whose lifestyles cannot be supported by his or her known income.

[86] See MLA section 7(2)(a)

EDUCATION AND TRAINING[87]

112. In order to ensure full implementation of the procedures, recommendations, and requirements contained in these Guidance Notes, the staff of financial institutions must be made fully aware of the background against which the Guidance Notes have been issued, and the serious nature of money laundering crimes and terrorism financing activities. Furthermore, efforts must be made to ensure that all staff understands the basic provisions of the MLA[88], MLR and TPA.

113. Members of staff must also be sensitised as to their personal obligations under the MLA and the TPA and the fact that they can be held personally liable for failing to report relevant information to the Designated Authority, or otherwise failing to carry out their responsibilities under the relevant statutes.

114. All financial institutions must therefore introduce programmes to ensure that all members of staff, at all levels of the organization, are informed of their responsibilities, and encouraged to provide prompt notification of suspicious as well as threshold transactions. Training/education programmes must be designed to clarify responsibilities and to provide sufficient guidance for staff to identify and provide prompt notification of suspicious as well as threshold transactions. Training/education programmes must be designed and implemented on an ongoing basis by individual institutions to ensure employees' awareness of: -

- Current as well as new and developing AML and CFT laws, regulations, standards and guidelines being established both locally and internationally;
- Their legal obligations and responsibilities to prevent and detect money laundering and terrorism financing;
- New money laundering and terrorism financing techniques, methods, typologies and trends;
- The institution's own AML and CFT policies and procedures.

In developing education and training programmes[89], particular emphasis needs to be placed on the following categories of staff:

[87] See MLA section 7(2)(c) and MLR regulation 3(1)(b)
[88] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA.
[89] See FATF Recommendation 15 and CDD Paragraphs 56 and 57

a) **New Employees.** All new employees, irrespective of their level of seniority, should be informed as to the background and nature of money laundering and terrorist financing and the need for reporting suspicious and threshold transactions to the Designated Authority, through the institution's Compliance Officer. They should be made aware of their personal legal obligation as well as that of the institution, to report suspicious transactions. As mentioned above, institutions should also institute appropriate screening processes so as to thoroughly investigate the background, honesty, and integrity of prospective employees.

b) **Front Line Staff**. The first point of contact of an institution with potential money launderers or persons attempting to finance terrorist activities is usually through staff who deal directly with the public. 'Front-line' staff members (such as Tellers, Cashiers and Foreign Currency Staff) should therefore be provided with specific training on examples of suspicious transactions and how these may be identified. They must also be informed about their legal responsibilities and the institution's reporting systems and procedures to be adopted when a transaction is deemed to be suspicious. Additionally, they must be informed as to the institution's policy for dealing with occasional customers and 'one-off' transactions, particularly where large cash transactions are involved.

c) **Account Opening/Customer Service Staff**. Members of staff who deal with account opening or the approval of new customers must receive the training given to tellers etc. in (b) above. They should also be trained as to the need to verify the identity of a customer and the institution's account opening and customer verification procedures. They must further be advised that a business relationship or 'one-off' transaction should not be established or continued until the identity of the customer is verified. Staff should also be made aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the appropriate Compliance Officer, whether the funds are accepted or not, or the transaction proceeded with, or terminated.

d) **Administration/Operations Supervisors and Managers**. A higher level of instruction covering all aspects of money laundering procedures should be

provided to persons with the responsibility for supervising or managing staff. Such training must include familiarization with the offences and penalties arising under the MLA[90], the DOFPA[91], and the TPA, the procedures relating to monitoring orders and production orders, the requirements for non-disclosure and for retention of records, and management's specific responsibility vis-à-vis dealings with 'high risk' customers.

[90] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA.
[91] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the DOFPA.

SECTION VII - COMPLIANCE MONITORING

Internal Compliance Programme

115. An effective internal compliance programme is essential to a financial institution's endeavour to comply with the law and international best practice standards and prevent involvement in illicit activities.

116. The MLA[92] and the TPA specifically require that financial institutions make arrangements for an independent audit, in order to ensure that the programmes itemized in these Guidance Notes and adopted in policy manuals, are being implemented. An officer at the senior management level must have explicit and ultimate responsibility for the financial institution's internal compliance program, which at a minimum would involve: -

(a) Establishment of an adequately resourced unit responsible for day to day consideration and monitoring of compliance;

(b) Establishment of a strong compliance plan that is approved by the Board of Directors of the institution and that provides for ongoing independent review and testing of staff's compliance with AML and CFT requirements;

(c) Proactive follow-up of exceptions to ensure that timely corrective actions are taken;

(d) Regular reporting of compliance levels, including exception reporting to senior management. Senior management should also be made aware of any corrective measures being implemented;

(e) Regular consultation with the Designated Authority to ensure that the institution is carrying out its obligations under the law.

[92] Once the Proceeds of Crimes Act (POCA) comes into effect it will replace the MLA.

SECTION VIII - CONCLUSION

117. These Guidance Notes are intended to bring to the attention of financial institutions, the **minimum standards** required of an effective programme to detect and deter money laundering and terrorist financing. The Supervisory Authority wishes to emphasize that the AML and CFT policies and procedures of financial institutions should be developed in accordance with the law and these Guidance Notes inclusive of Appendices, giving consideration to each institution's own internal procedures, practices and personnel structures.

SECTION IX - APPENDICES

Appendix I Examples of Unusual/Suspicious Activities

PROVISION OF INSUFFICIENT OR SUSPICIOUS INFORMATION

Cash Transactions

a) Cash deposits which are not consistent with the business activities of the customer.

b) Increases in cash deposits of the customer without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

c) Unusually large cash deposits by a customer whose ostensible business activities would normally be generated by cheques and other instruments.

d) Cash deposits by a customer, by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

e) Requests for the exchange of large quantities of low denomination notes for those of higher denomination.

f) The transfer by a customer of large sums of money to or from overseas locations with instructions for payment in cash.

g) Frequent exchange of cash into other currencies.

h) The constant pay-in or deposit of cash by a customer to cover requests for financial institutions drafts, money transfers or other negotiable and readily marketable money instruments.

i) Large cash deposits using night depository facilities, thereby avoiding direct contact with financial institution staff.

j) Company accounts whose deposits and withdrawals are by cash rather than the forms of debit and credit normally associated with commercial operations (for example, cheques, Letters of Credit, Bills of Exchange, etc.).

Operation of Accounts

a) The use of a number of trustee or clients' accounts which do not appear consistent with the customer's type of business, including transactions which involve nominee names.

b) Increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts especially if the deposits are promptly transferred between other client company and trust accounts.

c) Large number of individuals making payments into the same account without an adequate explanation.

d) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

e) Matching of payments out with credits paid in by cash on the same or previous day.

f) Paying in large third party cheques endorsed in favour of the customer.

g) High account turnover inconsistent with the size of the balance (suggesting that funds are being "washed" through the account).

Additional Considerations for Transactions Involving Terrorist Financing

a) Accounts that receive relevant periodic deposits and are dormant at other periods;

b) A dormant account with a minimal sum suddenly receiving a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed;

c) Customer refuses to provide information required by financial institution, or attempts to reduce the level of information provided or to provide information that is misleading or difficult to verify;

Investment Related Transaction

a) Purchasing of securities to be held by the financial institution in safe custody, where this does not appear appropriate given the customer's apparent standing.

b) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

c) Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customers' apparent standing.

Off-Shore International Activity

a) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

c) Regular and large payments by customers, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receipt of regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs or money laundering, or which are regarded as tax havens.

d) Unexplained electronic fund transfers by customers on an in-and-out basis and without passing through an account.

Secured and Unsecured Lending

a) Customers who repay problem loans unexpectedly.

b) Requests to borrow against assets held by the financial institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

c) Requests by customers for a financial institution to provide or arrange financing where the source of the customer's financial contribution to the transaction is unclear, particularly where property is involved.

d) Requests for loans to offshore companies, or loans secured by obligations of offshore financial institutions.

e) Customers purchasing certificates of deposit and using them as loan collateral.

Appendix II Customer Due Diligence for Banks issued for Basel Committee for Financial Banking Supervision

http://www.bis.org/publ/bcbs85.htm

General Guide to Account Opening and Customer Identification

Appendix III – Basic Duties and Responsibilities of the Compliance Officer

The "Compliance Officer" should be responsible for day-to-day monitoring of the financial institution's compliance with AML/CFT laws, regulations and industry best practices. The officer should possess the requisite skills, qualification and expertise to effectively perform the assigned tasks; and most importantly, he/she should have access to all operational areas and report independently to the board. This duty must be independent of the internal audit function.

The duties and functions of the Compliance Officer should at a minimum include, inter alia, the following:

1. Act as liaison between the financial institution and the Bank of Jamaica and law enforcement agencies (FID, DPP, etc) with respect to compliance matters and investigations;

2. Evaluate new products and services to determine the level of risk(s);

3. Evaluate reports of suspicious/unusual transactions by bank personnel and ensuring the timely filing of Suspicious Activity Reports;

4. Coordinate with financial institution's audit, legal and security departments on AML matters and investigations;

5. Prepare report to Senior Management, Board of Directors at least on an annual basis on the effectiveness of the AML/CFT framework. (This report should be subject to review by the Bank of Jamaica);

6. Advise business units of proposed or pending regulatory changes;

7. Prepare and update policies and procedures and disseminate information to financial institution personnel;

8. Assist in implementing compliance programmes;

9. Oversee administrative matters related to Code of Conduct and Compliance with Anti-money Laundering and Terrorist Financing Activities; and

10. Develop training material and coordinate anti-money laundering training.

Appendix IV FATF Forty Plus Nine Recommendations on Money Laundering and Terrorist Financing

The 40 Recommendations of the FATF on Money Laundering (MF)

9 Special Recommendations (SR) on Terrorist Financing (TF)

Appendix V - CFATF Nineteen Recommendations on Money Laundering

Caribbean Financial Action Task Force

Appendix V.A. – Amendments Made to the Guidance Notes between 2004 and 2006

APPENDIX VA (I)

LIST OF AMENDMENTS TO
THE
BOJ REVISED AML/CFT GUIDANCE NOTES

1. **Paragraphs 1, 6, 7, 8, 9, 11** no longer refer to the Terrorism Prevention Bill but now refer to the Terrorism Prevention Act (TPA) and the passage thereof.

2. **Section III** – Legislative and Regulatory Framework - has been adjusted to include discussions on the Terrorism Prevention Act. This section therefore now incorporates eight new paragraphs (22A-H) which briefly highlight certain provisions in the Terrorism Prevention Act that will directly impact the operations of financial institutions. The sections highlighted include -

   Section 4 TPA - Providing, making available etc. property or services for terrorist purposes.

   Section 5 TPA - Using or possessing property for terrorist purposes.

   Section 6 TPA - Dealing in property for terrorist purposes.

   Section 15 TPA - Duty of entities to report.

   Section 16 TPA - Duty to report suspicious transactions.

   Section 17 TPA - Unauthorized disclosures.

   Section 18 TPA - Regulatory controls by certain entities.

   Section 19 TPA - Monitoring orders.

3. **Paragraph 92** - Funds Transfers – The guidance on funds transfers has been expanded to:-

   i) include FATF definitions of "originator" of funds transfers;
   ii) include FATF definitions of "wire transfers" and "funds transfers";
   iii) remind financial institutions that KYC processes are applicable for transactions of this nature before the business relationship is commenced; to existing customers and otherwise, where appropriate.

4. **Paragraph 100A** – This is a new paragraph that has been inserted in the Guidance Notes and constitutes the expansion of the guidance issued on suspicious transactions. Included in this guidance is an indication that the term "pay special attention to " as used in section 6B of the MLA should be interpreted to mean the examination of the

background and purpose of these types of transactions, the recording of the institutions' findings and the retention of these findings for a period not less than five years.

APPENDIX V.A. (II)

LIST OF AMENDMENTS AND NEW AREAS COVERED UNDER THE BOJ REVISED AML/CFT GUIDANCE NOTES

1. Guidance Notes –front page

   Reflects the issue date for the revised Guidance Notes of February 2005.

2. Guidance Notes Paragraph 1 – page 5 and page 71

   Clarification made in respect of the history of the dates of issuance of AML Guidance Notes by the Bank of Jamaica ("the Bank") to the industry.

3. Guidance Notes Paragraph 7 – page 7

   Insertion to confirm amendments to the financial legislation which will permit regulatory sanctions including licence suspension and/or licence revocation for non-compliance with the MLA, MLR and any other statute which imposes obligations on a financial institution.

   Paragraph 7 was also amended to reflect that regulatory sanctions for non-compliance with the MLA, MLR and any other statute, which imposes obligations on a financial institution, can also be taken against building societies.

4. Guidance Notes Paragraph 17 – page 12
   Insertion of correct reference to the FATF (CFT) Recommendations so that the paragraph refers to the FATF 'Special Recommendations' on CFT.

5. Guidance Notes Paragraph 31 – pages 20, 21 and 22
   Insertion made to alert financial institutions to Jamaica's specific international obligations under U.N. Resolution 1373 (2001) and the U.N. International Convention for the Suppression of the Financing of Terrorism (1999).

6. Guidance Notes Paragraph 31A – page 22

This is the previous paragraph 31 which is now renumbered accordingly and amended to include the FATF **Ninth Special Recommendation on the detection and prevention of terrorist financing.** This additional area has to do with 'cash couriers' a service FATF sees as presenting increasingly significant opportunities for the laundering of money. This Ninth Recommendation requires countries to have measures in place to detect the physical cross border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation. This Recommendation was formally incorporated in the FATF CFT Special Recommendations in 2005.

7. Guidance Notes – Appendix IV

This is a consequential amendment to the Appendix to refer to the FATF 40 + 9 Recommendations.

8. Guidance Notes Paragraph 48(a) – page 32

The reference in the listing of acceptable identification to 'drivers licences' was amended to delete the requirement that these licenses be issued by the authorities in the parish in which the licence was obtained. This requirement now only speaks to the drivers licence tendered being one which is issued by the authorities in the country in which the person is resident".

9. Guidance Notes Paragraph 59 – pages 37 and 38

Definition inserted of the term 'repeat customer' in relation to transactions conducted with cambios and remittance companies.

10. Guidance Notes Paragraph 61 – page 38

Correction made to reflect that 'de minimus' transactions constitute transactions amounting to or exceeding US$250.00 (or the equivalent in other currencies). This amendment brings this wording in line with the proposed position in relation to 'de minimus' transactions that is contained in the draft amendments to the Money Laundering Regulations.

11. Guidance Notes Paragraph 63 – page 41

This paragraph now includes additional guidance to cambios and remittances that 'source of funds' details need not be obtained from 'Authorized Dealers or cambios' operating in the capacity of 'applicant for business'. (This position is taken given the nature of the services provided by cambios.)

Correction also made to amend the reference to transactions exceeding US$1,000 so that same includes the clarifying words ("or its equivalent in other currencies").

Guidance Notes Paragraph 63 – page 44
Clarification of the compliance expected of cambios in relation to the implementation of "KYC" due diligence procedures for corporate customers has been inserted.

Clarification of the compliance expected of remittance companies in relation to the implementation of "KYC" due diligence procedures in relation to inbound transactions has been inserted. The requirement that identifications be photocopied is therefore applicable only in respect of outbound transactions.

12. Guidance Notes Paragraph 66 – page 42
Clarification of the compliance expected of remittance companies in relation to their acceptance of school identifications when disbursing inbound transactions. (This position is taken given the nature of the services provided by remittance companies and the extent by which their services are used to remit funds for the maintenance of persons attending high/secondary schools and tertiary institutions.)

13. Guidance Notes Paragraph 69 – page 44
Clarification inserted to reflect that transactions of the nature discussed in this paragraph should be reported to the 'designated authority'.

14. Guidance Notes Paragraph 106A – page 62
This paragraph was amended to synchronize the respective guidance stated in relation to suspicious transactions and transactions red flagged for higher scrutiny at paragraph 69 of the Guidance Notes.

APPENDIX VA (III)

LIST OF AMENDMENTS TO THE BOJ REVISED AML/CFT GUIDANCE NOTES

1) Guidance on procedures to combat the financing of terrorism. Please note that these procedures will also be applicable as of the 31 August 2004 notwithstanding the fact that the Terrorism Prevention Bill (TPB) has not been passed into law. Compliance with the Guidelines in this respect will therefore now form part of the BOJ's onsite examination process;

2) International anti-money laundering/combating of the financing of terrorism (AML/CFT) regulatory requirements and best practices such as the Forty Plus Eight Recommendations of the Financial Action Task Force (FATF) issued in 2003 as well as the Best Practice Standards for Customer Due Diligence Procedures issued by the Basel Committee on Banking Supervision;

3) Inclusion of enhanced identification requirements when dealing with high risk customers, accounts opened by intermediaries, politically exposed persons (PEPs) and countries with inadequate AML/CFT frameworks;

4) More detailed guidance/directives as regards record-keeping, monitoring and compliance standards as well as employee integrity and awareness;

5) Insertion of a new section that provides guidance for these operations (refer to Section IV (B) of the Guidance Notes).

6) Further revisions have also been made to address various issues raised by the industry. In this regard, particular attention must be paid to the following areas: -

   - Know-Your Customer procedures (see Section IV)

   - Transaction Monitoring and Reporting (Section V), which has included greater details regarding the role of the Compliance Officer.

   - The insertion of two additional Appendices to detail the Duties and Responsibilities of Compliance Officers and to attach Extracts from the 2003/4 AML/CFT Typologies Exercise Covering Wire Transfers, Non-Profit Organizations, Politically Exposed Persons and Gatekeepers.

Appendix VI. Extracts From the FATF 2003/2004 AML & CFT Typologies Exercise Covering Wire Transfers, Non-Profit Organizations, Politically Exposed Persons and Gatekeepers

Executive summary of observations[93]

1. The FATF's 2003/2004 typologies exercise focused on the following topics: Wire transfers and non-profit organisations (NPOs) and their links to terrorist financing, politically exposed persons (PEPs) and gatekeepers.

2. Wire transfers are a fast and efficient way of moving funds, thus they can also be used for terrorist purposes. Complex wire transfer schemes can be used to create a deliberately confusing audit trail to disguise the source and destination of funds destined for terrorist use. Currently, there a limited number of indicators to help identify potential terrorist wire transfers – primarily the source and destination of the funds and the names of the individuals involved when this information is available. It was acknowledged during this year's exercise that there was a need to identify further information to develop potentially suspicious transactions.

3. The examination of terrorist misuse of NPOs found that the diversion of a very small volume of the funds can represent a potentially serious terrorist financing problem. Various categories of non-profit organisations were recognised, and within each category an associated set of risk profiles began to be identified. Although most governments have some kind of regulation and oversight of the NPO sector, additional measures are likely to be necessary to reduce the misuse within the sector. The experts concluded that there was a need to develop and enhance mechanisms and gateways for information sharing to counter the terrorist financing risk.

4. PEPs are individuals who are or have been in the past entrusted prominent public functions in a particular country. New revelations of suspected PEPs' involvement in financial crime – especially as related to corruption – occur frequently in the press. PEPs, when involved in criminal activity, often conceal their illicit assets through networks of shell companies and off-shore financial institutions located outside the PEPs' country of origin. PEPs were noted as frequently using middlemen or family members to move or hold assets on their behalf. The techniques used by PEPs to hide assets are similar to those of money launderers. Financial institutions may thus be able to detect potential illegal activity of PEPs by applying enhanced due diligence methods similar to those used for countering money laundering.

5. Increasingly, money launderers seek out the advice or services of specialised professionals to help facilitate their financial operations. This trend toward the involvement of various legal and financial experts, or gatekeepers, in money laundering schemes has been documented previously by the FATF and appears to continue today. The work undertaken during the 2003/2004 exercise confirmed and expanded the FATF's understanding of specific characteristics of this sector and what makes it vulnerable to money laundering. A key conclusion of the experts was that many of the risks and vulnerabilities identified for gatekeepers could be reduced if AML/CFT measures were consistently and thoroughly applied.

[93] The full report can be accessed at the FATF's website at www.fatf-gafi.org.

INTRODUCTION

6. Money laundering and terrorist financing are two types of financial crime with devastating effects that go beyond seemingly innocuous financial transactions. From the profits of the low-level narcotics trafficker to the assets looted from State coffers by dishonest government officials, criminal proceeds have the power to corrupt and ultimately destabilise communities or whole national economies. Terrorist networks are able to carry out their insidious activity – on a global scale and in places that could once be considered immune to such phenomena – through their undetected financial support structures. In both instances, criminals or terrorists are able to exploit loopholes or other weaknesses in the legitimate financial system to launder criminal proceeds and to support terrorist activity.

7. The Financial Action Task Force (FATF) holds an annual exercise to examine the methods and trends – the typologies – of money laundering and, since 2001, of terrorist financing. The primary objective of this work is to obtain material that will help the FATF policy makers develop and refine anti-money laundering and counter-terrorist financing (AML/CFT) standards. In addition, the findings obtained from the annual exercise serve as the basis for informing a wider audience – regulatory authorities, law enforcement agencies and financial intelligence units (FIUs), as well as the general public – on the characteristics and trends of money laundering and terrorist financing.

8. Each year, the FATF typologies exercise focuses on a series of topics or themes that were agreed to by the FATF Plenary. The Plenary attempts to select topics according to the current work of the body or to follow up on methods or trends identified in previous typologies exercises. Five topics were therefore chosen for this year. Examining the terrorist financing links with wire transfers and these same links with non-profit organisations (NPOs) were two of the topics of the FATF-XV exercise. They follow up on earlier typologies work, as well as provide material to support further refinement of the guidance issued by the FATF for the Eight Special Recommendations on terrorist financing. The FATF also looked at the money laundering risks associated with politically exposed persons (PEPs) and with specialised financial advice providers or "gatekeepers" as the last two topics. With the issue of the revised FATF Forty Recommendations in June 2003, there are now measures that apply with respect to PEPs and gatekeepers; therefore, this year's typologies work was intended to provide additional information on the nature and scope of the threat for these two areas.

9. This report on the FATF-XV typologies exercise describes key conclusions for each of the subject areas as they have been developed. As is the usual practice of the FATF, the report includes case examples taken from written contributions and presentations made during the meeting. The texts of these examples are reproduced here – wherever possible – as they were submitted for the exercise. However, country names, currencies and certain other details have been modified in order to protect sensitive aspects of any cases cited here.

WIRE TRANSFERS AND THEIR RELATION TO TERRORIST FINANCING

10. Terrorists use wire transfers to move funds intended for the financing of their activities. The financial support structure revealed after the September 11th attacks in the United States showed the essential role played by wire transfers in providing the hijackers with necessary financial means to plan for and eventually carry out their attacks.[94] It was this use of wire transfers that the FATF had in mind when it issued Special Recommendation VII in October 2001. In order to consolidate information on the characteristics and role of wire transfers in terrorist financing, the FATF chose this as the focus for the first of the workshops held during this year's meeting of experts on typologies.

11. When the FATF uses the term *wire* or *funds transfer*, it is referring to any financial transaction carried out for a person through a financial institution by electronic means with a view to making an amount of money available to a person at another financial institution. In some cases, the sender and receiver could be the same person.[95] Wire transfers include transactions that occur within the national boundaries of a country or from one country to another. Given that wire transfers do not involve the actual movement of currency, they are a rapid and secure method for transferring value from one location to another.

12. Payment systems at both inter-financial institutions and retail level now provide better coverage and efficiency for both domestic and cross-border wire transfers. The continuing development of world-wide networks such as SWIFT has enhanced the reliability and efficiency of inter-financial institutions payment systems allowing a large number of transactions to be processed daily. Within the retail financial institutions sector, services such as telephone and internet financial institutions allowing customers to execute transactions on a non face-to-face basis from any location with telephone or internet access.

13. Advances in payment system technology have had a twofold impact in relation to the potential abuse by terrorist financiers and money launderers of such systems. On the one hand, electronic payment systems provide greater security for transactions by permitting an increased ability to trace individual transactions through electronic records that may be automatically generated, maintained and/or transmitted with the transaction. On the other hand, these advances also create characteristics that may be attractive to a potential terrorist or money launderer. For instance, the increased rapidity and volume of wire transfers, along with the lack of consistent approach in recording key information on such transactions, in maintaining records of them and in transmitting necessary information with the transactions, serve as an obstacle to ensure traceability by investigative authorities of individual transactions.

14. A further complication is presented by transfers that take place through non-financial institutions financial institutions such as money remitters, bureaux de change or other similar types of businesses. In some countries, these businesses perform wire transfer functions either directly with counterpart businesses in their own country or abroad or else through conventional financial institutions (i.e. financial institutions). Again, differences in requirements for recordkeeping or transmission of information on the originator of transfers

[94] See the statement of Federal Bureau of Investigation to the US Congress, which was cited in last year's FATF report and is available from http://www.fbi.gov/congress/congress02/lormel021202.htm. The statement contains financial profiles of the September 11th hijackers and mentions the use of wire transfers for moving funds.

[95] See Interpretative Note to SR VII: Wire Transfers.

conducted through such businesses may be used to the advantage of terrorist or other criminals that desire to move funds without being easily detected by authorities.

Typologies

15. The FATF experts recognised that wire transfers are a fast and efficient way of moving funds for terrorist purposes. For example, a simple network for transmitting terrorist funding can be set up merely by taking advantage of the differences in the monitoring regimes of various countries. If no records on the originator of the transaction are kept at the starting point of the wire, or the information is not further transmitted by an intermediary along the way, investigators will thus not have access to information that may help to establish terrorist links.

16. More complicated wire transfer schemes have been observed and can involve multiple wire transfers to create a complex and deliberately confusing trail of financial transactions in order to avoid detection.

17. A few common characteristics were also noted as relevant to the typologies of potential terrorist financing through wire transfers. One important characteristic is the use of false identities, “straw men” or front companies in transactions to provide clean names and thus avoid detection. Another characteristic is to channel funds through several different financial institutions so that the wire transfers appear to come from different and seemingly unrelated sources. There also seems to be some use of wire transfers through non-financial institutions financial institutions or alternative remittance services by terrorists (informal money or value transfer systems) with the idea that avoiding mainstream financial institutions will help terrorist funding – like the proceeds of non-terrorist criminal activity – remain undetected by financial monitoring systems or investigative authorities.

Case 1: Terrorist funds collected in Country A transferred to a terrorist organisation in Country B

A terrorist organisation would make use of its overseas contacts to "tax" the expatriate community on their earnings and savings. The tax would go to a "calling fund" and would then be wired to the representative office, which was also the political wing of the group based in the neighbouring country.

The neighbouring country had a significant cross-border ethnic spread in the “target” country, and weapons and material would be purchased and smuggled across the border into the autonomous province where the terrorist organisation carried out its attacks.

Case 2: A terrorist organisation uses wire transfers to move money to further its activities across borders

A terrorist organisation in Country X was observed using wire transfers to move money in Country Y that was eventually used for paying rent for safe houses, buying and selling vehicles, and purchasing electronic components with which to construct explosive devices. The organisation used "bridge" or "conduit" accounts in Country X as a means of moving funds between countries. The accounts at both ends were opened in the names of people with no apparent association with the structure of terrorist organisation but who were linked to one another by kinship or similar ties. There were thus the apparent family connections that could provide a justification for the transfers between them if necessary.

Funds, mainly in the form of cash deposits by the terrorist organisation were deposited into financial institutions accounts from which the transfers are made. Once the money was received at the destination, the holder either left it on deposit or invested it in mutual funds where it remained hidden and available for the organisation's future needs. Alternatively, the money was transferred to other financial institutions accounts managed by the organisation's correspondent financial manager, from where it was distributed to pay for the purchase of equipment and material or to cover other ad hoc expenses incurred by the organisation in its clandestine activities

Case 3: Wire transfers are used as part of a terrorist fundraising campaign

An investigation in Country A of Company Z, a company thought to be involved in the smuggling and distribution of pseudoephedrine (a suspected source of revenue for terrorist organisations), revealed that employees of Company Z were sending a large number of negotiable cheques to Country B. Additional evidence revealed that the target business was acting as an unlicensed money remitter. Based on the above information, search warrants were obtained for the Company Z premises and two residences. Analysis of the documents and financial institutions records seized as a result of the search warrants indicated that the suspects had wire transferred money to an individual with suspected ties to a terrorist group.

Later that year the investigators engaged in a series of co-ordinated searches. Three subjects were arrested and charged for failure to register as a financial business, and approximately USD 60,000 in cash and cheques were seized. Additionally, a financial institutions account was identified containing approximately USD 130,000 which was used to facilitate the illegal wire transfers to destinations outside Country A. The subjects are currently awaiting trial.

18. There was agreement among the experts present at this year's meeting that, other than the generally small size of such transactions, the value of individual transfers was generally not a distinctive feature when carried out for terrorist financing purposes. Indeed, the low value of the transfers when compared with the high overall volume of such transactions is an additional factor that further complicates detection of terrorist use of the financial system. Even establishing an average size for terrorist related wire transfers was

impossible, although one delegation reported observing transfers as low as the range of USD 25 to USD 500. A few experts did note, however, that wire transfers often appear to have been structured in amounts below any mandatory reporting requirements.

Case 4: Payments are structured 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. Later an investigation was initiated in relation to Company S based on a suspicious transaction report.

The investigation showed that over the four-year period, Mr. A's business had received over USD 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 financial institutionss in Country X. In order to avoid reporting requirement in effect in Country X, Mr. A and others always deposited the cash with the financial institutionss in sums less than USD 10,000, sometimes making multiple deposits of less than USD 10,000 in a single day.

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

19. Despite these observations made for wire transfers carried out for terrorist financing purposes, the experts reaffirmed the sense that at present investigators and financial institutions still have a limited number of useful types of indicators that help to detect possible terrorist use of wire transfers. In instances when information is available on an individual cross-border wire transaction, often the only factors that may help to link the transaction to terrorism is the name of the originator or beneficiary and the originator or destination location. The size of the transaction does not seem to follow any specific patterns, although the experts believed that they are generally low either because individual instances of terrorist financing may not involve large sums of money or because there is a conscious attempt to send smaller transactions to avoid detection.

Policy Implications

20. Guidance for preventing and detecting the misuse of wire transfers systems by terrorists – and by other non-terrorism related criminals – is set forth in FATF Special Recommendation VII and in the Interpretative Note issued subsequently by the FATF. The Recommendation calls for the recording, maintaining and, in the case of cross-border transfers, transmitting of certain key elements of information on the originator of the transfer. This information, once available at the receiving end of the transfer will enable financial institutions to make initial assessments of potential terrorist / criminal connections (i.e., for purposes of suspicious transaction reporting) and ultimately to FIUs, law enforcement or other competent authorities (i.e., for the initial stages of their analytical or investigative process).

21. The inclusion and retention of meaningful originator information on a wire transfer can assist the fight against terrorist financing and money laundering in several ways. Transactions that contain full information assist beneficiary financial institutions to identify

potentially suspicious transactions. These would require extra diligence and potential onward reporting to an FIU. When reports on unusual or suspicious wire transfers are received by an FIU, those that contain complete information can be more thoroughly researched and analysed. Finally, ensuring that originator information is readily available assists the appropriate law enforcement authorities to detect, investigate and prosecute terrorists or other criminals.

22. While it was not the purpose of the workshop to look at the overall effectiveness or appropriateness of measures called for in SR VII, the general view of participants in the exercise was in support of the measures. **Having "complete and meaningful" information on the originator of a wire transfer message available to financial institutions and competent authorities was deemed as critical to being able to detect or prevent terrorist and criminal use of the wire transfers.**

23. The Interpretative Note to SR VII issued in February 2003 provisionally allows for the existence of *de minimis* thresholds of USD 3,000 with regard to the measures called for in the Recommendation. Thus, although countries must still require the collection and retention of originator information on wire transfers valued below this amount, the transmission of this information with the wire is not required. The experts discussed the issue of having a threshold in connection with the wire transfer measures in SR VII. The majority of experts indicated that wire transfer transactions that are potentially related to terrorism would generally involve small amounts. The consensus of the experts then was that the existence of a threshold for SR VII requirements – from an operational perspective – could hinder the detection of what might be relevant transactions. It was also noted that the lack of a threshold could also serve as a deterrent to the use of wire transfers by terrorists or criminals by making the risk of detection greater.

24. The experts also acknowledged, however, that in the absence of other specific indicators, the lack of a threshold could lead to an excessive number of transactions being reported to the FIU. Reports on individual transactions would perhaps have less value as a means of detecting terrorist financing, although they would still be important in helping to build a picture of financial structures supporting terrorism when detected through other channels (for example, through intelligence reports or investigations conducted by other agencies). **As indicated above, the most important elements in detecting terrorist-related wire transfers at present are the names of the parties involved and the geographical source or destination of the transaction.** The experts agreed, therefore, that more work needs to be done to develop clearer indicators of terrorist use of wire transfers. These indicators could assist financial institutions in identifying the transactions that may require increased scrutiny and ultimately be reported to competent authorities as suspicious or unusual.

25. A potential solution for finding additional indicators would be to encourage the development of information technology systems that could look for objective indicators within wire transfers. One delegation proposed using a system that identifies such indicators based on key words occurring in the wire transfer messages. Establishing a score based on differing values assigned to the key words permits the system to select a smaller pool of transactions that may require further analysis.

NON-PROFIT ORGANISATIONS AND LINKS TO TERRORIST FINANCING

26. The FATF examined the role of non-profit organisations (NPOs) as part of its last typologies exercise (2002-2003). At that time, it was able to make some preliminary findings on the nature of the risk to the sector. In order to expand on this work, NPOs and potential for misuse for terrorist financing purposes was selected once again and became the second workshop topic for this year's exercise. As indicated in the introduction, all three workshops had additional preparation before the experts meeting. The preparation for the NPO workshop, however, was the most extensive of the three workshops, consisting of several small meetings of experts and numerous exchanges of analyses and position papers. For this reason, the NPO workshop was able to obtain a greater degree of detail in its findings which are then reflected in this report.

27. While some countries have relatively extensive experience with terrorism financing through NPOs, other countries clearly have a more limited experience. Only some of the material provided as part of this year's exercise described cases of *proven* terrorist financing. Much of the material therefore related to *suspected* or *possible* terrorist financing — many cases involved investigations that were still ongoing — while a few of the cases dealt with other possible forms of misuse of NPOs.

28. Most countries share the concern over the difficulties in detecting terrorist financing through misuse of NPOs. It is generally acknowledged that such organisations play a crucial social and financial support role in all societies, and obviously this role is not called into question. Nevertheless, the sheer volume of funds and other assets held by the NPO 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 sector should be considered a matter of serious concern for the whole international community.

29. 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 of these organisations have a global presence that provides a framework for national and international operations and financial transactions, often within or near 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

30. The case examples presented during this year's typologies exercise appeared to show that NPOs can be misused in a variety of ways and for different purposes within the framework of terrorism financing. First of all, NPOs can be used by terrorists and terrorist organisations to raise funds, as was the case for many of the larger NPOs that had their assets frozen on the basis of the UN Security Council Resolution 1373 (2001). Often – but not always – these organisations have applied for and received a formal charitable or tax exempt status. Moreover, some of these organisations were 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.

31. A number of the experts noted the importance of *informal cash collection* in many ethnic or religious communities and the difficulties in accurately monitoring those funds. 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 the process is thus a form of money laundering for terrorist purposes.

Case 5: Raising of funds through an NPO

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.

32. NPOs can also be used by terrorists *to move funds.* In this case, terrorists exploit the fact that financial transactions which 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 seem to have been chosen carefully in order to avoid regulation and monitoring (for example, cultural associations established in some countries by indigenous ethnic communities). A few apparently related case examples were cited by several delegations 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 financial institutions 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 6: An NPO is used to transfer money to suspected terrorists

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 on the list conducted its operations under different variations of the same name in a number of countries. It was described as a tax-exempt NPO for which the stated purpose was to conduct humanitarian relief projects throughout the world. Among the multiple locations provided UN list 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 financial institutions 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.

Case 7: NPOs used to make illegal transfers

An on-going criminal investigation into a network of foundations (at least 215 NPOs) established by the members of a particular immigrant community revealed that the network was transferring large sums of money regularly to a few accounts in another country. Suspicious transaction reports from the financial institutionss were triggered by the unusually high amount of the transactions in comparison with the stated purpose and activities of the foundations. After an initial analysis, it became clear that one of the beneficiaries of the transactions carried out by these organisations was a company contained in the UN Security Council list of designated persons. The FIU forwarded the case for further investigation by law enforcement agencies.

Although the stated purpose of these foundations was charitable, the size and frequency of the transfers (both through regular financial institutions accounts and by using money transfer services) were difficult to explain. Over a 3-year period, the 35 NPOs sent over USD 160 million overseas. The network consisted of a sizable number of foundations spread throughout the country, with a concentration in cities with a large presence of the same immigrant community. The ongoing criminal investigation concluded that the NPOs were most likely a cover for an alternative remittance system. Although it is still too early to draw a clear conclusion about the source and destination of the funds of this network, there is at least the possibility that the funds were raised within this immigrant community with the deliberate intent to support terrorist acts.

33. Finally, 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 8: Senior members of an NPO use the organisation to fund terrorism

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.

Categories of misuse

34. An important conclusion from this year's work on NPOs is that various categories of these organisations have different sets of risk profiles and thus vary in the types of unusual characteristics that may be detected and used in identifying terrorist financing. It is important, for example, 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.

35. 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 that have been 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.

36. Another distinction that can be made relates to the differing degrees of complicity between an NPO and its donors. While in most of the relevant cases considered by the experts this year involved 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.

Detecting terrorist financing in the NPO sector

37. Given the typologies discussed above, the experts came to the conclusion that the method with the best chance of success for detecting possible terrorist financing links to NPOs is through intelligence or police work, which builds on links with other NPOs (operational, financial or through common management and personnel) or though connections to individuals that are already suspected of terrorist or terrorist financing activities. In some cases, the directors or managers of the NPO may already have a history of extremism or even a criminal or terrorism-related record. In other cases, links may be established with well-known terrorist organisations or with other NPOs that are already on the various lists of designated persons or entities maintained by the United Nations or individual countries. Public concerns and tips about the possible involvement of NPOs in questionable activities can also play a role in detecting possible misuse.

38. The reporting of suspicious unusual transactions by financial institutions and the subsequent analysis by FIUs or law enforcement also play an important role in bringing certain cases of suspected terrorist abuse of NPOs to the surface. In some countries, suspicious transaction reports related to unusual NPO-activity have actually led to the initiation of an investigation, while in other cases the reporting system and FIU-analysis have contributed to the development of further leads in ongoing investigations.

39. The monitoring activities of supervisory or tax authorities responsible for NPO oversight do not appear to have identified any initial leads into terrorist financing cases within the charitable sector. However, these authorities have sometimes played an important role in developing relevant leads by being able to ask further questions or inspect entities and/or share information with law enforcement agencies.

40. The experts agreed that each of these detection mechanisms had a complimentary function that could be pursued or enhanced collectively. This diversity of possible detection mechanisms and information sources regarding potential terrorist abuse of charities underscores the importance of constructing effective information-sharing arrangements both within and among government authorities.

Warning indicators

41. Besides the links to suspected terrorists, terrorist organisations or other suspect NPOs, the experts also identified a number of individual unusual characteristics or "red flags" in the case examples considered during this year's typologies exercise. Some of these unusual characteristics could be particularly helpful for financial institutions; others may be more useful for supervisory or investigative authorities.

Specific financial characteristics:

- Incongruities between apparent sources and amount of funds raised or moved such as situations in which large amounts of funds are apparently raised within communities that have a very modest standard of living.

- A mismatch between the pattern and size of financial transactions on the one hand and the stated purpose and activity of the NPO on the other, for example (as mentioned above) a cultural association that after ten years of existence opens a

financial institutions account for handling the proceeds of a music festival and deposits a disproportionately large amount of money into the account.

- A sudden increase in the frequency and amounts of financial transactions for the account of an NPO or the inverse, that is, the NPO appears to hold funds in its account for a very long period.

- Large and unexplained cash transactions by NPOs.

- The absence of contributions from donors located within the country of origin of the NPO.

Other characteristics:

- The existence of foreign directors, particularly in combination with large outgoing transactions to the country of origin of such directors and especially if destination is a high-risk jurisdiction.

- The existence of a large number of NPOs with unexplained links: for example, several NPOs transfer money to each other or share the same address, same managers or personnel; or a large number of NPOs are related to the same community and use the services of the same gatekeeper.

- NPOs with little substance, that is, in relation to their stated purpose and financial flows, or else they appear to have little or no staff, suitable offices or telephone number.

- Operations in or transactions to or from high-risk jurisdictions could of course also be considered as a reason for higher scrutiny by financial institutions. It could also serve as a criterion for initiating increased attention by supervisory or other competent authorities.

Policy implications

Different oversight systems and approaches

42. The consensus among those experts involved both in this year's typologies exercise and specifically in the NPO workshop was that additional measures will likely need to be developed to reduce the vulnerabilities of NPO to misuse for terrorist financing purposes. The extent and the nature of such measures remain to be defined, however. In part, the lack of clear direction in this area reflects the fact that there are great differences among countries in how they oversee and ensure transparency within the NPO sector. Some countries, for example, have a long-standing tradition of active government oversight of NPOs, while other countries put more emphasis on criminal investigation and detailed record-keeping requirements. Still other countries have implemented far-reaching regulatory systems that include detailed record keeping and reporting requirements,

external auditors, licensing, the mandatory use of authorised financial institutions accounts, permits for international transactions, and detailed customer due diligence requirements for financial institutions (with regard to NPOs).

43. The differences in approach among countries appear to be mostly related to different philosophies with regard to the role of government in the regulation of charities and other types of NPOs. Some countries believe that the protection of donors is a legitimate reason for comprehensive government regulation and supervision of NPOs. Others believe that protection of donors is primarily the responsibility of those who contribute to NPOs, thus it is private watchdog organisations, etc., which are responsible for this oversight.

44. Many countries have some kind of regulation and oversight of those NPOs that have been granted a full or partial tax-exempt status by fiscal authorities. In certain countries, these authorities may even play an important and active role in the oversight of such organisations. For example, the fiscal authorities may require detailed annual reports from each registered NPO and then make this information publicly available upon request. In other countries, government regulation and oversight is mainly geared towards protecting the integrity of certain types of legal entities, which have a specific license to handle large amounts of charitable funds.

45. Finally, there is of course another reason to increase regulatory oversight of the NPO sector, namely to prevent criminal abuse, not only for terrorism financing, but also for money laundering and fraud. No matter which approach is taken, most countries still appear to have significant loopholes in their systems. The experts identified a number of important constraints that might prevent jurisdictions from effectively reducing the threat posed by terrorist financing or other criminal misuse of the NPO sector.

46. Most countries can only dedicate a limited part of its resources to the regulation and oversight of the NPO sector, which in some cases consists of hundreds of thousands of organisations that handle a significant percentage of the GDP of a country. This observation is particularly true for many of the recipient or developing countries, where NPOs of all sizes, often community-based, play a particularly crucial role in the economy. Sometimes the NPO-sector in those countries has a larger economic weight and importance than the public sector.

47. In most countries, a large percentage (up to 90%) of the total number of NPOs consists of very small organisations. For these smaller NPOs, it can be difficult to carry a substantial administrative burden that would be required for complying with detailed government regulation. Even for larger organisations, there are limits to what can be considered a reasonable compliance burden, since the resources of NPOs are by their very nature scarce in relation to the often essential services they provide. Furthermore, some countries have certain legal or even constitutional provisions that prevent or limit the imposition of regulatory requirements on certain categories of NPOs. Examples of such provisions are the freedom of association or the special status of religion-based organisations.

Conclusions and issues for follow up

48. There was a consensus among the experts of this year's typologies exercise that, whatever approach is taken, government regulation or oversight should have a risk-based character. Any oversight regime (whether a genuine regulator or tax authorities) should have a targeted function and focus on areas of high risk. An argument was made by some experts

that an oversight function may be more useful in developing a terrorist financing lead in the early stages of investigation when there is not yet sufficient ground for a criminal investigation, rather than in generating independent leads. Others believed that government oversight could also have a clear preventative and lead-generating function by requiring enhanced scrutiny on certain high-risk categories of NPOs. In any event, it was recognised that having the authority and means to follow up on the suspicious or unusual characteristics of an NPO before there is sufficient grounds for initiating a criminal investigation is perhaps one of the most crucial elements of an effective system to combat misuse of the NPO sector.

49. Regardless of the approach taken to oversee of NPOs, many countries may nevertheless continues to have certain exceptions or loopholes in their systems that limit any reduction in the vulnerability of the sector as a whole. For example, some countries may be unable to monitor NPOs that do not register for tax-exempt status, religious organisations or NPOs established in certain other unregulated legal forms. There is thus a need to examine how vulnerable these parts of the NPO sector are to terrorist financing or other forms of misuse and then to identify alternative solutions to guarantee transparency and access, when necessary, to competent authorities. A solution mentioned by one country was to require NPOs to register with fiscal authorities in order to open a financial institutions account.

50. In order to generate and develop leads, the experts considered it important to further develop or enhance mechanisms and gateways for sharing information both nationally and internationally. To facilitate co-operation on the national level, there was considerable support for the idea of creating “national task forces” of law enforcement agencies, intelligence and security services, FIU personnel, NPO supervisors and tax authorities. Such task forces could: (i) examine and assess the risk of terrorist financing in the NPO sector; (ii) recommend appropriate development or enhancement of an effective yet reasonable oversight mechanism to combat this risk, and (iii) share information on potential or suspected terrorist financing activity occurring in the sector.

POLITICALLY EXPOSED PERSONS

51. The FATF examined PEPs and the risk they represent to the financial sector when it looked at the money laundering vulnerabilities of private financial institutions in 2001. New revelations of suspected PEPs' involvement in financial crime – especially as related to corruption – occur frequently in the press. After issuing the revised Forty Recommendations in which there are enhanced measures meant specifically to target the risk posed by PEPs, the FATF decided as well to include a short examination of this subject as part of this year's typologies exercise. The issue was therefore discussed during the full meeting of experts, and some initial findings were made.

52. *Politically exposed person* or *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.

53. From the material presented during the experts' meeting and the written submissions made by participants in the exercise, several observations can be made. First, 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 13: An associate of a PEP launders money gained from large scale corruption

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[96]. 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

[96] And an additional USD 22 million was later discovered.

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 financial institution, Financial institutions M, which in June 1999 was bought by another financial institution in Country A. Mr. Y was in charge of seeking investments on behalf of Financial institution M and identified construction and real estate projects for the financial institutions 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 Financial institution 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 Financial institution M in exchange for kickbacks from borrowers. When some loans defaulted, Mr. Y would purchase the financial institution's projects at extremely low prices for resale at a profit.

In addition, Mr. Y and members of Financial institution 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 Financial institution M. From there, it flowed into numerous accounts under a variety of names in financial institutions in foreign jurisdictions to conceal the origin of the funds.

Mr. Y consistently used a group of financial institutionss abroad to launder his and others' share of criminal proceeds. Ms. D, a financial institutioniser who is married to Mr. Y's cousin, formerly was a member of the board of directors of Financial institution N, helped Mr. Y conceal more than US$ 20 million in one jurisdiction.

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

54. Another observation is that 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 many cases 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 14: A senior government official launders embezzled public funds via members of his family.

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 financial institution establishment in neighbouring Country D. This movement formed legitimate grounds for this financial institution's 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 financial institution's accounts held in their country of origin (A), and the fact that the wife held accounts in other national financial institution establishments also provisioned by international transfers followed by withdrawals. The absence of any apparent economic justification for the financial institution 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 financial institution's account. An investigation has been initiated.

55. 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 financial institutionss 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 15: A senior employee of a state-owned company involved in high level corruption

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 financial institutions 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 this regular account activity, 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:

<u>The senior politician, senior official</u>

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 off-shore. 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.

<u>Wife of a PEP</u>

Money was transferred from Company A to one of the financial institutions accounts owned by Mr. A; Mr. A then placed funds into a solicitor's client account and an off-shore financial institutions 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.

<u>Friend and associate of the PEP</u>

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

56. According to one FATF member, there are two principal ways in which to detect the illegal financial activities of a PEP. The first is when there is a change in government in the home country of the PEP, and his or her illegal activities are revealed by the successor regime. While this may the clearest available indicator, it is not completely reliable. In some instances, accusations or illegal or corrupt practices by the new government represent a "political settling of scores". The second way that a PEP's illegal financial operations might be detected is through suspicious or unusual transactions in which persons acting on his or her behalf may be involved. When these transactions are viewed in the context of the relationship between the middleman and the PEP on whose behalf he or she may be acting, there may then be more reason to suspect an illegal source for the funds or assets involved.

57. In addition to the potential obstacles indicated above for conducting due diligence on PEPs, applying know-your-customer principles or detecting links between them (or their associates) and criminal activity, sometimes investigations into suspected illegal financial connections may be hampered by specific factors associated with PEPs. The most important of these, according to one of the participating experts, is the lack of necessary "political support", especially when the investigation appears to show connections between the foreign PEP and senior officials in the government where investigation is taking place. Obviously, the inability to obtain needed information – or to obtain it in a timely manner – from foreign counterparts also hinders the successful completion of such investigations.

Case 16: Laundering the proceeds of embezzlement

The financial institutions accounts of a petroleum minister (Mr. Y) of a former dictatorship under which numerous embezzlement offences had been committed were credited with a sum of USD 6 million in the space of a few months. This provided grounds for the case to be referred to the judicial authorities who decided to indict the minister.

On investigation the FIU discovered that Mr. Y was operating under the cover of an alias. The recently opened account controlled by Mr. Y had been credited with a notary's cheque for over USD 575,000 corresponding to the sale of a property. This sum did not correspond in any way to the market value of the property.

Policy implications

58. Several implications for AML/CFT measures arise from the discussion of PEPs during this year's typologies exercise. It was emphasised by more than one expert that dealing with the financial activities of a PEP in one respect is the same as dealing with those of any customer of a financial institution: proper due diligence should be conducted on both a PEP or the persons acting on his or her behalf. Similarly, know-your-customer principles should be applied without exception.

59. With regard to persons who either are or appear to be acting on behalf of someone else, either in performing financial transactions or holding assets, determination should be made as to the real or ultimate beneficiary / owner. One delegation raised issue of the difficulty once the true owner has been determined of finding out if the person is a PEP in his country of origin. It was pointed out that senior officials often change – even within an individual jurisdiction – thus someone who is a PEP now might no longer be so in the next

government. Two possible solutions were indicated: one would be to create a database that would contain information on current senior government officials. While this solution might be ideal, some delegations pointed out the difficulties that maintaining such a database would entail. Another solution would be simply to maintain appropriate databases at national level and then further encourage informal co-operation (for example, among FIUs) in enquiring about possible PEPs and their financial connections.

60. The FATF experts concluded that the techniques employed by PEPs to launder illegal proceeds were very similar to those of other criminal money launderers. If solely viewed from the perspective of the financial institution, these techniques look exactly the same. It has been noted in previous typologies exercises that PEPs may use distinctive financial institutions arrangements to assist them in creating a complex or sophisticated network of transactions to protect illicit assets they may have generated. Again, this was indicated as another important reason that financial institutions should perform all the necessary due diligence on PEPs, including their obligation to report suspected cases of money laundering.

61. Finally, while it was understood that the issue of PEPs extends by definition only to senior-level "exposed persons" and their associates, the experts believed that the issue of corruption below the senior level is also important. In the words of one delegation, the "biggest risk" to the financial system in some jurisdictions "is the underlying culture of corruption" and, in particular, the underpaid government official holding important responsibilities. The experts considered that this issue must be addressed in a systematic way with a global approach that takes into account the differing nature and degree of corruption in both developing and developed countries.

GATEKEEPERS AND MONEY LAUNDERING

62. As anti-money laundering measures are implemented in financial institutions, the risk of detection becomes greater for those seeking to use the financial institutionsing system for laundering criminal proceeds. Increasingly, money launderers seek out the advice or services of specialised professionals to help facilitate their financial operations. This trend toward the involvement of various legal and financial experts, or gatekeepers, in money laundering schemes has been documented previously by the FATF[97] and appears to continue today. The revised FATF Forty Recommendations issued in June 2003 address this issue by calling for the expansion of preventative financial measures to legal and financial professionals that are at risk of being involved in money laundering.[98] For these reasons, the FATF decided to look once again at how the services of these professionals may be misused for money laundering purposes.

63. 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.

64. 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. In the material considered for this year's typologies exercise, the experts appear to confirm the findings of earlier FATF typologies work.

Case 17: Accountant and lawyers assist in a money laundering scheme

Suspicious flows of more than USD 2 million were identified being sent in small amounts by different individuals who ordered wire transfers and financial institutions drafts on behalf of a drug trafficking syndicate who were importing of 24 kg of heroin concealed in cargo into Country Z. Financial institutions drafts purchased from different financial institutions in Country Y (the drug source country) were then used to purchase real estate in Country Z.

[97] See previous typologies reports: FATF-IX: http://www.fatf-gafi.org/pdf/TY1998_en.pdf, FATF-XI: http://www.fatf-gafi.org/pdf/TY2000_en.pdf and FATF-XII: http://www.fatf-gafi.org/pdf/TY2001_en.pdf

[98] Recommendation 12 now calls for extending certain obligations for customer due diligence and record keeping to lawyers, notaries, other independent legal professionals and accountants. Recommendation 16 extends to this category of professionals the obligation to report suspicious transactions, subject to professional secrecy or legal professional privilege.

An accountant was used by the syndicate to open financial institutions accounts and register companies. The accountant also offered investment advice to the principals.

A firm of solicitors was also used by the syndicate to purchase the property using the financial institutions drafts that had been purchased overseas after they had first been processed through the solicitor's trust account. Family trusts and companies were also set up by the solicitors

Case 18: Legal professionals facilitate in money laundering

A director of several industrial companies embezzled several million dollars using the financial institutions accounts of offshore companies. Part of the embezzled funds were then invested in real estate in Country Y by means of non-trading real estate investment companies managed by associates of the person who committed the principal offence.

The investigations conducted in Country Y, following a report from the FIU established that the creation and implementation of this money laundering channel had been facilitated by accounting and legal professionals - gatekeepers. The gatekeepers had helped organise a number of loans and helped set up the different legal arrangements made, in particular by creating the non-trading real estate investment companies used to purchase the real estate. These professionals also took part in managing the structures set up in Country Y. The investigation is ongoing

Case 19: An accountant provides specialist financial advice to organised crime.

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 financial institutions 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.

65. A number of FATF members have begun to look more closely at the role of gatekeepers in facilitating money laundering. In one jurisdiction, which has extended the obligation to report suspicious transactions to independent legal and financial professionals, it found that less than two percent of reports dealing with solicitor or notary involvement were made by the professions themselves. It was thus in the vast majority of cases the financial

institutions that detected potentially suspect activity. Among these reports, nearly 40 percent were related to the opening or administering of "trust accounts". Actions considered suspicious included cash transactions into or out of the account in rapid succession, flows of funds into or out of the account involving unknown sources or from sources that appeared to have no explainable relation, and transactions in amounts that appeared incompatible with their stated economic purpose.

Case 20: A lawyer uses offshore companies and trust accounts to launder money

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.

Case 21: A solicitor uses his client account to assist money laundering

Over a period of three years Mr. X repatriated the funds to Country Y for his use and benefit. He was assisted by lawyers and accountants using false transactions and offshore corporations. Mr. Y, formerly a lawyer, facilitated Mr. X's repatriation scheme by managing Mr. X's off-shore corporation and financial institutions accounts in several important financial centres. Mr. Y drafted documents that purported to be "loan" agreements between the off-shore shell corporation and a Mr. X nominee in Country Y. These loan agreements served as the basis for the transfer of millions from financial institutions accounts in several different countries to the Mr. X's home country. Upon arrival in the financial institutions accounts opened by Mr. X's nominee, the funds were

transferred to Mr. X. Mr. Y's lawyer used the law firm's financial institutions accounts to facilitate the transfers

66. Another FATF jurisdiction indicated that organised crime groups were further insulating themselves from detection by using one or more "corrupted" gatekeepers to channel funds through structures set up by another layer of gatekeepers. In this way, the second level of gatekeepers did not need to be as fully implicated in the scheme, and the risk to the organised crime group was further reduced by additional separation from the money laundering process. Two particular preferred methods using gatekeepers and identified by this jurisdiction were real estate transactions and the use of legal and accounting experts to build impenetrable audit trails. In the former case, land transfers or "conveyancing" is used because relatively large amounts of criminal proceeds can be efficiently laundered in a single transaction. This delegation also noted that accounting professionals involved in setting up the complex audit trail for a money laundering scheme often may not become known to investigators because they do not actually handle directly any of the relevant financial transactions.

Case 22: A trust fund is used to receive dirty money and purchase real estate

A lawyer was instructed by his client, a drug trafficker, to deposit cash into the lawyer's trust account and then make routine payments for mortgages on properties beneficially owned by the drug trafficker. The lawyer received commissions from the sale of these properties and brokering the mortgages. While he later admitted to receiving the cash from the trafficker, depositing same into his trust account, and administering payments to the trafficker's mortgages, he denied knowledge of the source of the funds

Policy implications

67. Many experts noted that even when the obligation already exists for gatekeepers to report suspicious transactions, the number of reports is often low. While in some jurisdictions this may be attributable to the relatively recent implementation of such rules, there are still may be perceived obstacles to full participation of gatekeepers in the anti-money laundering system. This in large part could be due to lack of awareness on the part of these professions or hesitations due to traditions of professional client secrecy. It was pointed out by one delegation, however, that gatekeepers have access to information that could be critical in understanding complex money laundering schemes, and theirs would therefore be a critical contribution in detecting such schemes. It is thus important that legal and accounting professionals involved in providing financial services or advice have the clear legal framework within which to report suspicious transactions.

68. It is also apparent that both gatekeepers and the financial institutions with which they deal should carry out the full customer due diligence procedures. Most likely the number of legal and financial professionals knowingly involved in facilitating money laundering is rather small. However, as indicated by many of the experts in this year's typologies exercise, one of the key reasons that services or gatekeepers are sought out by criminal organisations is to offer the appearance of additional legitimacy to their financial operations.

CONCLUSION

69. As indicated at the beginning of this report, the goals of this year's typologies exercise were to examine subjects of particular relevance to the current work of the FATF and to follow up on methods or trends initially identified in earlier typologies work. Terrorist financing and the implementation of the Eight Special Recommendations remain a primary concern of the FATF, thus examination of the role of wire transfers and non-profit organisations in terrorist financing in this year's exercise was deemed essential to the FATF's overall work. This year's look at money laundering vulnerabilities of the insurance sector expands on some of the issues identified in last year's exercise. While PEPs and gatekeepers have been addressed before by previous exercises, their inclusion in this year's programme is justified by the issue of the new FATF Forty Recommendations which provide a number of measures intended to deal with the risks in these two areas.

70. A new approach was used in preparing for the exercise and examining three of this year's topics (wire transfers, non-profit organisations and the insurance sector). This approach involved additional analysis and debate of the topics prior to the experts' meeting. It also included workshops during the experts' meeting itself to promote increased focus and serve as an additional means for exchanging ideas on the issues. The reaction of the experts to this new approach was for the most part positive, and it is therefore likely that organisers will use this experience to further improve future typologies exercises.

71. With regard to wire transfers and their connection to terrorist financing, the experts concluded that this was a mechanism that is frequently used to support various types of terrorist organisations. While investigators have been able to reconstruct terrorist links through use of wire transfers after such use has been detected, the fact that many cross border transfers do not include full identifying information on the originator is a key obstacle in determining those links. Furthermore, the initial detection of terrorist use of wire transfers remains difficult at present given the generally small size of individual transactions and the general lack of other useful indicators.

72. Non-profit organisations and their role in facilitating terrorist financing continue to be a key concern of the FATF. The experts in this year's typologies exercise made progress in understanding the types of misuse of NPOs and the specific financial "red flags" that may be indicative of it. The experts also attempted to identify some of the issues concerning oversight systems for this sector and measures that might be applied to reduce the vulnerability of NPOs to exploitation by terrorists. Additional work will need to be done to further refine this understanding of the terrorist financing risks as they relate to specific parts of the NPO sector in some countries.

73. This year was the first time that the FATF has looked at the risks that are specifically associated money laundering in the insurance sector. The experts discussed whether the amount of money laundering detected in the sector seems disproportionately small when compared to the size of the sector as a whole. Moreover, there are potential vulnerabilities that appear to be inherent to the sector. However, the experts did not reach consensus on these issues. A better understanding of these vulnerabilities as they relate to specific areas or product types seems to be emerging; however, the experts agreed that more work will need to be done to ensure that all risk areas have been identified. As well, work may be necessary to develop additional indicators specifically related to these areas.

74. Previous FATF typologies exercises have looked at some of the money laundering risks associated with politically exposed persons. The discussions of presentations and material provided for this year's exercise on this subject confirms earlier observations both as to the nature of and trends associated with this risk. While certain cases show that PEPs have used middlemen or other intermediaries to avoid detection, very often it seems that a PEP's illegal financial activities would have become clear if the financial institution opening or operating the account would have performed appropriate customer due diligence. The experts drew attention to some of the difficulties in determining whether a person should be considered a PEP, and for now, the best solution seems to be reinforcing informal co-operation among counterparts on the international level.

75. Similarly, the FATF has also examined some of the risks associated with the services provided by specialised legal and financial professionals, so-called gatekeepers. Again, the work during this exercise confirmed and expanded somewhat an understanding of the specific characteristics of this sector that make it vulnerable to money laundering. Many FATF members have begun implementing measures that would bring gatekeepers under the same obligations as currently held by financial institutions with regard to customer due diligence, record keeping and suspicious transaction reporting. A number of experts stressed that some of the vulnerabilities or risks identified regarding gatekeepers – as well as for dealing with PEPs – could be lessened if AML/CFT measures are consistently and thoroughly applied.

76. Countries from throughout the world – both FATF and non-FATF members – as well as a number of international organisations participated in the FATF-XV typologies exercise. Their experts were able to bring together the diverse experiences of individual jurisdictions in confronting the challenges of money laundering and terrorist financing and then apply them to the five themes of this year's exercise. While efforts such as the FATF typologies exercise help to increase awareness of the specific topics selected for a particular exercise, they also serve as an important forum for exchanging views between experts from operational backgrounds (i.e., police, prosecutors, regulators, FIUs) and those from the policy making side of government. It is this exchange of views that is ultimately an essential element of the FATF's efforts to promote and, as necessary, further refine the Forty Recommendations and the Eight Special Recommendations on terrorist financing.

Appendix VII. Extracts from the FATF October 2006 Report on the Misuse of Corporate Vehicles, Including Trusts and Company Service Providers

1. Introduction

Corporate entities, including corporations, trusts, foundations and partnerships with limited liability characteristics, conduct a wide variety of commercial activities and are the basis for a broad range of entrepreneurial activities in market-based economies. However, despite the important and legitimate roles these entities play in the global economy, they may, under certain conditions, be used for illicit purposes, including money laundering, bribery and corruption, improper insider dealings, tax fraud, financing of terrorist activities and other forms of illegal activities[1]. Criminals have responded to the money laundering defenses put in place by banks and other financial institutions by misusing corporate vehicles, and those who provide trust and company services, to disguise and convert their proceeds of crime before it enters the traditional financial system.

Organized crime groups or individual criminals tend to seek out the services of professionals to benefit from their expertise in setting up schemes that the criminals then use for illicit purposes. Criminals may seek advice from trust and company service providers (TCSPs) as to the best corporate vehicles or jurisdictions to use to support their schemes, with the TCSPs having varying degrees of awareness of or involvement in the illicit purposes underlying their client's activities.

General concerns about the misuse of corporate vehicles by criminals to disguise and convert the proceeds of their illegal activities, as well as concerns about the use of trust and company services to help facilitate this misuse, are reflected in the extension of the scope of the FATF Forty Recommendations to lawyers, accountants and TCSPs, and, in particular, in the wording of Recommendations 5, 33 and 34. They are concerns that have also been specifically referred to by the G7 Financial Stability Forum, the European Commission, the International Organisation of Securities Commissions (IOSCO) and the Organisation for Economic Co-operation and Development (OECD).

Of particular concern is the ease with which corporate vehicles can be created and dissolved in some jurisdictions, which allows these vehicles to be used not only for legitimate purposes (such as business finance, mergers and acquisitions, or estate and tax planning) but also to be misused by those involved in financial crime to conceal the sources of funds and their ownership of the corporate vehicles. Shell companies can be set up in onshore as well as offshore locations and their ownership structures can take several forms. Shares can be issued to a natural or legal person or in registered or bearer form. Some companies can be created for a single purpose or to hold a single asset. Others can be established as multipurpose entities. Trusts are pervasive throughout common law jurisdictions. When in February 2000 the FATF reviewed the rules and

practices that impair the effectiveness of money laundering prevention and detection systems as part of its non-cooperative countries and territories initiative, it found in particular that:

Shell corporations and nominees are widely used mechanisms to launder the proceeds from crime, particularly bribery (e.g. to build up slush funds). The ability for competent authorities to obtain and share information regarding the identification of companies and their beneficial owner(s) is therefore essential for all the relevant authorities responsible for preventing and punishing money laundering.

The aims/objectives of the project: [2] This typologies project's prime aim has been to seek to identify in respect of corporate vehicles areas of vulnerability for money laundering and terrorist financing, along with evidence of their misuse. It has also sought to identify differences among jurisdictions for establishing and using corporate vehicles, how these may be exploited and what steps have been or are being taken by jurisdictions to address this threat[3].

While this typologies project is concerned with the misuse of corporate vehicles for money laundering and terrorist financing, the findings and the issues for further consideration can be expected to have similar application to other types of criminal activity. In addition to their use in facilitating money laundering, corporate vehicles are frequently mis-used to help commit tax fraud, facilitate bribery/corruption, shield assets from creditors, facilitate fraud generally or circumvent disclosure requirements.

The concerns arising from the misuse of corporate vehicles by criminals have been well documented by a number of other authorities.[4] However, it is hoped that from this typologies project will come a clearer picture of the misuse involved. This in turn should help focus and prioritize efforts made in the anti-money laundering (AML) and combating the financing of terrorism (CFT) areas to meet those concerns.

Corporate vehicles play a complex, varied and essential role in modern economies. The scope and scale of a typologies project that looks at the misuse of corporate vehicles is therefore potentially enormous. Extensive literature already exists on the subject, and the considerable jurisdictional variation in the nature, scale and oversight of corporate vehicles means that there are also many differing viewpoints on the subject to be taken into account. Similarly, many specific issues arise regarding the creation, administration and operation of corporate vehicles.

In examining the potential misuse that corporate vehicles may be subject to, it is important to bear in mind that, of the millions of companies that exist, the vast majority engage in legitimate business, and only a small minority are misused. Likewise among the trusts that are set up, the majority serve legitimate purposes, and only a small minority are misused.[5] In considering the misuse of corporate vehicles, it will be essential

therefore to distinguish between those vehicles that pose a high risk and those that pose a low risk in relation to money laundering and
terrorist financing.

The initial step for this project was to establish a team of experts which included persons drawn from FATF jurisdictions, observer organisations and FATF-style regional bodies (FSRBs) with skills/experience in the process of corporate vehicle formation and administration, and in particular the formation and administration of shell companies, and in regulatory action and law enforcement in this field. The experts came from a range of countries including common law and civil law jurisdictions, countries from outside the FATF and also countries with a substantial TCSP and/or non-resident business activity sectors.

The first step taken by the team of experts was to conduct a survey (by means of a questionnaire) [6] as a way of obtaining a fuller picture of the international diversity in the formation and administration of corporate vehicles, and of providing both FATF and FSRB members with an opportunity to contribute to the exercise.

Faced with the vast scope of a general project on corporate vehicle misuse mentioned above, it was clear to the team of experts that the most effective way to deal with the subject was to focus first on what they and prior studies considered to be the most significant feature of the misuse of corporate vehicles – the hiding of the true beneficial ownership. It is therefore with this aspect in mind that this report is primarily concerned. This is not to deny that there are other aspects that are worthy of attention, and that more detailed work on other areas could be done later.

The terminology used in the context of corporate vehicles is also quite varied and complex, and it often differs from one study to another. Therefore, a glossary of terms used in this report is included in Annex 1. At the start of this report, it is useful however to highlight two key terms as they will be used for this study:

- ***Corporate vehicle*:** This term has the same meaning as that used by the OECD[7] and thus includes corporations, trusts, partnerships with limited liability characteristics, foundations, etc.

- ***Trust and company service provider (TCSP)*:** This term has the same meaning as used by the FATF[8] and thus includes those persons and entities that, on a professional basis, participate in the creation, administration and management of corporate vehicles.

2. Typologies

As a starting point for this study, the team of experts first examined a series of case examples of misuse of corporate vehicles[9]. By examining such material, certain key elements and patterns for this misuse were identified. The following typologies then

derive from case examples that were submitted as part of the response to the survey as well as from several databases.

This section uses a selection of the submitted cases[10] to focus on examples in which one of the main objectives of the misuse was to hide the ultimate beneficial owner. The case studies indicate how difficult it can be to determine who actually benefits from the structure. The different ways to maintain anonymity and to hide identity are described in the following case examples. Often these structures are used to perform two functions simultaneously: the execution of a criminal scheme and the diversion of money flows as part of a money laundering scheme.

All submitted case studies show several common features. For illustrative purposes, four typologies were selected, each of which focuses on a specific method or element of a corporate vehicle structure that is commonly used to hide identity. As indicated above, the selection of cases was made so as to highlight the key characteristic involved. The remaining case examples are included in Annex 4, which classifies the examples according to individual typologies and main characteristics that can be useful for money laundering activities.

Typology 1 – Multi-jurisdictional structures of corporate entities and trusts[11]

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[12]. 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. The cases belonging to this typology are described briefly in the next few paragraphs, with more detailed descriptions set out in the boxes below.

In Case 1, third parties were persuaded to invest savings and retirements accounts in a series of trusts. The investors were led to believe that the trusts would ultimately provide investment income. In fact, however, the trusts, which were tied to offshore bank accounts, served as conduits for channelling funds to the perpetrators of the fraud scheme.

In Case 2, a multi jurisdictional structure was set up to purchase insurance companies and again divert the assets to the creators of the structure.

Case 3 concerns an investment fraud scheme. To realise the scheme, offshore corporations from Antigua, Isle of Man and Belize were used. The structure was also used to divert the money and hide the profits from fiscal authorities.

Case 1

Mr. [A] was a trust service provider operating a trust company [L]. Using a series of domestic trusts that he established, he wired large sums of money to 51 different US and offshore bank accounts. In total it is estimated the scheme defrauded over 500 investors of approximately $56 million.

The thrust of the scheme was that A and associates convinced their clients to form ["Pure Trust Organizations"(PTO)] and to place their life savings, including their retirement accounts, into these trusts created by [L]. Clients were advised that the [PTO] provided asset protection providing concealment of their assets from the government and other creditors. The [L] package promised the formation of a [PTO] and off- shore bank accounts. The clients were told that when the funds were placed in these off-shore bank accounts the funds was beyond the reach of the US government and any creditor.

Once the clients had placed their assets into the trusts, [A] used another corporation to provide investments for the assets in the trusts. In reality there were no real investments, and [A] and his associates defrauded the trust owners.

Case 2

Mr. [B] set up an international structure with on- and offshore companies as well as trusts to purchase insurance companies. The insurance companies were actually bought through a trust to hide the personal involvement of [B]. The assets of these companies were subsequently drained and used for personal benefits. The draining of these assets was concealed by transferring the money into accounts in and out of the US via wire transfers. Immediately after the acquisition, [B] would transfer million of dollars of reserve assets to a corporation he set up in the US. The funds were transferred to an offshore bank account in the name of another corporation that he controlled. Once these funds were deposited into the offshore bank account, [B] used them to pay for his personal expenses. In this way [B] laundered about USD 225 million over a period of 9 years.

Case 3

This case example shows a pyramid investment scheme. It caused more than USD 8.4 million in losses to almost 8,000 investors in the US. The investigation focused on an association [M]. [M] was a pyramid business enterprise that sold various products to its members including investment plans. It was alleged that [M] leaders were promoting the sale of an investment, identified as [Private Placement Offers (PPO)]. The investment promised a 30 to 1 return within a year. To be able to benefit, the investment members were encouraged to establish offshore corporations and bank accounts in Antigua, Isle of Man and Belize. They were advised that financial transactions relating to these investments should be transferred through their offshore accounts. The funds of all the investments were deposited into bank accounts in the US. Instead of using these monies as purported, [M's] leaders diverted the funds to their personal use and used the funds to promote the carrying on of the illegal enterprise. Potential investors were fraudulently lulled into believing that the investment was guaranteed by a bank and the principal insured by a major insurance company. The new investor funds collected and not yet turned over to the US Corporation were used to issue checks to investors within the group who were expecting their first returns from investment. The appearance that the program was working caused a windfall of new investor money to begin pouring in for the [PPO].

Case 4

The identity of the beneficial owner remained unknown in the management of several investment funds. Fund E was established in the British Virgin Islands. This fund had over EUR 93 million in assets in Bank A. The fund was managed by Company F in Dublin.

One of the shareholders of Fund E was Bank G in Switzerland. Another shareholder was Fund H (Bahamas), managed by Company I (Bahamas). Fund H was 100% controlled by Bank J, another Swiss bank.

However, for Fund E, Bank A was not able to compare the subscriptions with the total amount of capital issued by the fund. Moreover it appeared from business correspondence found during the on-site mission led by the French Banking Commission that Mr K was directly involved in the management of Fund E. It was likely that Mr K's family was the beneficial owner of the fund, but the bank had no evidence thereof.

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 5

A company initially established in an offshore centre had moved its registered office to become a limited company under Belgian law. It had consulted a lawyer for this transition. Shortly afterwards the company was dissolved and several other companies were established taking over the first company's activities. The whole operation was executed with the assistance of accounting and tax advisors. The first investment company had opened an account in Belgium that received an important flow of funds from foreign companies. The funds were later transferred to accounts opened with the same bank for new companies. These accounts also directly received funds from the same foreign companies. Part of it was invested on a long term basis and the remainder was transferred to various individuals abroad, including the former shareholders of the investment company. These funds were also transferred to the new companies. The whole structure was set up by tax accountants.

Case 6

Mr. [C] was an accountant who started his own accounting and financial services business [N] in Panama. He advertised his services primarily on the internet and through mass mailings. [N] provided a variety of services including the following:

- *Formation of offshore entities to disguise ownership of assets;*

- *Passports and dual citizenship, mostly using new nominee names;*
- *Movement of cash and other assets offshore and back onshore using various methods;*
- *Issuance of debit cards for the purpose of anonymously repatriating and spending offshore funds;*
- *Use of correspondent bank accounts to skim profits of legitimate businesses and repatriate funds through the purchase of assets and use of debit cards;*
- *Anonymous trading of securities through accounts with two major brokerage houses;*
- *False invoicing/re-invoicing schemes to support fraudulent deductions on tax returns;*
- *False investment losses, to disguise transfer of funds overseas.*

[C] was identified pursuant to an Internal Revenue Service investigation of one of his clients for illegal importation and sale of goods. The targets of this investigation were using a re-invoicing scheme devised by [C] to illegally import these chemicals into the US for sale. [C] assisted the targets in the re-invoicing scheme by preparing the invoices, receiving the proceeds of the scheme and hiding the proceeds in a myriad of Panamanian corporations for later use by the targets.

As a result of this investigation, [C] became a subject of investigation for the formation of illegal trusts to facilitate money laundering and other crimes. The investigation disclosed that [N] had about 300-400 active clients/investors. The investigation also disclosed that it created between 5,000-10,000 entities for these clients, including the layering of foreign trusts, foundations and underlying business corporations, which were formed in offshore countries. The primary package purchased by the client was referred to as the Basic Offshore Structure that includes a foreign corporation, a foreign trust and a foundation. In 2003, [C] was found guilty of money laundering and other criminal violations. He was sentenced to 204 months' imprisonment and fined USD 20,324,560 and ordered to pay restitution to the Internal Revenue Service in the amount of USD 6,588,949.

Typology 3: – Nominees

The next series of cases provides examples of the extent to which the use of nominees may be used to hide the identity of the beneficial owners. Within this typology, the use of nominees may be grouped into the following categories: nominee bank account, nominee shareholders and nominee directors.

Case 7

Mr [B] and his associate bought insurance companies. The assets of these companies were drained and used for personal benefits. The draining of the assets was concealed by transferring them into accounts in and out the US via wire transfers. The first step in the scheme was establishing a trust in the US. [B] concealed his involvement and the control of the trust through the use of nominees as grantors and trustee. [B] then used the trust to purchase the insurance companies. Immediately after the acquisition, [B] would transfer millions of dollars of reserve assets to a corporation he set up in the US. The funds were

then wire-transferred to an offshore bank account in the name of another corporation that he controlled. Once these funds were deposited into the offshore bank account, [B] used them to pay for his personal expenses.

Case 8

Beginning in 1997, Mr. [D] assisted his clients with various schemes to hide income and assets from the IRS, including a method by which an individual used 'common used trusts' to conceal ownership and control of assets and income and the use of offshore trusts with related bank accounts in which the assets would be repatriated through the use of a debit card. [D] also set up international business corporations (IBC) that had no economic reality and did not represent actual ongoing business concerns, on behalf of his clients, to conceal the clients' assets and income from the IRS. Concerning his own liabilities, [D] opened and maintained nominee bank accounts both in the US and abroad to conceal his income from the IRS.

Case 9

Mr. E, a CEO of a local telecommunication company received corrupt money of RM 300.000 as an inducement to award supply and work worth RM 5 million to a company P which belonged to Mr. F. Mr. F paid the corrupt money as a payment by company P to company Q for services rendered. Company Q also belonged to Mr. F but was merely a dormant and shell company with RM 2.000 paid up capital. The money was later withdrawn from company P and placed in a stock broking firm under the name of Mr. G., a nominee of Mr. E, who opened an account with the same stock broking company using his son's name. The money in G's account was used to purchase shares in the open market and later sold to Mr. E's son using numerous married deal transactions whereby the shares were later sold by Mr. E's son in the open market at a higher price. Capital gains subsequently were used to open fixed deposits, sign up for a insurance policy (under the name of Mr. E) as well as purchase assets in the name of Mr. E's relatives.

Typology 4: Shell companies.

The use of shell companies to facilitate money laundering is a well-documented typology. 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.

THE WHITE WHALE CASE

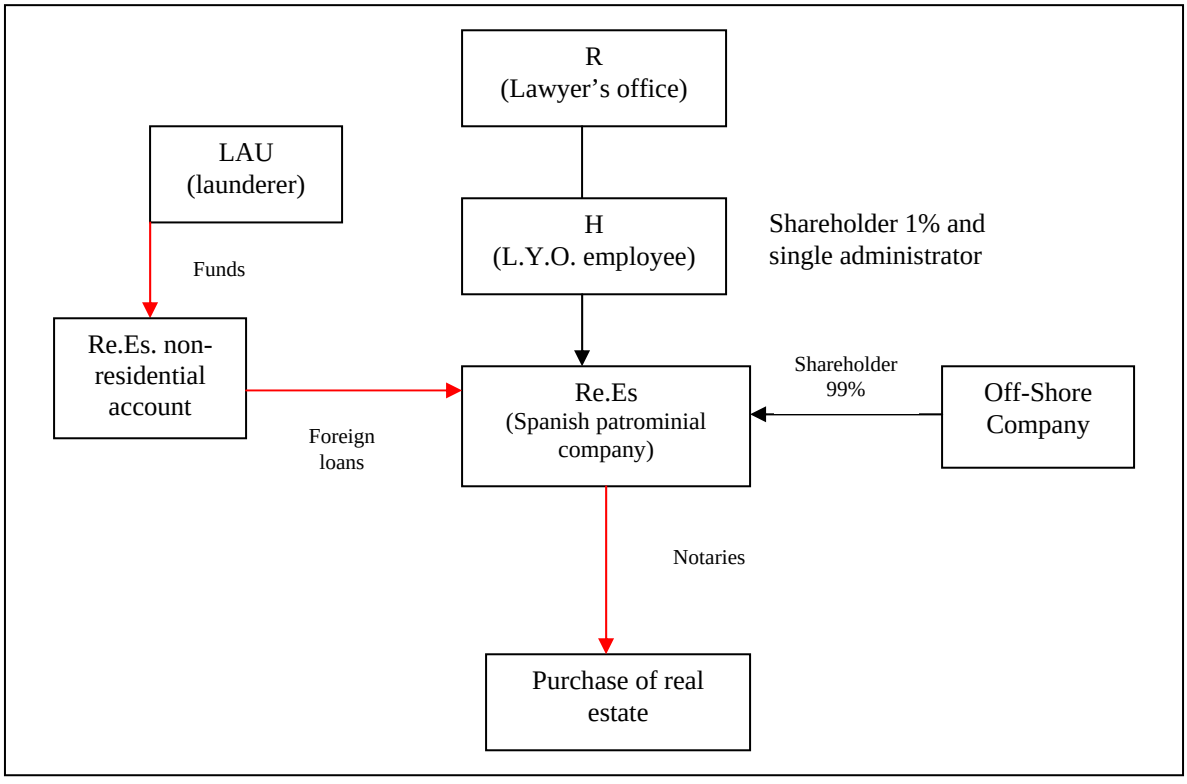
The investigations started in September 2003 by cross referencing data from an investigation on drug trafficking, with information coming from another investigation on assets owned by Eastern European citizens living in the Costa del Sol (Malaga).

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.

Analysis of the Typologies

From the typologies presented here, the methods for concealing the identity of the beneficial owner and/or his customer may be broken down into the following groupings based on the types of corporate vehicles used in the structure of the money laundering scheme.

Figure 1

Use of (various types of) companies	7 cases
Use of banks or investment funds	2 cases
Use of one of more trusts	5 cases
Use of companies and trusts	4 cases
Use of nominees	6 cases
Use of TCSPs	5 cases

Traditionally the money laundering process is broken down into three phases — placement, layering and integration. Since corporate vehicles may be used for multiple purposes in the different phases of the money laundering process, a slightly modified version of this template might be considered to better describe the role that such entities can play in money laundering13. For the analysis of the case studies four phases of money laundering were distinguished.

In the "placement" phase, dirty money is inserted into the financial system. In the second or "layering" phase, the money is moved through various bank accounts, mostly belonging to several different corporate vehicles in multiple jurisdictions. The third phase, known traditionally as the "integration" phase consists of two sub phases: "justification" and "investment". In the "justification" phase, the proceeds are re-integrated into regular business activities, for instance by way of a loan structure. In the "investment" phase, the now laundered money is invested for personal gain, such as purchasing real estate.

Looking at the cases sampled for this study, the following breakdown may be made of the particular phases in which the corporate vehicles appeared to play a preponderant role in the money laundering process.

Figure 2

Money laundering phase	**Number of case studies**
Placement	22
Layering	5
Justification	2
Investment	4
Unknown (more specific details are needed for classification)	2
No money laundering process identified	4
Combination of money laundering phases	6

As can be seen from this overview, it was found that the majority of the cases presented involved misuse of corporate vehicles in the first phase of money laundering. In a number of cases, corporate vehicles are used to lure third parties in fraudulent investment schemes or committing other types of fraud. It is clear that this finding is based on the information available and that the case studies from which information has been obtained involve crimes other than money laundering. However, the techniques observed – the use of corporate vehicles, the use of specialised intermediaries, and the use of foreign jurisdictions – are all common to the techniques used for money laundering and therefore can be considered to be of equal relevance.

In analysing the submitted case studies, certain common elements were found. These elements are sometimes combined with the typologies (e.g. the involvement of financial or legal experts) and sometimes with an additional element to help achieve the goal (e.g. concealing identity, diverting money flow). The most common elements are the following:

- Multi-jurisdictional and/or complex structure of corporate entities and/or trusts (cases 1, 2, 3, 4 and White Whale);
- (Foreign) payments without a clear connection to the actual activities of the corporate entity (cases 5, 11,and White Whale);
- Use of offshore bank accounts without clear economic necessity (cases 1, 4, 3, 6, 17, 21, 27, 28, 30, 31, 32, 34, and White Whale);
- Use of nominees[14] (cases 2 7, 8, 27, 28, 35, and White Whale);
- Use of shell companies (White Whale);

- Tax, financial and legal advisors were generally involved in developing and establishing the structure. In some case studies a TCSP or lawyer was involved and specialised in illicit services for their clients (cases 1,5,6,7 and White Whale).

When hiding or disguising the identity, often a combination of the above mentioned elements and various layers with a foreign element is established to maintain as much anonymity as possible. These elements can be considered as indicators or "red flags" for such activity. The more of these elements observed, the greater the likelihood (and the risk) that the identity may be able to remain unknown. It is therefore essential for authorities to be able to determine the ultimate beneficial owners of a company and the trustees, settlors, beneficiaries involved with a trust.

3. Analysis of the Questionnaires

The following is an analysis of the responses of 32 jurisdictions to the survey conducted by the FATF as part of this study[15]. The assumption underlying the survey is that one of the main purposes of the misuse of corporate vehicles is to hide the identity of the natural person(s) benefiting from and/or controlling the money laundering, that is, the beneficial owner (BO). Thus the primary aim of the survey was to ascertain how criminals might use corporate vehicles to hide their identities and how, in practice, this may have occurred. The survey sought to achieve this aim by eliciting information on (1) the types of corporate vehicles in a particular country, (2) the types of BO relationships, (3) the sources of BO information and methods of obtaining such information, and (4) examples of the misuse of corporate vehicles in that jurisdiction. Beneficial ownership, the sources of information and the regulation thereof are addressed below. The case examples provided earlier demonstrate how the weaknesses identified are exploited in practice. The analysis is based solely on the information obtained through the survey; no verification of the information provided by respondent jurisdictions was undertaken.

The types of corporate vehicles are described in Annex 6[16]. Although many different types of corporate vehicle can be abused, the submitted case studies show that the legal entity most commonly misused is a private limited company with shared capital combined with activities in a jurisdiction other than the jurisdiction where the entity was created.

Section 1: Beneficial Owners

The FATF Methodology Glossary defines a beneficial owner (BO) as the natural person "who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement."[17] Accordingly, the issues of ownership, control, and, for trusts, beneficiary identification must be addressed.[18]

A. Ownership

The potential for anonymity is a critical factor in facilitating the misuse of corporate vehicles.[19] In particular, the fact that ownership of a corporate vehicle may be through corporate shareholders, nominee shareholders and bearer shares presents a special challenge to determining beneficial ownership of a corporate vehicle.[20] Each of these

types of ownership is considered in Figure 2.1. It should be noted however that the ownership and control structures described below have many legitimate purposes.

Figure 3

PRACTICE: Ownership through…	**Defining Characteristics**	**Associated Problems/ Risks**	**Where permitted among reporting jurisdictions**
Corporate shareholders[21]	Shares are owned by a legal entity.	Creates an extra layer between BO and entity.	Not addressed in questionnaire
Nominee shareholders][22]	Shares are registered in the name of another (such as a stockbroker)	Reduces usefulness of shareholder register	Not addressed in questionnaire
Bearer shares[23]	Negotiable instruments according ownership of a corporation to the person who possesses the bearer share certificate.	Can be easily transferred without leaving a paper trail	NL,[24] UK,[25] TR, LB, LV, NZ, QA, HK, MH, DE, SK, CH, US, DK Permitted but dematerialised[26] in: VI, BE, LT, MO, FR

B. Control[27]

Corporations serving as directors and nominee directors can be used to conceal the identity of the natural persons who manage and control a corporate vehicle.[28] Corporate directors and nominee directors are described in Figure 4.

Figure 4

PRACTICE: Control through…	**Defining Characteristics**	**Associated Risks**	**Where permitted among reporting jurisdictions**
Corporate directors	Corporation is selected to serve as a director. Management functions performed by representative of the selected corporation.[29]	Creates an extra layer in establishing identity of natural person who controls. May facilitate abuse of CVs if legal system cannot timely assign responsibility to physical persons.	NL, MY, US, GI, LV, MA, GG, QA, UK,[30] HK, MH, DE, PW, TR, LB, VI[31], BE, BA
Nominee directors [32]	Director nominates another entity or person to act as the director in its place.	Increased difficulty in identifying those who exercises de facto control.	Not addressed in questionnaire

Nineteen of the 32 jurisdictions responding to the survey indicated that corporations are permitted to serve as directors, whereas corporate directors are prohibited in eight. Five jurisdictions failed to provide an answer to this item on the questionnaire.[33] None of the responding jurisdictions that permit corporate directors indicated that foreign corporate directors were prohibited. One jurisdiction stated that "a fit and proper test applies to corporate directors, however executing these tests on foreign directors tend to be difficult due to lack of information."[34]

Although the survey did not specifically address the use of nominee directors, at least one respondent indicated that this practice is one of the greatest contributors to a corporate vehicle's vulnerability to misuse.[35] Typically, a nominee director appears as a director on all company documents and in any official registries, but passes the requisite duties of the directorship on to the beneficial owner.[36]

One jurisdiction allows TCSPs to act as nominee directors if certified to do so.[37] In this jurisdiction, TCSPs can face significant liability for failure to practice customer due diligence (CDD) and generally cannot be released from liability as nominees.[38] This jurisdiction further indicated that TCSPs are required to obtain indemnity insurance before acting as nominee directors.

C. Beneficiaries

A beneficiary is someone for whose benefit property is held in trust, especially one designated to benefit from a disposition or assignment or to receive something as a result of a legal arrangement or other instrument. Traditionally, trusts have been treated like contractual agreements between private persons and subjected to less regulation and oversight and to fewer disclosure requirements, thus making them susceptible to abuse.[39] Trusts can legally be established in seventeen of the jurisdictions surveyed.[40]

Section 3: Information Sources

Information about corporate vehicles may be obtained from a variety of sources such as the corporate vehicles themselves, from a company registry, from public sources such as government or regulatory authorities, exchange operators, via intermediaries such as TCSPs or lawyers, notaries or accountants, or from other sources through the use of compulsory or investigatory measures.[41]

A. Corporate Vehicles

Corporate vehicles often keep shareholder registers. Fifteen jurisdictions indicated that corporate vehicles are obliged to keep shareholders lists that are then available to competent authorities.[42] One jurisdiction indicated that international business companies (IBCs) are required to maintain a register of shareholders at its registered office.[43] To be clear, the shareholder registers may contain accurate information on legal ownership, but not necessarily on beneficial ownership.[44]

B. Company Registries

All jurisdictions responding to the survey indicated that company registries with information on legal ownership are required. Twenty jurisdictions include foundations in these registries[45], twenty-five jurisdictions include limited liability partnerships[46], and three jurisdictions include trusts.[47] Eighteen jurisdictions indicated that it is mandatory for the registry to be regularly updated.[48] One jurisdiction requires that any change in the beneficial ownership of shares be reported to the public registry.[49] These registries are accessible to the public in all but three jurisdictions.[50] One jurisdiction indicated that it is optional for companies to be recorded in the company registries.[51] Five jurisdictions require that a corporate vehicle be approved before it can be included in the company registry.[52]

C. Intermediaries

Intermediaries, such as TCSPs, lawyers, notaries and accountants, commonly play a role in the formation and management of corporate vehicles.[53] In the cases submitted as part of the survey, intermediaries played a role in many instances. Twelve jurisdictions require TCSPs to carry out customer due diligence procedures that are predicated upon a verified identification of the beneficial owner[54], and nine jurisdictions mandate that TCSPs apply for a license before engaging in the business of the formation or management of corporate vehicles[55].

About half of the jurisdictions use TCSPs for the formation and management of corporate vehicles.[56] Within these jurisdictions, TCSPs face sanctions for deficiencies in exercising due diligence. These sanctions can include making public statements, the imposition of conditions on continued licensure, requiring specific actions, and license revocation.[57]

Twenty-nine jurisdictions allow lawyers, notaries, and accountants to participate in the formation and management of corporate vehicles.[58] However, only seven jurisdictions specifically reported that their governments enforce AML regulations with respect to intermediaries.[59] Of those six, three jurisdictions defined penalties for failure to follow AML regulations.[60] Those penalties included letters of disapproval, automatic governmental access to books and accounts, and loss of license. Ten jurisdictions rely on private regulation of intermediaries for the civil enforcement of AML.[61]

One jurisdiction stated that it places significant reliance on financial institutions to obtain information on the beneficial owner. It noted the importance of CDD and KYC practices for the success of their reliance on financial institutions.[62]

D. Other Sources

Other sources of information can be utilised through a jurisdiction's investigatory powers, including both the ability to gather information from public records as well as the authority to compel corporate vehicles to release information. Thirteen jurisdictions rely exclusively on investigatory powers to obtain information on beneficial ownership.[63]

Typical means employed by jurisdictions relying on investigatory powers include examining the tax returns of corporations through the local internal revenue office,[64] retrieval of information from online databases,[65] and acquiring information from a jurisdiction's securities exchange commission. According to one jurisdiction, the inability to use evidence gathered by investigation at trial presents a problem with this method.[66] Another jurisdiction indicated that it uses its governmental powers to "undertake monthly updates of records of selected companies."67

The obstacles to obtaining information are compounded by the fact that in almost all cases of the misuse of corporate vehicles, there is one or more cross border relationship, as was evidenced by the cases submitted for the survey. In these examples, the cross-border structures had different corporate vehicles "stacked" on top of each other, with each vehicle holding (all or some) shares in the vehicle below it, they had non-resident Management (directors)[68], or else the corporate vehicle had been incorporated in jurisdiction other than the one in which the related activity took place:

Figure 5

Jurisdiction or state of incorporation is *not* the same as jurisdiction or state where the actual activities take place	23 cases
Jurisdiction or state of incorporation is the same as jurisdiction or state where the actual activities take place	2 cases

Unknown (lacking information)	8 cases
Total number of analysed cases	33 cases

Indeed, the lack of economic and/or logistic benefits when using a multi-jurisdictional structure for corporate entities or the related money flow would appear to be an important indicator of possible abuse.

Furthermore, foreign (offshore) bank accounts were used in 13 of the 33 analysed cases. In 11 out of the 13 cases, a combination of multi-jurisdictional structure and foreign bank accounts was identified.

Section 4: Overview of survey responses

The responses to the survey highlighted the main areas of risk with respect to corporate vehicles, indicated frequent problems in obtaining information on beneficial ownership, and suggested areas for further investigation.

A. Areas of Risk

Several jurisdictions continue to have practices that make use of corporate vehicles which are relatively more vulnerable to exploitation for illicit purposes, such as ownership through nominee shareholding and bearer shares, and control through nominee and corporate directors.

Where information on a corporate vehicle must be disclosed upfront, there is a potential problem with ensuring that this information remains current and accurate over time. Dealing with this issue will require learning more about how jurisdictions with upfront disclosure systems for corporate vehicles enforce and update their company registers.

TCSPs, lawyers and accountants are required in most jurisdictions to practice CDD. Based on responses to the questionnaire this normally results in the information on beneficial owners being obtained by persons subject to AML requirements, but it does not necessarily mean this information is then directly accessible by the authorities.[69] Also, in jurisdictions with strong confidentiality rights, information held by the TCSPs may be treated in the same way as information held by legal professionals, thus making it harder for competent authorities to gain access to the records.[70] Although bearer shares can serve legitimate purposes, they can also be used to mask the true ownership and control of a company and thus may be used for money laundering, self-dealing and/or insider trading. Sixteen of the thirty-two jurisdictions permit the use of bearer shares, and in two jurisdictions bearer shares can also be used by private companies.[71] Five jurisdictions indicated that they have dematerialized or immobilized bearer shares in an effort to verify the identities of their owners.[72]

B. Prevalent Problems in Obtaining Information[73]

Twenty-nine of the jurisdictions surveyed stated that they are willing to exchange information on beneficial ownership with foreign jurisdictions[74], although nine expressed concern about bureaucratic delays associated with obtaining information from foreign authorities[75]. Also, seven noted that the inability to gather necessary information from analogous regulatory bodies in other jurisdictions was due to insufficient disclosure from corporate vehicles and TCSPs, not from lack of co-operation.[76]

In summary: the survey appears to show that in the reporting jurisdictions–

- There is a wide variety of types of "corporate vehicles";
- "Beneficial owners" are involved with corporate vehicles in a number of different ways –through direct shareholding and through indirect shareholding (corporate shareholders, nominee shareholders, bearer shares, trusts);
- There are a large number of different competent authorities with oversight of corporate vehicles;
- Information on "corporate vehicles" can be found in a number of different places, such as company registries, financial institutions, and TCSPs;
- The degree of regulation applied to the creation and administration of corporate vehicles varies significantly from jurisdiction to jurisdiction – for example, a few jurisdictions regulate trust and company service providers, but the majority still do not;
- Many countries permit bearer shares to be issued and also permit the appointment of corporate and nominee directors;
- In some countries, the corporate vehicle itself is obliged to furnish/maintain certain information, and it is sometimes subject to criminal liability;
- In all countries covered by the survey, a company registry exists, but the extent of the information available from the registry varied significantly from jurisdiction to jurisdiction. Some require full shareholder information, others only partial information. Some provide information from the time of creation and have no update obligation; others include an obligation to register changes in shareholding. In nearly all cases, the information in the company registry relates to legal ownership – and not necessarily the beneficial ownership – of the corporate vehicle;
- Lawyers and accountants that are involved in establishing corporate vehicles are subject to AML regulation in the majority of countries surveyed.

4. Overall findings and conclusions

From the foregoing analysis of the typologies and the survey, it seems clear that prevention of corporate vehicle misuse for ML purposes could be improved by knowing or being in a position to determine in a timely fashion who are the ultimate beneficial owners of a company and who are the trustees, settlors, beneficiaries involved with a trust. It would also be important to find out for what purpose the corporate vehicle was formed, why foreign jurisdictions are being used for creation/administration of the entity, and why complex structures are being built.

The level of misuse of corporate vehicles could be significantly reduced if the information regarding the ultimate beneficial owner, knowledge of the source of assets and the business objective of the company or a trust within a structure were readily available to the authorities that might need it, especially in situations containing many or all of the "risk indicators" cited on pages 13/14. Since many of the structures are set up and / or managed by trust and company service providers it might be advisable that TCSPs be obliged to gather and maintain the above mentioned information. Some of this is already part of the present FATF-recommendations (at least the identification of the beneficial owner, as well as suspicious transaction reporting).

Another conclusion that may be drawn is that, in theory, it matters less who maintains the required information on corporate vehicles, namely:

- the corporate vehicle itself;
- the trust and company service provider;
- the registrar of companies; or
- another authority;

provided that the information on beneficial ownership exists, that it is complete and up-to-date and that it is available to competent authorities. It is thus an essential corollary that competent authorities – especially across jurisdictional lines – need to know where relevant corporate vehicle information is held and how it can be obtained. Both the OECD and IOSCO have emphasised that it is important for competent authorities to be able to co-operate with other competent authorities within and without their own jurisdiction to share relevant information on beneficial ownership.[77]

Company registers are an important source of information on legal ownership, although they may not always contain the most current information on the corporate vehicle. Nevertheless, as is indicated by the results of the survey, checking company registries is an important first step in obtaining information about the structure of corporate vehicles that are of concern. It is thus important that such registries be as comprehensive and as up-to-date as possible. Similarly, legal ownership information held by other public entities such as filings with financial regulatory authorities or stock exchanges should also be accurate and current.

Individuals and corporate vehicles have legitimate expectations of privacy and business confidentiality in their affairs and, from the information obtained through the survey, it is evident that jurisdictions adopt different approaches to protect legitimate privacy interests.[78] Certain of the arrangements and practices however, including the absence of appropriate regulation/supervision, would appear to contribute to the potential for corporate vehicle misuse by making it very difficult, and perhaps even impossible, for the authorities to identify beneficial owners and controllers.

As with all regulation – and as confirmed by the survey – it appears that there is a need to strike a balance between the need for robust regulation and/or supervision to prevent corporate vehicle misuse and the need to avoid unnecessary restrictions on legitimate business. In developing further guidance for this area, it will be important to consider the

potential impact on overall economic performance, market integrity, market efficiency, market transparency and incentives.

The analysis of the typologies submitted as part of the survey, as well as prior studies relating to this topic,[79] points toward a number of frequently occurring risk factors associated with the corporate vehicle misuse (see Section 2 above). From this can be concluded that the further development of these common risk factors could be useful for countries in determining their own factors that help to identify such misuse and could be used in conjunction with other, existing, diagnostic tools, such as the OECD Template and the IOSCO Multilateral MOU. Examples of these factors are included in Figure 6.

Figure 6

Examples of Risk Assessment Factors

1. What are the corporate vehicle formation requirements in the source jurisdiction?

- *Is information concerning the beneficial ownership and control of a company required to be recorded, maintained and kept up-to-date?*
- *Do similar requirements apply concerning information on the settlor or founder, trustee and beneficiaries of a trust or foundation, and the partners of a partnership?*
- *Are regularly updated list of the shareholders, directors and principal officers of all companies required to be maintained?*

2. Are there adequate regulatory and/or AML standards or investigative capacities in the jurisdictions where the corporate vehicle has been incorporated /formed/administered (e.g. particularly in the application to lawyers, accountants and trust and company service providers engaged in the formation and administration of corporate vehicles)?

3. How might information on the beneficial owners be made available, or be obtained, in the jurisdiction of incorporation and/or the country in which the company and trust administration services are provided?

• Is all or some of the information required to be maintained:

*a. On a public register (and how easy it is to obtain the information)? *80*

*b. On a private register available to financial institutions;**

c. On a private register available to regulators/law enforcement agencies (and under what circumstances can they share information available to them with other domestic/foreign regulatory authorities or law enforcement agencies)?

d. By licensed/regulated trust and company service providers (and under what circumstances and to whom are they permitted or required to make information available)?

e. By unregulated trust and company service providers (and under what circumstances and to whom are they permitted or required to make information available)?

f. By the entities themselves (and under what circumstances and to whom are they permitted or required to make information available)?

*• Is there a register (public or otherwise) of the corporations, trusts, foundations and partnerships that are created, incorporated, registered or administered in the jurisdiction?**

• Is the information referred to in the preceding bullet point required to be maintained in:–

(a) The country of creation/incorporation?

(b) The country(ies) of administration or operation (if different to (a))?

(c) Both (a) and (b)?

*4. What is known about the beneficial owner?**

*5. Is the corporate vehicle a regulated or unregulated entity?**

*6. What is the purpose of the corporate vehicle? Does it have 'real' activities (e.g. manufacturing, trading) or is it solely involved with holding/administrating the assets of the beneficial owner?**

*7. If applicable, why has the corporate vehicle been established in a foreign jurisdiction?**

*8. If applicable, why has an individual given up control over his assets to trustees, through the formation of a trust?**

9. What is the purpose behind naming corporate shareholders, nominee shareholders, corporate directors or bearer shares –*

• Are bearer or nominee shares permitted, and if so, is there an effective mechanism that will allow the ultimate beneficial owner of the shares to be ascertained? Who can use this mechanism and with whom can the information be shared?

• Are corporate or nominee directors permitted, and if so, is there an effective mechanism that will allow the person with ultimate control of the company to be ascertained? Again, who can use this mechanism and with whom can the information be shared?

• Is there a requirement that at least one director of the company/trustee of a trust/administrator of a foundation/partner in a partnership must be a natural person resident in the jurisdiction of creation/incorporation/administration?

10. Can shell or shelf companies be formed in the jurisdiction of incorporation?

*11. What is known about the source of funds?**

*12. What is known about the scale of the business/funds?**

*13. Are the business activities unusual, particularly with regard to the nature of the beneficial owners?**

*14. Are there any other unusual features about the structure/business activities of the corporate vehicles?**

15. Are corporate vehicles administered by lawyers, accountants, trust company service providers or other individuals, and are intermediaries identified as the legal owner?

16. Is there a lack of oversight of those engaged in the formation and administration of corporate vehicles (e.g. is there a fit and proper test for those able to form and administer corporate vehicles; is there adequate control over the opening of bank accounts in the name of the corporate vehicles in the jurisdiction where the vehicle is formed)?

17. Do secrecy laws prevent or unduly restrict access to beneficial ownership information?

18. Are financial institutions and intermediaries obliged to obtain beneficial ownership information, and perform customer due diligence at the commencement, and during the course of, a business relationship, in particular when opening an account for a customer?

19. Have competent authorities been designated to oversee and monitor compliance with the requirements referred to in the preceding bullet point, including imposing sanctions for non-compliance where appropriate?

20. Can law enforcement agencies, and financial regulatory authorities, obtain or access beneficial ownership information, and is there evidence of information being obtained on a timely basis:

(a) For their own investigative or regulatory purposes?

(b) Based upon a legitimate request from another domestic or similar foreign authority, and share that information on a timely basis, and without unduly restrictive conditions?

21. Is there evidence of a lack of effective international cooperation exhibited by the authorities in the jurisdictions where the corporate vehicle is formed and/or administered?

22. What are the penalties or other consequences for non-compliance with international standards in the jurisdiction where the vehicle is formed and/or administered?

As suggested by the typologies examined as part of this research, there appear to be two essential factors that further protect against the misuse of corporate vehicles: (1) the quality of available information and (2) the quality of the "gateway" through which that information can be obtained. There is little value in having good gateways if no information on beneficial owners can be obtained. Likewise there is little value in knowing that there is good quality information available when investigators are unable to get access to it.

The conclusions drawn from the typologies are further reinforced by findings made in other sources that were consulted as part of this research project (extracts from these sources are included in Annex 5).

4. Issues for consideration

As stated at the beginning of this paper, the focus of research for this FATF typologies project has been on the beneficial ownership issues that are directly tied to the misuse of corporate vehicles for money laundering purposes. Despite this limited focus, however, the information and typologies examined through the project survey suggest a number of areas that may call for further and separate consideration – by the FATF and/or other relevant international organisations[81] – in preventing corporate vehicles and their activities from misuse by criminals. Some of the most important questions are as follows:

- Are the existing AML/CFT standards as a whole adequate to discourage the misuse of corporate vehicles?
- Are the specific FATF Recommendations 12, 16 and 24 sufficient as a basis for dealing with the issue of corporate vehicle misuse?
- What more can be done to ensure that adequate, accurate and timely information on the beneficial ownership and control of legal persons/legal arrangements may be obtained or accessed in a timely fashion by competent authorities?
- What can be done to ensure that those engaged in the formation and administration of corporate vehicles are "fit and proper"? Is there a need for an international standard for TCSPs or professionals engaged in providing trust and company services?
- What steps can and should be taken to ensure that the actions of those engaged in the formation and administration of corporate vehicles are properly monitored or subject to investigation as necessary?
- Should TCSPs be regulated or should there be enhanced regulation of such service providers, including lawyers and accountants where they offer similar services?
- Should existing corporate governance standards such as OECD Principles) be extended to include factors relating to the role of TCSPs, lawyers and accountants in relation to the potential misuse of corporate vehicles?
- Should guidance in other forms be produced – for example risk assessment check lists – to help the competent authorities focus their risk-based approaches in relation to the different types of misuse of legal persons and legal arrangements?
- Where should beneficial ownership information be held?
- What more needs to be done to enhance the effectiveness of company registers, and other publicly available information?
- Is there any practical action that needs to be or can be taken to enhance the information publicly available in respect of legal arrangements?[82]

This typologies report should be seen as an initial report. It has addressed what is seen as the key issue in limiting the misuse of corporate vehicles – namely who is the beneficial owner and what is the purpose behind the corporate vehicles being used. There are however many matters deserving of further consideration which are further evidence of

the scale and complexity of the issues involved in preventing the misuse of corporate vehicles.

Endnotes:

[1] Organisation for Economic Corporation and Development (OECD), Options for Obtaining Beneficial Ownership and Control Information: A Template (OECD Template) p.7

[2] This report is the product of research carried out by a project team operating under the umbrella of the FATF typologies initiative.

[3] Some jurisdictions, such as the US, do not have a national or nationally uniform system of incorporation or registration of corporations, trusts and other business entities but instead have a dual Federal State or multi-regional systems. References in this report to the laws and principles in such jurisdictions are necessarily generalisations regarding the majority of states or regions, or the most common elements of the specific law or principle referenced.

[4] See the bibliography and Annex 5.

[5] Annex 2 refers to the many legitimate uses for trusts as well as the potential for their misuse.

[6] A copy of the questionnaire used is attached at Annex 7.

[7] See the OECD report *Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes (Behind the Corporate Veil), 2001*.

[8] See the glossary to the FATF Forty Recommendations.

[9] A detailed description of all characteristics of these case studies is included in Annex 4 which was compiled with the considerable assistance of the Netherlands authorities.

[10] A detailed description of all characteristics of these case studies is included in Annex 4.

[11] This relates to cases 1, 2, 3, 12, 16, 17, 24, 25, 26, 27, 28, 29, 31, 32, 33 and 34.

[12] The scheme mostly involves types of financial fraud and Ponzi schemes.

[13] It should be noted that the case studies showed that, unlike most other methods used to launder money, legal entities are used not only to launder money, but also to generate it, e.g. from earnings of a criminal offence (money with illegal origin) or as windfalls (earnings) of tax evasion (money with legal origin).

[14] Other legal structures that could lead to same result are the use of bearer shares and corporate directors.

[15] The participating jurisdictions are listed in Annex 3, along with the abbreviations used hereafter. The analysis was undertaken with the considerable assistance of the World Bank.

[16] In the case studies, varying types of corporate vehicles are referenced, such as *offshore corporate vehicles* (case 3), *limited companies* (case 17), *UK limited companies* (case 19), *limited liability companies* (case 18,19), *corporate vehicles* (case 20), , *shell companies* (case 21), *Nevada corporations* (case 22), *trusts* (case 33 and 34). Both formal terms (e.g. *limited liabilitycompany*) and informal or "popular" terms (e.g. *shell companies*) were used interchangeably.]

[17] FATF Methodology, www.fatf-gafi.org/glossary.

[18] In view of the lack of universally accepted definitions or principles regarding control, beneficial ownership and related concepts, this report does not attempt to provide a detailed analysis of these concepts.

[19] OECD *Behind the Corporate Veil*, 2001, pp. 21.

[20] Id pp. 29-32

[21] This type of ownership was not addressed in the survey, but the layering of different corporate entities on top of each other is a common characteristic in many cases of misuse of corporate vehicles, and hence it is included here. Of

course this is not so much a "practice", but rather a logical characteristic of corporate law; anyone can hold shares, be it a natural person or a legal entity.

[22] This type of ownership was also not addressed in the survey. It is included here because two jurisdictions mentioned this issue (GI and IM). Of course ownership through nominee shareholders being simply a contractual relationship, it is possible in any jurisdiction that does not explicitly prohibit it, and this type of ownership is necessary for any broker trading on a stock exchange where shares are held on behalf of a client.

[23] A majority of bearer shares are book entries and are "dematerialised". Shares are dematerialised when they are registered. Dematerialisation is achieved by requiring registration upon transfer or requiring registration in order to vote the shares or collect their dividends. While physical transfer of bearer shares is possible it is believed to be rare.

[24] A majority of the bearer shares are *book entries* and are dematerialised. While physical transfer of bearer shares is possible it is believed to be rare.

[25] Some of the bearer debt in the United Kingdom is dematerialised, while another part of it is immobilised in International Central Securities Depositories (ICSD). The records of the ICSDs cannot be inspected.

[26] Shares are dematerialised when they are registered. Dematerialisation is achieved by requiring registration upon transfer or requiring registration in order to vote the shares or collect their dividends.

[27] Of course ownership will in many cases entail (a degree of) control. This paragraph deals only with those relationships of

[27] Of course ownership will in many cases entail (a degree of) control. This paragraph deals only with those relationships of control that do not derive from ownership.

[28] OECD. *Behind the Corporate Veil 2001* pp. 31.

[29] In some jurisdictions this representative can be liable for civil and criminal penalties. It is unclear from the questionnaires which jurisdictions in fact enforce these penalties.

[30] Legislation requiring that at least one natural person serve on the board is pending in the UK.

[31] VI has passed legislation requiring that at least one natural person serve on the board.

[32] Jurisdictions may have nominee directors, but this was not addressed in the survey.

[33] The item on the questionnaire reads "Are corporate directors possible?"

[34] NL, noting risk mitigation factors that effectiveness is limited to domestic corporate directors.

[35] GI, noting that the concept of nominee directors "does not exist in law". IM and TR also indicated permission of nominee directors.

36 OECD *Behind the Corporate Veil*, 2001, pp. 31.

37 IM.

38 IM.

[39] OECD Behind the Corporate Veil, 2001 pp. 25-26.

[40] GG,IM,MH,HK,UK,QA,MY,GI,NO,PW,MA,NZ,JE,VI,JP,BA,US. Other countries may recognize trusts pursuant to the Hague Convention on the Law applicable to Trusts and on their Recognition.

[41] OECD *Behind the Corporate Veil*, 2001, pp. 41-42.

[42] GI, MY, CH, US, LT, SK, MA, QA, HK, FR, TR, LB, BE, VI, NL.

[43] BA, noting how it obtains information on ownership of companies.

[44] MY, GI, SK, MO, GG, BH, LB and JE require upfront disclosure with respect to beneficial ownership prior to start up. However, for GG, BH and LB, this information is not required to be updated. Only JE reported an explicit requirement that information on beneficial ownership be updated.

[45] NL,GI,MY,CH,US,SK,NZ,MO,ES,QA,DE,DK,PW,TR,LB,FR,JP,AU,BE,BA.

[46] NL,GI,MY,US,SK,NZ,MO,BH,ES,IM,QA,UK,HK,MH,DE,DK,PW,LB,FR,JE,VI,AU,BE,BA.

[47] For GI,MY and HK it is unclear whether registration is required.

[48] GI,MY,SK,NZ,MO,MA,BH,IM,UK,HK,DK,TR,LB,FR,JE,BE,BA,CH.

[49] JE, noting how it obtains information on the beneficial owner.

[50] BH,TR and JP did not report that the registries were open for public inspection, although they indicated that the registries could be accessed through investigatory means.

[51] VI

[52] NL, MY,LV,BH,GG

[53] *Behind the Corporate Veil*, 2001 pp. 50 (company formation agents, trust companies, lawyers, notaries, trustees, and other professionals).

[54] NL,GI,MY,CH,MA,GG,IM,UK,HK,JE,VI,BA

[55] NL,GI,NO,CH,MA,GG,IM,JE,BA

[56] NL,GI,NO,MY,CH,MA,GG,IM,UK,HK,DE,QA,LT,JE,VI,AU,BA

[57] JE, noting penalties regulatory bodies may impose on TCSPs

[58] GI, NO, MY, CH, US, LT, MO, LV, MA, BH, GG, IM, QA, UK, HK, MH, FR, DE, DK, PW, TR, LB, AU, NL, JP, VI, BE, BA, JE. Out of these, LT, GG, VI, NL and JP do not allow accountants to participate in these functions.

[59] MY, LT, HK, FR, AU, BE. BA noted that AML applies to all its citizens in compulsion for information but did not state any specific facts regarding lawyers, accountants, and notaries.

[60] MY, HK, BE

[61] MY, MO, LV, UK, HK, TR, LB, FR, JP, BE

[62] BA, noting the importance of financial institutions gaining BO information

[63] NO, US, SK, LV, QA, MH, DE, DK, PW, TR, LB, JP, AU, BE

[64] US,NL,UK,PW,SK,NL all noted the information on beneficial ownership could be obtained through tax returns.

[65] US noted availability of information from Dunn & Bradstreet, Lexis/Nexis, and Choicepoint.

[66] NO, noting its difficulties in using acquired intelligence information.

[67] MO.

[68] See cases 4, 10, 11, 17, 19

[69] For example, MY, noting that TCSPs are not required to give information to investigators unless a warrant is obtained.

[70] Id.

[71] TR,LB.

[72] LV,MO,FR,VI,BE.

[73] Note: there are a number of current international initiatives to improve the ability of regulatory authorities to share information (e.g. IOSCO).

[74]NL,GU,NO,MY,CH,LT,SK,MO,LV,MA,BH,GG,IM,QA,UK,HK,MH,DE,PW,TR,LB,FR,JE,JP,AU,BE, VI,BA, US

[75] GI,NO,MY,MA,IM,HK,PW,LB,JP

[76] NL,GI,LV,MA,GG,HK,LB

[77] OECD, Options for Obtaining Beneficial Ownership and Control Information: A Template (OECD Template) Annex 1, p33; IOSCO, Multilateral Memorandum of Understanding Concerning Consultation and Co-operation and the Exchange of Information (IOSCO Multilateral MOU); and IOSCO, Methodology for Assessing Implementation of the IOSCO Objectives and Principles of Securities Regulation, Principles 11-13.

[78] OECD Template 2002, Annex 2, p34.

[79] Id.

[80] Items marked by an asterisk should also be of particular interest to financial institutions when undertaking CDD in respect of corporate vehicles seeking to use their services.

[81] For example, the OECD, who have already conducted extensive work in this area

[82] See Annex 2 for information on the South African system for registering the information on trusts.

The full text can be accessed at the following link:
Report on Misuse of Corporate Vehicles Published

Appendix VIII - Extracts from the FATF October 2006 Report on New Payment Methods

Executive Summary

New and innovative methods for electronic cross-border funds transfer are emerging globally. These new payment tools include extensions of established payment systems as well as new payment methods that are substantially different from traditional transactions. New payment methods raise concerns about money laundering and terrorist financing because criminals can adjust quickly to exploit new opportunities.

The present study analyzes prepaid cards; Internet payment systems; mobile payments; and digital precious metals in order to: (1) Identify trends in the adoption of new payment technologies; (2) Assess money laundering (ML) and terrorist financing (TF) vulnerabilities; and (3) Determine whether the Financial Action Task Force (FATF) Forty Recommendations and Nine Special Recommendations (40 + 9) adequately address any potential vulnerabilities.

The study found there is a legitimate market demand served by each of the payment methods analysed, yet potential money laundering and terrorist financing vulnerabilities do exist. Specifically, offshore providers of new payment methods may pose additional money laundering and terrorist financing risks compared with service providers operating within a jurisdiction.

While it is believed that the FATF 40 + 9 provide the appropriate guidance to address the vulnerabilities associated with these new methods of payment, the study does suggest further examination of the effect these evolving technologies may have on cross-border and domestic regulatory frameworks in order to ensure their compatibility with the FATF 40 + 9.

2. Background

How payment system innovations emerge is associated with a number of factors specific to each country, including the underlying economic environment, technology, preferences, actual and perceived costs, along with regulations, policies, and practices of government and private entities with significant influence on the payments system. The fundamental trend, however, across all nations is the migration from paper to electronic payments.

Moving away from paper payments to standardized electronic transaction processing has had the effect of breaking down the payment system into distinct business segments. Hardware, software, communications lines, systems management, accounting, marketing, and distribution have all emerged as distinct business lines for distinct payment services. This segmentation, and the specialization that has resulted, has led to the entry of for clearing services.[10[

While banks remain the core providers to end-users for most retail payment instruments and services, payment applications are now available from a wider range of service providers. The move from paper to electronic transactions has enabled non-bank service providers to customize their payment instruments and to package them with complementary products in order to serve niche markets.

Non-banks now serve as Internet payment portals, transferring payments between payers, payees and their account-holding institutions. Non-bank intermediaries also transfer payments between buyers and sellers who transact through Internet retail storefronts and through online auction sites. Nonbanks, in fact, pervade the payments industry, processing transactions, maintaining databases, and even operating as value providers in e-money schemes. The result is that "the line between the direct provision of retail payment services to end users by non-banks and the provision of related support services to users and payment providers is much less clear than in the past."[11]

Traditional and Non-traditional Retail Payments

Traditional retail payments are generally low-value, consumer payments that do not require immediate settlement.[12] Traditional electronic payments include bank payment products and services and money transfers that are carried out through nonbank intermediaries such as Western Union, which generally work as credit transfers but do not rely directly upon the transfer of funds between bank accounts.

The FATF defines a money or value transfer system as a "financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer system belongs."[13]

Supplementing these traditional retail payments are newer, innovative payment products, or non-traditional retail payments. For the purposes of this report, we refer to these types of payments as "new payment methods", although they are also often referred to as "e-money" by international payments system experts. NPMs include a variety of innovative products that involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems. NPMs also include products that do not rely on traditional payment systems to transfer value between individuals or organizations.[14] This report considers the following NPMs: prepaid cards, electronic purses, mobile payments, Internet payment services, and digital precious metals. Table 1 below provides for a schematic distinction, amongst NPMs, between those that are an extension of traditional payment instruments and those which are *strictu senso* new payment methods.

10 Clearing and Settlement Arrangements for Retail Payments in Selected Countries, Committee on Payment and Settlement Systems,

NPM Money Laundering and Terrorist Financing Risks

Payment Method	Potential Risk Factors	Current and Potential Risk Mitigants
Prepaid cards: open system	▪ Anonymous card holder ▪ Anonymous funding (inflow) and anonymous access to funds (outflow) ▪ High card value limit and/or no limit on the number of cards an individual can acquire ▪ Access to cash globally through ATMs ▪ Offshore issuers may not observe laws in all jurisdictions	▪ Verify cardholder identification ▪ Limit funding options ▪ Limit card value and/or the number of cards that an individual can acquire and/or value per transaction ▪ Limit cross-border access to cash ▪ Monitor transactions and report suspicious activity ▪ Implement a card/account block ▪ Limit access to network by undesirable merchants and ATM providers/networks
Prepaid cards: closed system	▪ Anonymous card holder ▪ Anonymous funding ▪ High card value limit ▪ Substitute for bulk cash smuggling ▪ No limit on the number of cards an individual may purchase	▪ Verify cardholder identification ▪ Limit card value and/or the number of cards any one purchaser may acquire ▪ Limit funding options ▪ Monitor transactions and report suspicious activity ▪ No direct cash access via ATM ▪ Implement a card/account block
Electronic Purse	▪ Anonymous card holder ▪ Anonymous funding and receipt of funds ▪ High card value limit ▪ No transaction record	▪ Verify cardholder identification ▪ No card-to-card transfer capability ▪ Limits on the amounts that can be spent/stored ▪ Limited cross-border functionality ▪ Limit funding options ▪ Monitor transactions and report suspicious activity ▪ Implement a card/account block
Mobile payments	▪ Anonymous accounts ▪ Anonymous funding and receipt of funds ▪ High or nonexistent account funding limit	▪ Account holders are identified when phones are used ▪ as an access device to a bank or credit card account or ▪ when the telecom verifies phone owner identification ▪ Limited cross-border functionality ▪ Limited account and

		transaction value ▪ Limit funding options ▪ Monitor transactions and report suspicious activity ▪ Implement a card/account block ▪ Limit access to network
Digital precious metals	▪ Anonymous accounts ▪ Anonymous funding and receipt of funds ▪ High or nonexistent account funding ▪ limit ▪ Offshore service providers may not ▪ observe laws in other jurisdictions	▪ Identify account holder ▪ Maintain transaction record with payer and recipient ▪ Monitor transactions and report suspicious activity ▪ Limit funding options ▪ Implement account block ▪ Limit access to service
Internet payment systems	▪ Anonymous accounts ▪ Anonymous funding and receipt of funds (ATM) ▪ High or nonexistent account funding limit ▪ Offshore service providers may not observe laws in other jurisdictions	▪ Identify account holder ▪ Maintain transaction record identifying payer and recipient ▪ Monitor transactions and report suspicious activity ▪ Limit funding options ▪ Implement account block ▪ Limit access to the service

7. Conclusions and Issues for Further Consideration

The answers provided by countries to the questionnaire that was sent at the beginning of this study, reflected a legitimate market demand served by each of the payment methods analyzed, yet some actual and potential ML and TF vulnerabilities do exist. The FATF 40+9 Recommendations seem to allow for the pursuit of payment system innovation and AML/CFT, since they provide for the needed degree of flexibility in the application of AML/CFT standards to new emerging technology-based payment methods.

Among the main risk factors identified, specifically, this study notes that providers of new payment methods that are located outside the jurisdiction of a given country may pose additional risks compared with domestic service providers, especially when: (i) the distribution channel used is the Internet; (ii) no face-to-face contact with the customer takes place; and (iii) the NPM operates through an open network that can be accessed in a high number of jurisdictions.

The extent to which the new payment methods identified in this study are used for illegitimate purposes is difficult to determine at this time. The responses to the questionnaire issued by the project team provide only a limited number of typologies and show that the level of development and/or awareness of new payment methods is not uniform across the world. In this regard it should be noted that new payment methods are developing quickly and considerably; law enforcement cases may consequently increase as well in the near future.

As previously noted, it is believed that the FATF Forty Recommendations and Nine Special Recommendations provide an appropriate framework to address the vulnerabilities associated with these new methods of payment that have been identified by the project team. However, given the different characteristics and development that new payment methods may have in each jurisdiction, the study does highlight an opportunity for further examination of specific measures that could be adopted by countries to limit identified risks. In the case of new payment methods, technology plays a twofold role: on the one hand, it may increase typical ML/TF risks (i.e. anonymity, global use, speed of transfers, legal arbitrages, offshore provision of services) and on the other hand, help prevent or limit such risks (e.g. usage and spending limits, electronic record of transactions, etc.). Such additional measures could be applied in addition to or instead of traditional AML provisions (for example, CDD could be replaced by spending and loading limits on a payment instrument, which would represent thresholds, or by usage limits – such as non-reloadability or geographic limitations in the use of a payment instrument).

In light of the findings of this project, it is recommended that the WGTM considers the following possible future actions on this topic:

a) Providing guidance to jurisdictions as to what preventive measures may be taken to limit the risk of NPMs being used to launder money and/or finance terrorism (this could occur under FATF Recommendation 8);

b) Updating this study on the development of new payment methods as well as the relative typologies and risks analyses after a period of two years;

c) Proposing the inclusion of new payment methods as a specific issue to be monitored – during the two years period mentioned under letter b) above - under the project on ML and TF trends and indicators.

Appendix VIII - Extracts from the FATF October 2006 Report on Trade-Based Money Laundering

http://www.fatf-gafi.org/dataoecd/60/25/37038272.pdf

Issued by Bank of Jamaica
Revised March 2007
Revised May 2006
Revised June 2005
Revised March 2005
Revised and Reissued August 2004
Circulated for discussion and preliminary issue, January & April 2004
Revised and Reissued July/August 2000
Initially issued on 27th July 1995