GUIDANCE NOTES ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

December 2008

These Guidance Notes have been prepared by the Cayman Islands Monetary Authority and the professional associations for general guidance. This document should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions. However, *Financial Services Providers* should be aware of the enforcement powers of the Authority under subregulation 5(4A) of the Money Laundering Regulations as they relate to supervisory or regulatory guidance.

Issued by the Cayman Islands Monetary Authority and the following associations:

The Bankers Association, the Funds Administrators Association; the Company Managers Association; the Insurance Managers Association; and The Society of Trust and Estate Practitioners (Cayman Islands Branch).

The following associations have also indicated that they expect their members to observe these guidance notes insofar as they conduct relevant financial business, within the scope of the regulations:

Cayman Islands Real Estate Brokers Association, the Cayman Islands Society of Professional Accountants, the Cayman Islands Law Society, the Caymanian Bar Association and the Cayman Islands Compliance Association.

Contact: Cayman Islands Monetary Authority
Elizabethan Square
P.O. Box 10052
Grand Cayman KY1-1001
Cayman Islands

Tel: 345-949-7089 Fax: 345-945-6131
Website: www.cimoney.com.ky Email: CIMA@cimoney.com.ky

FOREWORD

The Cayman Islands as a leading international financial centre has framed its regulatory system around international standards of supervision and co-operation with overseas regulatory authorities in the fight against financial crime. The Islands seek to maintain their position as a premier jurisdiction, while at the same time ensuring that its institutions can operate in a competitive manner.

The Monetary Authority is particularly aware of the global nature of the fight against money laundering (ML), terrorist financing (TF) and other financial crime, and the consequent need for all jurisdictions to operate their regulatory regimes co-operatively and compatibly with each other. This is both to limit opportunities for "regulatory arbitrage" by criminals and to promote an internationally level playing field for legitimate businesses. Where jurisdictions have relevant and appropriate regulatory regimes of an equivalent standard to that of the Cayman Islands, and this is recognised by their inclusion in Schedule 3 due reliance may be placed by a Cayman Islands Financial Service Provider on application of the regulatory regime of that jurisdiction by those subject to such regulation.

These Guidance Notes provide guidelines that should be adopted by those involved in the provision of financial services in order to maintain the integrity of the Cayman Islands' financial sector in respect of money laundering and terrorist financing. For the purposes of providing guidance to the industry with respect to money laundering, these notes replace the Code of Practice, which was previously issued under the Proceeds of Criminal Conduct Law (2005 Revision). The Code of Practice has been withdrawn and should no longer be referred to as a point of guidance to the industry.

These guidance notes are based on similar Guidance Notes issued by the UK and some of the Overseas Territories and Crown Dependencies, modified to accord with the laws of the Cayman Islands. The Cayman Islands are grateful to these countries for allowing them to draw on their guidance notes as well as to the authors of the Code of Practice.

The Cayman Islands Monetary Authority stands ready to discuss individual cases with *Financial Services Providers* to assist in practical implementation. We hope that you find the enclosed guidelines of assistance.

CONTENTS

SECTION 1 - INTRODUCTION

1.1 Having an effective anti-money laundering (AML) / countering the financing of terrorism (CFT) regime has become a major priority for all jurisdictions from which financial activities are carried out. One of the best methods of preventing and deterring money laundering and terrorist financing is a sound knowledge of a customer's business and pattern of financial transactions and commitments. The adoption of procedures by which *Financial Services Providers* "know their customer" is not only a principle of good business but is also an essential tool to avoid involvement in money laundering and terrorist financing. For the purposes of these guidance notes the term *Financial Services Providers* refers to businesses carrying on *relevant financial business* as defined under the legislation.

1.2 These Guidance Notes are designed to assist *Financial Services Providers* in complying with the Cayman Islands Money Laundering Regulations. It is recognised that *Financial Services Providers* may have systems and procedures in place which, whilst not identical to those outlined in these Guidance Notes, nevertheless impose controls and procedures which are at least equal to, if not higher than, those contained in these Guidance Notes. This will be taken into account by the Monetary Authority in the assessment of a *Financial Services Provider's* systems and controls and compliance with the Regulations.

1.3 An overriding aim of the Money Laundering Regulations and these Guidance Notes is to ensure that appropriate identification information is obtained in relation to the customers of Financial Service Providers and the payments made between them. This is both to assist the detection of suspect transactions and to create an effective "audit trail" in the event of an investigation subsequently proving necessary. Given the increasingly international character of legitimate financial business, there will be many circumstances where payments to and from a Financial Service Provider will quite properly be received in accounts and/or processed in one or more jurisdictions other than the Cayman Islands. Where such payments are received or processed by or on behalf of a Financial Service Provider by a person or institution in a Schedule 3 country that is subject to the regulatory regime therein, compliance by such persons or institutions with the requirements of such Schedule 3 country in respect of the transactions carried out for the Financial Service Provider shall be regarded as compliance with the Regulations and Guidance Notes of the Cayman Islands. The Monetary Authority may at any time require written evidence from the Financial Service Provider of the suitability of any person or institution operating anti-money laundering procedures on its behalf in another jurisdiction and of the nature of those procedures pursuant to the foregoing provisions, together with confirmation of the regulatory status of such person or institution.

1.4 In some respects, these Guidance Notes go beyond the requirements of the Money Laundering Regulations. Nonetheless, it is expected that all institutions conducting *relevant financial business* pay due regard to all the Guidance Notes in developing

responsible anti-money laundering and terrorist financing procedures suitable to their situation. If a *Financial Services Provider* appears not to be doing so the Monetary Authority will seek an explanation and may conclude that the *Financial Services Provider* is carrying on business in a manner that may give rise to sanctions under the applicable legislation.

1.5 It is important that the management of *Financial Services Providers* view money laundering and terrorist financing prevention as part of their risk management strategies and not simply as a stand-alone requirement that is being imposed by the legislation. Money laundering and terrorist financing prevention should not be viewed in isolation from an institution's other business systems and needs.

1.6 Throughout these Guidance Notes there is reference to an 'account' or 'accounts' and procedures to be adopted in relation to them. This is a matter of convenience and has been done for illustrative purposes. It is recognised that these references may not always be appropriate to all types of *relevant financial business* covered by the Regulations. Where there are provisions in these guidelines relating to an account or accounts these will have relevance to mainstream banking activity but should, by analogy, be adapted appropriately to the situations covered by other relevant business. For example 'account' could refer to bank accounts, mutual funds or other investment product, trusts or a business relationship etc.

1.7 This document provides references to other web sites for convenience and informational purposes only. Referenced web sites are not under the control of the Cayman Islands Monetary Authority or any of the other members of GNC, and thus the members of GNC are not responsible for the contents of any referenced site or any link contained in a referenced site, or any changes or updates to such sites. GNC members are not responsible for any transmission received from a referenced site. The inclusion of a reference site does not imply endorsement by the GNC of the site, its content, advertisers or sponsors. External sites may contain information that is copyrighted with restrictions on reuse. Permission to use copyrighted materials must be obtained from the original source and cannot be obtained from the GNC.

WHAT IS MONEY LAUNDERING?

1.8 Money laundering is the process by which the direct or indirect benefit of crime is channelled through financial institutions to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the money can lose its criminal identity and appear legitimate.

1.9 In basic terms, the money launderer wants to:-

(a) place his money in the financial system, without arousing suspicion;

(b) move the money around, often in a series of complex transactions crossing multiple jurisdictions, so it becomes difficult to identify its original source; and
(c) then move the money back into the financial and business system, so that it appears as legitimate funds or assets.

A more detailed analysis of the background to money laundering, the processes the launderer follows, and international initiatives to prevent it, are included as Appendices A, and B respectively.

WHAT IS TERRORIST FINANCING?

1.10 Terrorism is the unlawful threat of action designed to influence the government or intimidate the public for the purpose of advancing a political, religious or ideological cause. These actions include serious violence against a person, endangering a person's life, serious damage to property, creating serious risk to public health and safety, or serious interference with or disruption to an electronic system. By contrast, financial gain is the main objective of other types of financial crimes. Nonetheless, terrorist groups, like criminal organisations, must develop sources of funding, a means of laundering those funds, and a way of using those funds to obtain materials and logistical items to commit terrorist acts.

1.11 Sources of funding for terrorism could be unlawful sources such as kidnapping, extortion, smuggling, various types of fraud (e.g. through credit cards or charities), thefts and robbery, and narcotics trafficking. *Financial Services Providers* must be aware however, that funding for terrorist groups, unlike for criminal organisations, may also include funds derived from legitimate sources or from a combination of lawful and unlawful sources. This funding from legal sources is a key difference between terrorist groups and traditional criminal organisations.

1.12 A terrorist group needs to obscure or disguise links between it and its legitimate funding sources. It must therefore find ways of laundering the funds in order to be able to use them without drawing the attention of authorities. Some of the particular methods detected with respect to various terrorist groups include: cash smuggling (both by couriers or bulk cash shipments), structured deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments (travellers' cheques, bank cheques, money orders), use of credit or debit cards, and wire transfers. There have also been indications that some forms of underground banking (particularly the *hawala* system) have had a role in moving terrorist related funds. While underground banking may not play a major role in the domestic economy, *Financial Services Providers* should be aware of their existence and develop procedures for identifying transactions that may be linked to such systems.

1.13 The Terrorism Law, 2003 defines the offence of terrorism and criminalises the act of terrorism. The law applies to actions, person, property, or both inside and outside of the

Cayman Islands. Any person who believes or suspects that another person has committed an offence under the law must disclose this information to the FRA or to a constable as soon as is reasonably practical. Failure to do so is an offence and is liable a) on summary conviction, to imprisonment for two years and a fine of four thousand dollars; or b) on conviction on indictment, to imprisonment for fourteen years, and to a fine. The court may also make a forfeiture order.

1.14 Financial Services Providers should take note of their obligations under The Al-Qa'ida and Taliban (United Nations Measures) Order 2002, made in the UK, pursuant to Article 41 of the Charter of the United Nations (and extended to the Cayman Islands). Particular attention should be given to that section of the Order regarding "Funds" :

- Making funds available to Osama bin Laden and associates (article 7);
- Freezing of funds (article 8);
- Facilitation of activities prohibited under article 7 or 8 (article 9); and
- Failure to disclose knowledge or suspicion of measures offences (article 10).

1.15 Related information can be found through the UN website link provided in Appendix L.

AREAS OF CONCERN

1.16 No financial sector is immune from the activities of criminals and all *Financial Services Providers* should consider the money laundering and terrorist financing risks posed by the products and services that they offer, and devise and document their procedures with due regard to that risk.

1.17 Historically money laundering and terrorist financing have been concentrated on the traditional banking sector. However criminals have responded to the measures taken by banks and have sought to convert illegally earned funds or mix them with legitimate income before they enter the banking system, thus making them harder to detect. Non-bank financial institutions have become increasingly vulnerable to being used for money laundering.

1.18 The highest risk category relates to those products or services where unlimited third party funds can be freely received, or where funds can be regularly paid to, or received from third parties without evidence of identity of the third parties being taken. Examples of products in the highest risk category are, products offering money transfer facilities through chequebooks, telegraphic transfers, deposits from third parties, cash withdrawals, credit and debit cards or other means.

1.19 Some of the lowest risk products are those in which funds can only be received from a named investor by means of a payment from an account held in the name of the investor, and where the funds can only be returned to the named investor. No third party funding

or payments are possible. However, despite their apparent low risk, they are not immune from money laundering. The geographical location of a *Financial Services Provider's* customer base will also affect the money laundering risk and terrorist financing analysis. *Financial Services Providers* that have a significant proportion of their customer base located in countries:

- without equivalent money laundering strategies; or
- where cash is the normal medium of exchange; or
- where there is a politically unstable regime with high levels of public or private sector corruption; or
- that are known to be drug producing or drug transit countries,

will need to ensure that additional 'Know Your Customer' (KYC) and/or monitoring procedures are in place to manage the enhanced risks of money laundering. Countries with equivalent AML/CFT strategies are listed in Schedule 3 of the Regulations (see Appendix C). This list represents countries which are considered by the *Monetary Authority* to have enacted legislation to safeguard their financial systems and to combat money laundering to the required standard and equivalent to legislation enacted in the Islands.

NEED FOR VIGILANCE

1.20 All institutions should be constantly vigilant in deterring criminals from engaging in any form of money laundering or terrorist financing. Although the task of detecting crime falls to law enforcement agencies, *Financial Services Providers* will be called upon to assist law enforcement agencies in the avoidance and detection of money laundering and terrorist financing activities and to react in accordance with the law in the reporting of knowledge or suspicion of such.

1.21 Financial Service Provider may evidence due diligence by ensuring that the following systems are in place:

- Training of key staff (where a Financial Services Provider has any staff)
- Procedures for the determination and confirmation of the true identity of customers requesting their services and the nature of business that the customer expects to conduct;
- Ongoing monitoring of business relationships;
- The recognition and reporting of suspicious activities to the *Reporting Authority*;
- Maintenance of records for the prescribed period of time;

- Close liaison with the *Reporting Authority* in relation to suspicious activity reporting and with the *Monetary Authority* on matters concerning vigilance policy and systems; and
- Ensuring that internal auditing and compliance departments regularly monitor and make recommendations for the up date of vigilance systems.

1.22 Due to the diversity of *Financial Services Providers*, the nature and scope of their vigilance systems will vary according to the size and nature of the institution. However, irrespective of these factors, all institutions must exercise sufficient vigilance to ensure consistency with the procedures as outlined in these Guidance Notes.

1.23 The "Appropriate Person" as defined in the legislation will be referred to in these guidance notes as the *Money Laundering Reporting Officer (MLRO).* Vigilance systems should enable staff to react effectively to suspicious circumstances by reporting them to the relevant *MLRO* within the organization as described in Section 6 "Training and Awareness." Staff should be adequately trained to enable them to identify such activity and be trained in the internal reporting systems required for compliance with the regulations. Staff training should be documented and will be subject to regulatory review. It is "good practice" for all institutions to maintain and regularly review their instruction manual for all employees relating to entry, verification and recording of customer information and reporting procedures.

1.24 The *MLRO* should be a member of staff at management level who acts as the main point of contact with the *Reporting Authority* and who has the authority to ensure internal compliance with the regulations.

1.25 In dealing with customers the duty of vigilance starts with the commencement of a business relationship or a significant one-off transaction and continues until that relationship ends. However, the keeping of records upon the cessation of the relationship must be in conformity with the record keeping procedures outlined in these Guidance Notes.

1.26 *Financial Services Providers* should not hesitate from asking their customers "awkward" questions in circumstances of unusual activity. Any failure by the customer to provide credible answers will almost always give grounds for further enquiry about his activities, make the *Financial Services Provider* reconsider the wisdom of doing business with him and, potentially, lead to a suspicious activity report being made.

COMPLIANCE CULTURE

1.27 It is recognised that *Financial Services Providers* exist to make a profit. Nevertheless, each *Financial Services Provider* should give due priority to establishing and maintaining an effective compliance culture.

1.28 The business objectives of customer care are closely aligned to the regulatory objectives of the KYC principle. Similarly linked are the philosophies behind the regulatory objectives of protecting the reputation of the Cayman Islands and the commercial desirability of protecting the reputation of individual corporations.

1.29 In these respects all *Financial Services Providers* are urged to give much consideration to ensuring that they encourage an open and welcoming approach to compliance and AML/CFT issues amongst staff and management.

1.30 Where a financial services provider in the Cayman Islands operates branches or controls subsidiaries, agencies or representative offices in another jurisdiction, it should:

- ensure that such entities observe the AML/CFT standards established in the laws, regulations, and Guidance Notes of the Cayman Islands, or adhere to local standards if those are at least equivalent;
- keep all such entities informed as to current group policy; and
- ensure that each such entity informs itself as to its own local reporting point equivalent to the FRA in the Cayman Islands, and that it is conversant with procedures for reporting suspicions activities equivalent to Section 5 (under the subheading: Reporting Suspicions to the Reporting Authority) of these Guidance Notes.

1.31 Licensees should inform the Authority if the local applicable laws and regulations prohibit the implementation of these standards.

SECTION 2 - CAYMAN ISLANDS LEGISLATIVE AND REGULATORY FRAMEWORK

OUTLINE OF THE OFFENCES

2.1 The legislation specifically relating to money laundering and terrorist financing is contained in the Proceeds of Crime Law, (2008), the Misuse of Drugs Law, (2000 Revision) and the Terrorism Law, 2003.

2.2 The money laundering offences are, in summary:

- Providing assistance to another in an arrangement, which helps him to retain or control benefits of his criminal conduct. This may be by concealment, removal from the jurisdiction, transfer to nominees or otherwise. In relation to drug trafficking this offence is to be found in Section 47 of the Misuse of Drugs Law, 2000 Revision; and in respect of other serious offences it is to be found in section 134 of the Proceeds of Crime Law (2008) and Section 22 of the Terrorism Law, 2003.

- For a person to be convicted of this offence, he must know or suspect, or have reasonable grounds for knowing or suspecting, that the other person is someone who is or has been engaged in criminal conduct.(See Section 136 of the Proceeds of Crime Law (2008) and Section 19 of the Terrorism Law 2003).

- The acquisition, possession or use (even temporary) of property knowing that it represents the proceeds of criminal conduct. This is to be found in Section 135 of the Proceeds of Crime Law (2008) and Section 48 of the Misuse of Drugs Law, 2000 Revision.

- Section 133 of the Proceeds of Crime Law (2008) creates the offence of concealing or disguising property, which is the proceeds of criminal conduct, or converting or transferring that property or removing it from the jurisdiction. The section applies to a person's own proceeds of criminal conduct or where he knows or has reasonable grounds to suspect that the property he is dealing with represents the proceeds of another's criminal conduct. Under section 22 of the Terrorism Law, 2003 a person commits an offence if he "enters into or become concerned in an arrangement that facilitates the retention or control by or on behalf of another person of terrorist property by concealment, by removal from the jurisdiction or by transfer to nominees."

- Tipping off the target or a third party about an investigation or proposed investigation into money laundering, any matter, which is likely to prejudice such an investigation or a report to the *Reporting Authority* (See Section 139 of the Proceeds of Crime Law (2008)).

- Failure to make a disclosure to the *Reporting Authority* as soon as reasonably practicable after knowledge or suspicion of money laundering comes to a person's attention in the course of his trade, profession, business or employment, is an offence. This is to be found in Section 136 of the Proceeds of Crime Law (2008). Section 23(2) of the Proceeds of Crime Law (2008) further states that, notwithstanding any other law to the contrary, the Reporting Authority shall receive all disclosures of information concerning money laundering and terrorist financing.

2.3 It is not necessary that the original offence from which the proceeds stem was committed in the Cayman Islands if the conduct would also constitute an indictable offence had it taken place within the Islands i.e. an offence, which is sufficiently serious to be tried in the Grand Court.

2.4 No duty is imposed on a *Financial Services Provider* to inquire into the criminal law of another country in which the conduct may have occurred. The question is whether the conduct amounts to an indictable offence in the Cayman Islands or would if it took place in the Cayman Islands. A *Financial Services Provider* is not expected to know the exact nature of criminal activity concerned or that the particular funds in question are definitely those which flow from the crime.

PENALTIES

2.5 Tipping off carries a maximum of 5 years imprisonment and an unlimited fine. Failure to disclose knowledge or suspicion of money laundering carries a maximum penalty of 2 years and an unlimited fine. The other offences carry a maximum penalty of 14 years imprisonment and an unlimited fine. No prosecution may be brought without the consent of the Attorney General.

OUTLINE OF THE DEFENCES

2.6 There are general defences enabling a defendant to prove, for example, that he did not suspect that an arrangement related to the proceeds of criminal conduct or that it facilitated the retention or control of the proceeds by the criminal. There are also specific defences provided by reporting a suspicious transaction. It will not be an offence to act in accordance with an arrangement which would otherwise be a crime if a report is made of the suspicion about the source of the funds or investment. If a disclosure of the arrangement is made before the action in question or volunteered as soon as it reasonably might be after the action, no offence is committed.

2.7 The Proceeds of Crime Law provides that a person making a report does not put himself at risk of prosecution by continuing the relevant action (e.g. immediate execution of a

transaction or a mandate), before receiving a consent to do so from the authorities. Whether or not it will be appropriate for the *Financial Services Provider* to stop the relevant transaction must depend on the circumstances.

2.8 An employee who makes a report to his employer in accordance with established internal procedures is specifically protected by the Proceed of Crime Law, (2008) sections 134, 135 and 136 as well as sections 23 and 24 of the Terrorism Law 2003. .

2.9 There is a risk that efforts to detect money laundering and follow the assets will be impeded by the use of alternative undetected channels for the flow of illegal funds consequent on an automatic cessation of business (because a service provider suspected that funds stemmed from illegal activity). To avoid that risk, *Financial Services Providers* are permitted to report their suspicions to the *Reporting Authority* but continue the business relationship or transaction. In carrying out transactions where an institution is considering making a suspicious activity report, the institution should consider duties owed to third parties such as in the case of a constructive trustee. In such cases, it is recommended that independent legal advice is sought.

2.10 By section 136 of the Proceeds of Crime Law (2008), it is a criminal offence to fail to disclose knowledge or suspicion of money laundering. *Financial Services Providers* should place themselves in a position to assist in the investigation of crime and to benefit from the statutory defence. It is a defence to a charge of committing an offence under section 136 if the person charged had a reasonable excuse for not disclosing the information or other matter in question. Similar provisions are found in Section 23 of the Terrorism Law (2003).

2.11 A report of a suspicious activity made to the *Reporting Authority* does not give rise to any civil liability to the client or others and does not constitute, under Cayman Islands law, a breach of a duty of confidentiality. There are statutory safeguards governing the use of information received by the *Reporting Authority*.

TIPPING OFF

2.12 Disclosure to a third party may constitute a criminal offence if the disclosure is likely to prejudice the investigation and it relates to the fact that a report of a suspicious activity has been made, that a police investigation is under way (or proposed) or that access to information orders under the money laundering legislation have been made or are sought.

2.13 It follows that caution must be adopted in determining what may be disclosed to a client in the event that a report of suspicious activity is made or information obtained about money laundering investigations.

REQUIREMENTS OF THE MONEY LAUNDERING REGULATIONS.

2.14 The *Money Laundering Regulations, (2006 Revision)* require that relevant persons have in place anti-money laundering policies, procedures and practices, as summarised in section 5(1) of the Regulations. *Financial Services Providers* should always refer to the provisions of the Regulations in determining the exact requirements applying to them. It is important to note that under the Money Laundering Regulations, the definition of "money laundering" include acts that constitute "terrorist financing" in sections 19 and 22 to the Terrorism Law, 2008.

2.15 The Regulations are included in these Guidance Notes as Appendix C. Specifically, the Regulations require that relevant persons should not form business relationships or carry out one-off transactions with or for another person unless they:-

(a) Maintain procedures which establish the identity of the *Applicant for Business* in accordance with regulations 7 and 9.

(b) Maintain record keeping procedures in accordance with regulation 12.

(c) Adopt appropriate internal controls and communication procedures in accordance with regulation 14.

(d) Comply with the identification and record keeping requirements of Part VII

(e) Adopt appropriate measures to ensure that employees are aware of and comply with the procedures under paragraph (a), and the enactments of money laundering

(d) Provide appropriate training for employees in accordance with regulation 5 (c).

(e) Establish internal reporting procedures in accordance with regulation 14.

BUSINESSES COVERED BY THE REGULATIONS

2.16 Although the primary legislation applies to all persons and businesses, the Regulations place additional legal and administrative AML/CFT requirements on relevant businesses. The definition of *relevant financial business* as detailed in Regulation 4(1), is:

(a) Banking or trust business carried on by a person who is a licensee under the Banks and Trust Companies Law (2007 Revision);

(b) Acceptance by a building society of deposits made by any person;

(c) Business carried on by a co-operative society within the meaning of the Co-operative Societies Law (2001 Revision).

(d) Insurance business and the business of an insurance manager, an insurance agent, an insurance sub-agent or an insurance broker within the meaning of the Insurance Law (2007 Revision);

(e) Mutual fund administration or the business of a regulated mutual fund within the meaning of the Mutual Funds Law (2007 Revision).

(f) The business of company management as defined in the Companies Management Law (2003 Revision);

(g) Dealers in precious metals and precious stones, when engaging in a cash transaction of fifteen thousand dollars or more, as stated in the Second Schedule of the Money Laundering Regulations; and

(h) Any of the activities set out in Schedule 2 of the Regulations (Appendix C)

SECTION 3 – IDENTIFICATION PROCEDURES

GENERAL

3.1 Two important aspects of knowing your customer are to

(a) be satisfied that a prospective customer is who he/she claims to be; and is the ultimate client.

(b) ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake, and any expected, or predictable pattern of transactions.

3.2 When considering entering into a business relationship, certain principles should be followed when ascertaining the level of identification and verification checks to be completed. See Appendix D for a flow chart summary of the different steps involved.

3.3 Reasonable measures should be taken to obtain sufficient information to distinguish those cases in which a business relationship is commenced or *Relevant Financial Business* is conducted with a person acting on behalf of others. If it is established that a client is acting on behalf of another (this also includes providing to his own client, fiduciary or nominee services or holds funds on "client accounts" which are omnibus accounts) then the procedures for verifying the identity of the *Applicant for Business* as set out in these Guidance Notes should be applied. It is also recognised that the guidance relating to corporate clients (other than those themselves regulated or listed) is principally directed at relatively small, closely controlled private companies without substantial physical activities. There is a distinguishable category of large private enterprise where it may be possible to obtain satisfactory evidence of identity from public sources, in which case the process by which the identity of the client is verified should be approved in writing by senior management of the Financial Service Provider. Copies of the identification evidence should be retained and maintained and made available to the Monetary Authority during the course of on site inspections.

3.4 If the intermediary applicant for business identified in paragraph 3.3 meets both of the following criteria:

a) acts in the course of business in relation to which an overseas regulatory authority exercises regulatory functions; and
b) is based or incorporated in or formed under the law of a country specified in a Schedule 3 country,

then the *Financial Services Provider* should require the *Applicant for Business* to complete and sign the *Eligible Introducers* form in appendix F or its functional

equivalent. If the intermediary *Applicant for Business* does not meet the above criteria, then full KYC procedures as outlined in these guidance notes should be followed.

3.5 There are situations in which a client is dealing in his own name on behalf of his own clients; for example, an attorney may himself enter into an arrangement on behalf of his client or a fund manager may operate an account with a bank for the benefit of a number of clients not identified to the *Financial Services Provider*. In this sort of case the intermediary is the *Applicant for Business* of the *Financial Services Provider* rather than the underlying clients for which the intermediary acts.

3.6 The position of the intermediary *Applicant for Business* must be distinguished from that of a person (an 'introducer') who introduces a client (which may also be his client). The Introducer may then withdraw from the business relationship established with the person he has just introduced or may provide other collateral services for him, for example by passing on instructions. The person who is being introduced is the *Applicant for Business* of the *Financial Services Provider*. It is the identity of the introduced *Applicant for Business* which must then be established.

3.7 Whenever appropriate and practical the prospective customer should be interviewed personally. If the prospective client fails or is unable to provide adequate evidence of identity or in circumstances in which the *Financial Services Provider* is not satisfied that the transaction for which it is or may be involved is bona fide, an explanation should be sought and a judgment made as to whether it is appropriate to continue the relationship, what other steps can be taken to verify the client's identity and whether or not a report to the *Reporting Authority* ought to be made.

In circumstances in which the relationship is discontinued, funds held to the order of the prospective client should be returned only to the source from which they came and not to a third party.

Financial Services providers should have polices and procedures in place to address any specific risks associated with non-face to face business relationships and transactions.

3.8 Below are the key principles that *Financial Services Providers* should follow. Verification of identity is a cumulative process. Except for small one-off transactions, it is not sufficient to rely on a sole piece of evidence of identity.

DIRECT PERSONAL CLIENTS

(a) Identification

3.9 It will be normally be necessary to obtain the following documented information concerning direct personal customers subject to paragraph 3.68.

(i) full name/names used;
(ii) correct permanent address including postcode, (if appropriate);
(iii) date and place of birth;
(iv) nationality;
(v) occupation;
(vi) the purpose of the account;
(vii) estimated level of turnover expected for the account; and
(viii) the source of funds (i.e. generated from what transaction or business.)

3.10 In the case of non-resident prospective clients, identification documents of the same sort which bear a photograph and are pre-signed by the client should normally be obtained. This evidence should, where possible, be supplemented by a bank reference with which the client maintains a current relationship or other appropriate reference. *Financial Services Providers* should be aware that other identifying information when practicable, for example, a social insurance number could be of material assistance in an audit trail. In any event, the true name, current address or place of business date of birth and nationality of a prospective client should be recorded.

3.11 Nationality should be established to ensure that the *Applicant for Business* is not from a nation that is subject to sanctions by the United Nations or similar prohibition from any other official body or government that would prohibit such business being transacted. Information on the status of sanctions can be obtained from the Foreign and Commonwealth Office in the UK, for which the website address is http://www.fco.gov.uk. Other useful websites include: http://www.un.org; http://www.fbi.gov, http://www.ustreas.gov.

3.12 Obtaining a date of birth provides an extra safeguard if, for example, a forged or stolen passport or driving licence is used to confirm identity which bears a date of birth that is clearly inconsistent with the age of the person presenting the document.

3.13 Information about a person's residency and/or nationality is also useful in assessing whether a customer is resident in a high-risk country.

(b) Documentation for evidence of identity

3.14 Information and documentation should be obtained and retained to support, or give evidence to, the details provided by the *Applicant for Business*.

3.15 Identification documents, either originals or certified copies, should be pre-signed and bear a photograph of the applicant, e.g.:-

(i) Current valid passport;
(ii) Armed Forces ID card;
(iii) A Cayman Islands employer ID card bearing the photograph and signature of the applicant; or
(iv) Provisional or full drivers licence bearing the photograph and signature of the applicant

3.16 Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as **sole** evidence of identity, e.g. birth certificate, credit cards, non-Cayman Islands provisional driving licence, student union cards. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which a *Financial Services Provider* is unfamiliar, either because of origin, format or language, the *Financial Services Provider* must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarised translation. *Financial Services Providers* should also be aware of the authenticity of passports.

(c) Persons without standard identification documentation

3.17 Irrespective of the type of business, it is recognised that certain classes of customers, such as the elderly, the disabled, students and minors, may not be able to produce the usual types of evidence of identity, such as a driving licence or passport. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous anti-money laundering procedures is recommended. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph.

3.18 If information cannot be obtained from the sources referred to below to enable verification to be completed and the account to be opened, a request may be made to another institution or institutions for confirmation of identity (as opposed to a banker's reference). Failure of that institution to respond positively and within a reasonable time should put the requesting institution on its guard.

(d) Verification of name and address

3.19 *Financial Services Providers* should also take appropriate steps to verify the name and address of applicants by one or more methods, e.g.: -

(i) obtaining a reference from a "respected professional" who knows the applicant;
(ii) checking the register of electors;
(iii) making a credit reference agency search;
(iv) checking a local telephone directory;

(v) requesting sight of a recent rates or utility bill. Care must be taken that the document is an original and not a copy, or

(vi) personal visit to the home of the applicant where possible.

3.20 The term 'respected professional' could be applied to for instance, lawyers, accountants, directors or managers of a regulated institution, priests, ministers or teachers.

3.21 Where an applicant's address is temporary accommodation, for example an expatriate on a short term overseas contract, *Financial Services Providers* should adopt flexible procedures to obtain verification under other categories, such as copy of contract of employment, or banker's or employer's written confirmation.

3.22 In circumstances where an accountholder appoints another person as an account signatory e.g. appointing a member of his family, full identification procedures should also be carried out on the new account signatory.

3.23 The form in Appendix E may be used for verification of identity, to supplement the identification documentation already held, and is an alternative to the procedures in 3.19.

3.24 For the avoidance of doubt, the form in Appendix E is not intended to be used as the sole means of obtaining evidence of identity of an applicant, but is designed to be a standardised means by which verification can be obtained concerning identification evidence already obtained.

(e) Certification of identification documents

(i) Suitable certifiers

3.25 A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated credit or financial institution, a notary public, a member of the judiciary or a senior civil servant. Such persons are expected to adhere to ethical and or professional standards and exercise his or her profession or vocation in a jurisdiction that has an effective anti-money laundering regime. The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address and phone number.

3.26 The list above of suitable certifiers is not intended to be exhaustive, and *Financial Services Providers* should exercise due caution when considering certified copy documents, especially where such documents are easily forged or can be easily obtained using false identities or originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. Where certified copy documents are accepted, it is the *Financial Services Provider's* responsibility to satisfy itself that the certifier is appropriate. *Financial Services Providers* may for instance, include in its

policies and procedures a list of suitable certifiers approved by senior management. In all cases, *Financial Services Providers* should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate, or other document.

(ii) Face-to-face

3.27 Where possible, face-to-face customers must show *Financial Services Providers'* staff original documents, and copies taken immediately and retained and certified by a senior staff member**.**

(iii) Non face-to-face

.

3.28 Any interaction between *Financial Services Provider* and a customer in a non-direct manner increases the exposure to risk. Not only does this allow for third parties to have access to assets or property through impersonation but may also disguise the true owner of that property by, for example, provision of false identification documentation. *Financial Services Providers* should put into place policies and procedures that appropriately address the risks posed by non-face to face contact for customers either at the opening of the business relationship or through the operation of that relationship. Financial business conducted on a non face-to-face basis includes internet and telephone banking and online share dealing and these are addressed further in paragraphs 3.55-3.58.

3.29 Where identity is verified electronically or copy documents are used, a Financial Service Provider should apply additional verification checks. For example, where it is impractical or impossible to obtain sight of original documents, a copy should only be accepted where it has been certified by a suitable certifier as being a true copy of the original document and that the photo is a true likeness of the *Applicant for Business*.

(iv) Intra-group

3.30 In intra-group business, *Financial Services Providers* should ensure that the certification of documents is in accordance with group policies.

CORPORATE CLIENTS

3.31 It will normally be necessary to obtain the following documented information concerning corporate clients:-

(i) Certificate of Incorporation or equivalent, details of the registered office, and place of business;

(ii) Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;

(iii) Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 10% interest or more or with principal control over the company's assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;

(iv) In the case of a bank account, satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;

(v) Evidence of the authority to enter into the business relationship (for example, a copy of the Board Resolution authorising the account signatories in the case of a bank account);

(vi) Copies of Powers of Attorney, or any other authority, affecting the operation of the account given by the directors in relation to the company;

(vii) Copies of the list/register of directors;

(viii) Satisfactory evidence of identity must be established for two directors, one of whom should if applicable, be an executive director where different from account signatories.

3.32 Consideration should also be given to whether it is desirable to obtain a copy of the memorandum and articles of association, or by-laws of the client.

3.33 Where the *Financial Services Provider* feels that there may be additional settlement, credit, or money laundering risk, it may obtain further evidence in order to reassure itself, which might include a full list of shareholders.

3.34 It is sometimes a feature of corporate entities being used to launder money that account signatories are not directors, managers or employees of the corporate entity. In such circumstances, *Financial Services Providers* should exercise caution, making sure to verify the identity of the signatories, and where appropriate, monitoring the ongoing business relationship more closely.

3.35 For the purposes of these Guidance Notes, a 'beneficial owner' is a person on whose behalf an account is opened, a business relationship is established or a transaction is

conducted. In some cases the identity of beneficial ownership may not always be the most relevant factor in establishing the control of a corporate client. In such circumstances focus should be placed upon principal control of the operation of the corporate entity. *Financial Services Providers* should therefore exercise prudent judgement in the spirit of these Guidance Notes in the identification verification process in such cases and the Monetary Authority will seek explanations for the approach adopted during the course of onsite inspections.

3.36 Where it is impractical or impossible to obtain sight of the original Certificate of Incorporation or equivalent, *Financial Services Providers* may accept a suitably certified copy in accordance with the procedures stated in paragraphs 3.25 to 3.28 of the Guidance Notes.

3.37 It is recognised that on some occasions companies may be used as a disguise for their beneficial owner. These are sometimes referred to as 'shell companies'. There is concern about the use of such companies to conduct money laundering. Financial Services Providers should therefore be alert to their potential for abuse. In keeping with these Guidance Notes, institutions should obtain satisfactory evidence of the identity of beneficial owners, directors and authorized signatories of shell companies. Where the shell company is introduced to the *Financial Services Provider* by a professional intermediary acting on its behalf, *Financial Services Providers* should follow the procedures for introduced business outlined in these Guidance Notes.

PARTNERSHIPS/UNINCORPORATED BUSINESSES

3.38 In the case of Cayman Islands limited partnerships and other unincorporated businesses or partnerships in which, for example, the general partner does not fall within the exempted category set out in this section, *Financial Services Providers* should obtain, where relevant:

- Identification evidence for at least two partners/controllers and/or authorised signatories, in line with the requirements for direct personal clients. When authorised signatories change, care should be taken to ensure that the identity of the current signatories has been verified.

- Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable).

- An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose. In cases where a formal partnership arrangement exists, a mandate from the partnership authorising the opening of an account or undertaking the transaction and conferring authority on those who will undertake transactions should be obtained.

TRUST AND FIDUCIARY CLIENTS

3.39 Trusts and other fiduciary relationships can be useful to criminals wishing to disguise the origin of funds, if the trustee or fiduciary does not carry out adequate procedures. So particular care is needed on the part of the Financial Services Provider when the Applicant for Business is a trustee or fiduciary who is not an Exempted Client (see paragraph 3.78) or an *Eligible Introducer* (see paragraph 3.61). In such cases the Financial Services Provider should normally, in addition to obtaining identification evidence for the trustee(s) and any other person who has signatory powers on the account:

- make appropriate enquiry as to the general nature of the trust (e.g. family trust, pension trust, charitable trust etc) and the source of funds;

- obtain identification evidence for the settlor(s), i.e. the person(s) whose property was settled on the trust; and

- in the case of a nominee relationship, obtain identification evidence for the beneficial owner(s) if different to the settlor(s).

3.40 In some cases it may be impractical to obtain all of the above (e.g. if the settlor has died). Discretion must be exercised but in a manner consistent with the spirit of these Guidance Notes.

3.41 Financial Services Providers providing trustee services should refer to section 8 of these Guidance Notes for guidance.

ASSOCIATIONS NOT FOR PROFIT (INCLUDING CHARITIES)

3.42 Associations not for profit may pose a potential risk of money laundering for FSPs. At the placement stage there may be difficulties in identifying the source of funds, the identity of the donor, and verifying the information where it is provided. In some circumstances, such as in the case of anonymous donations, the identity of the donor is not known and as a result neither is the source of the funds.

3.43 There is clearly a distinction from the point of view of risk as to whether the association not for profit is local, i.e. makes distributions primarily within the Islands, or foreign, i.e. makes distributions primarily overseas. Local associations not for profit are low risk in terms of being used to launder money as the amounts involved are usually very small, for specific purposes, and usually do not have fund transfers outside the Cayman Islands. On the other hand, since in most cases there will be no tax advantage to a foreign association not for profit establishing accounts in Cayman, the risks may be higher. There are however many legitimate reasons for associations not for profit using the services of *Financial Service Providers* in the Cayman Islands.

3.44 Where the entity is a corporate entity the account opening procedures should be in accordance with the procedures for corporate clients set out in 3.29 and in the case of Trusts the procedures in 3.37 should be followed.

3.45 Where an applicant for business is an association not for profit, it will normally be necessary to obtain the following documented information:

- An explanation of the nature of the proposed entity's purposes and operations; and
- The identity of at least two signatories and / or anyone who gives instructions on behalf of the entity should be obtained and verified.

3.46 Where an association not for profit is registered as such in an overseas jurisdiction, it may be useful for the *Financial Service Provider* to contact the appropriate charity commission or equivalent body, to confirm the registered number of the charity and to obtain the name and address of the commission's correspondent for the charity concerned. For example, www.guidestar.org provides a list of all IRS recognized non-profit organizations including charities; and www.charity-commission.gov.uk provides a list of registered charities. For various reasons, these bodies will not hold exhaustive lists of all legitimate associations not-for-profit in those jurisdictions.

3.47 Whilst it is not practical to obtain documentary evidence of identity of all donors, *Financial Service Providers* should undertake a basic "vetting" of **foreign** associations not for profit and Associations not for Profit established overseas, in relation to known money laundering and terrorist activities. This includes a reasonable search of public information; verifying that the not for profit association does not appear on any terrorist lists nor has any association with money laundering and that identification information on representatives / signatories is obtained. *Financial Service Providers* are advised to consult the websites listed in 3.11. Particular care should be taken where the purposes to which the associations' funds are applied are located in a high-risk country (see section 3.48 below).

POLITICALLY EXPOSED PERSONS (PEPS)

3.48 Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose *Financial Service Providers* to significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud. Such persons commonly referred to as 'politically exposed persons' (PEPs) or 'potentates' include heads of state, ministers, influential public officials, judges and military commanders.

3.49 Provision of financial services to corrupt PEPs exposes *Financial Service Providers* to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. In addition, public confidence in the ethical standards of a whole financial system can be undermined.

3.50 Financial *Service Providers* are encouraged to be vigilant in relation to PEPs from all jurisdictions, in particular High Risk Countries (see paragraphs [3.48] to [3.50, who are seeking to establish business relationships. *Financial Service Providers* should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.

b) Obtain senior management approval for establishing business relationships with such customers.

c) Take reasonable measures to establish the source of wealth and source of funds.

d) Conduct enhanced ongoing monitoring of the business relationship.

3.51 Financial Services Providers should obtain senior management approval to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes a PEP.

HIGH-RISK COUNTRIES

3.52 Certain countries are associated with predicate crimes such as drug trafficking, fraud and corruption and consequently pose a higher potential risk to *Financial Service Providers*. Conducting a business relationship with such a country exposes the *Financial Service Provider* to reputational risk and legal risk.

3.53 Financial *Service Providers* are advised to consult publicly available information to ensure that they are aware of those countries/territories described in 3.48. A source of relevant information for *Financial Service Providers* is the FATF website at www.oecd.org/fatf Other useful websites include: the Financial Crimes Enforcement Network (FinCEN) at www.ustreas.gov/fincen/ for country advisories; the Office of Foreign Assets Control (OFAC) www.treas.gov/ofac for information pertaining to US foreign policy and national security; and Transparency International, www.transparency.org for information on countries vulnerable to corruption.

3.54 *Financial Service Providers* should exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries. Caution should also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability.

OTHERS:

(a) Emerging technologies, internet banking and investment business accounts

3.55 *Financial Service Providers* should have policies and procedures in place or such measures as may be needed to prevent the misuse of technological development in money laundering or terrorist financing schemes, particularly those technologies that favour anonymity. Banking and investment business on the Internet, for example, add a new dimension to *Financial Services Providers*' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for money laundering, and fraud.

3.56 It is recognized that on-line transactions and services are convenient. However, it is not appropriate that *Financial Services Providers* should offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures.

3.57 However, initial application forms could be completed on-line and then followed up with appropriate identification checks. The account, in common with accounts opened through more traditional methods, should not be put into full operation until the relevant account opening provisions have been satisfied in accordance with these Guidance Notes.

3.58 The development of technologies such as encryption, digital signatures, etc., and the development of new financial services and products, makes the Internet a dynamic environment offering significant business opportunities. The fast pace of technological and product development has significant regulatory and legal implications, and *Financial Services Providers* must ensure that appropriate staff keep abreast of relevant technological developments and identified methodologies in money laundering and terrorist financing schemes. This may involve reviewing papers from international bodies such as the FATF on AML/CFT typologies; warnings and information issued by regulators and law enforcement as well as information issued by industry bodies or trade associations. The appropriate system must embrace keeping up to date with such developments and the potential new risks and impact they may have on the products and services offered by licenceholders. Risks identified must be fed into the business risk assessment.

.

(b) Provision of safe custody and safety deposit boxes

3.59 Where facilities to hold boxes, parcels and sealed envelopes in safe custody are made available, it is expected that *Financial Services Providers* will follow the identification

procedures set out in these Guidance Notes. In addition such facilities should only be made available to account holders.

(c) Managed *Financial Services Providers*

3.60 For the avoidance of doubt, those *Financial Services Providers* which are managed by other *Financial Services Providers* retain the ultimate responsibility for ensuring that the money laundering regulations are complied with.

It is recognised, however, that a managed Financial Service Provider may have to delegate money laundering compliance functions in accordance with the principles set out in these Guidance Notes. There is no objection to such delegation provided that:

i) Details thereof and written evidence of the suitability of any such person or institution to perform the relevant functions on behalf of the Financial Service Provider are made available to the Monetary Authority on request,
ii) There is a clear understanding between the Financial Services Provider and the delegate as to the functions to be performed,
iii) The relevant customer information is readily available to the Monetary Authority on request and to the FRU and law enforcement authorities in accordance with the relevant procedures, and
iv) The Financial Services Provider satisfies itself on a regular basis as to the reliability of the delegate's systems and procedures.

3.61 Where the delegate is located in a Schedule 3 country and is subject to the anti-money laundering regime of that Schedule 3 country, the Monetary Authority will regard compliance with the regulations of such jurisdictions as compliance with the Regulations and Guidance Notes.

TIMING AND DURATION OF VERIFICATION

3.62 The best time to undertake verification is *prior to entry* into the business relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed.

3.63 However, if it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority. This authority should not be delegated, and should only be done in exceptional circumstances. Any such decision should be recorded in writing.

3.64 Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may (or may not) consider that this is in itself suspicious.

3.65 In cases of **telephone or electronic business** where payment is or is expected to be made from a bank or other account, the person verifying identity should:

- satisfy himself/herself that such account is held in the name of the *Applicant for Business* at or before the time of payment, and

- not remit the proceeds of any transaction to the *Applicant for Business* or his/her order until verification of identity has been completed.

PROCEDURES FOR INTRODUCED BUSINESS

3.66 *Financial Services Providers* are required under the Money Laundering Regulations to maintain identification procedures that result in the production of satisfactory evidence of identity of Applicants for Business. According to the MLRs evidence of identity is satisfactory if it is reasonably capable of establishing that the applicant is the person he claims to be and the person who obtains the evidence is satisfied, in accordance with the procedures maintained under these regulations in relation to the relevant financial business concerned, that it does establish that fact.

3.67 There are however, circumstances in which obtaining and verifying such evidence may be unnecessary duplication, commercially onerous and of no real assistance in the identification of or subsequent investigation into money laundering. It may then be appropriate to place reliance on the due diligence procedures of third party "Eligible Introducers" who have conducted client verification procedures substantially in accordance with the Guidance Notes.

3.68 The *Financial Services Provider* is ultimately responsible for ensuring that adequate due diligence procedures are followed and that the documentary evidence of the *Eligible Introducer*, that is being relied upon, is satisfactory for these purposes. Satisfactory evidence is such evidence as will satisfy the anti-money laundering regime in the Schedule 3 country from which the introduction is made. Only senior management should take the decision that reliance may be placed on the *Eligible Introducer* and the basis for deciding that normal due diligence procedures need not be followed should be part of the financial services provider's risk-based assessment and should be recorded and the record retained in accordance with the Regulations. (See Appendix G, Introduced Business flow chart).

3.69 An *Eligible Introducer* is defined as one who meets the criteria detailed below in paragraphs 3.70 to 3.72 and is regulated and supervised for, and has measures in place to comply with CDD requirements in line with FATF Recommendations 5 and 10,

3.70 The applicable Regulation that would permit reliance on an EI is Regulation 10 (1) (c) and the Regulation specifies that the person should be a person:

a. who is bound by regulation 5(1); or
b. that acts in the course of a business in relation to which an overseas regulatory authority exercises regulatory functions and is based or incorporated in, or formed under the law of, a country specified in the Third Schedule,

3.71 An "overseas regulatory authority" means an authority which, in a country outside the Islands, exercises a function corresponding to a statutory function of the Authority in relation to relevant financial business in the Islands.

3.72 In this context the following categories or persons may be able to act as an EI.:

a) An entity in the Cayman Islands to which the Regulations apply (see paragraph 2.16 above and Regulation 4(1)),
b) A member of a local association or professional body to whom the regulations apply, which is subject to disciplinary procedures for failure to conduct relevant financial business in accordance with these Guidance Notes, or
c) A *Financial Institution* in a country with equivalent legislation specified in the Third Schedule that is subject to regulation by an overseas regulatory authority.
d) a lawyer or accountant, or firm of lawyers or accountants, which is regulated in a country with equivalent legislation (See Schedule 3 of the Regulations, Appendix C), or
e) a member of a professional body in a Schedule 3 country that is subject to disciplinary procedures for failure to conduct relevant financial business in accordance with equivalent rules and guidelines to these Guidance Notes, or
f) a lawyer or certified or chartered accountant or firm of lawyers or chartered or certified accountants, carrying on business in a country with equivalent legislation.

3.73 *Financial Services Providers* who depend on Eligible Introducers must take steps to satisfy themselves that:

a) each person that they have so identified meets the criteria of an Eligible Introducer set out in paragraph 3.70-3.72 and that the CDD procedures of the EI are satisfactory
b) the information provided clearly establishes that the identity of the customer or beneficial owner has been verified
c) the level of customer due diligence carried out is made known

d) the Eligible Introducer will make available, on request, copies of any identification and verification data and relevant documents on the identity of the customers (and any beneficial owners) obtained when applying customer due diligence measures

3.74 *To* satisfy itself that an introducer can be relied on *Financial Service Providers* should obtain satisfactory evidence to identify the status and eligibility of introducers. The FSP should maintain a written record of the basis on which it determines to rely on the Eligible Introducer. In the case of an overseas financial institution for instance, such evidence may comprise corroboration from the introducer's regulatory authority, or evidence from the introducer itself of such regulation. When considering whether it is reasonable to rely on a professional intermediary, senior management must consider the following:

a. whether the intermediary is a member of and in good standing within the professional body to which it belongs
b. whether there is a pre-existing client relationship between the Cayman FSP and the introducer and/or between the introducer and the client and the length of that relationship;
c. whether the nature of the business of the intermediary and client are appropriate to the business being introduced; and
d. whether the intermediary is itself established and reputable

3.75 *Financial Service Providers* should also test procedures on a random and periodic basis to ensure that CDD documentation and information is produced by the EI upon demand and without undue delay.

3.76 It *would* also be prudent for *Financial Service Providers* placing reliance on an EI to agree with that EI that the CDD information and verification documentation will be maintained for the period specified under the EI's regulations. It should also be established that the EI will notify the *Financial Service Providers* if he is no longer able to comply with any aspect of the agreement (e.g. if the EI ceases to trade or there is a change in the law) and provide the FSP with the records or copies of records.

3.77 *Financial Services Providers* and other persons that meet the criteria of eligible introducers who are themselves subject to the Regulations have no obligation to act as eligible introducers. Should they choose to do so however, they must be satisfied that the information provided has in fact been obtained appropriately and verified and will be made available to the person relying on it as soon as reasonably practicable. A Cayman Islands licensed bank branch for example should not provide confirmation to another party on any non compliant account or in circumstances where it would be in breach of the law to provide customer information.

3.78 If *Financial Services Providers* are aware of any cases where introducers have incorrectly been treated as eligible, they must take steps to obtain suitable CDD information and verification documents in accordance with the Regulations. Similarly, where applicants for business are introduced by non-Eligible Introducers, FSPs must verify the identity of the applicant for business.

3.79 The information provided by the EI should be in written form. The *Eligible Introducer's* Form in Appendix F or its functional equivalent should be completed in these circumstances.

3.80 If an Introducer fails or is unable to provide a written confirmation or undertaking of the sort required above, the relationship must be reassessed and a judgment made as to what other steps to verify identity are appropriate or, where there is a pattern of non compliance, whether or not the relationship should be discontinued.

3.81 The decision of senior management that reliance may be placed on the Eligible Introducer is not static and should be assessed regularly to determine whether there is a reason that the relationship should be discontinued.

3.82 The FSP should not enter into a relationship with or rely on an Eligible Introducer if the FSP:

(a) knows or suspects that the Eligible Introducer, the applicant for business or any third party on whose behalf the applicant for business is acting is engaged in money laundering or terrorist financing;

(b) has any reason to doubt the identity of the applicant for business, the Eligible Introducer or beneficial owner;

(c) is not satisfied that CDD information or documentation will be made available upon request and without delay

3.83 Where a relationship presents higher money laundering or terrorist financing risk, FSPs must consider whether it is appropriate to rely solely upon the Eligible Introducer or the terms of business provided by the Eligible Introducer containing the necessary information.

(a) Corporate Groups

3.84 When the prospective client is introduced by one part of a group to another and a new business relationship is being established, it is not necessary for identity to be re-verified or for records to be duplicated provided that:

a.) the identity of the client has been verified by the introducing parent company, branch, subsidiary or affiliate in a manner compatible with the Regulations and provided that written confirmation is obtained that the identification records will on request be provided.

b.) *Institutions that are relying on intra-group introductions must be certain that any group policy is absolutely adhered to and is of at least as high a standard as that set by these Guidance Notes.*

(b) Entities Governed by the Regulations and Overseas Financial Institutions

3.85 The Introducer should complete the Eligible Introducers Form or its functional equivalent (see Appendix F) where the client is introduced by:

a) An entity in the Cayman Islands to which the Regulations apply,
b) A member of a local association or professional body to whom the regulations apply, which is subject to disciplinary procedures for failure to conduct relevant financial business in accordance with these Guidance Notes, or
c) A *Financial Institution* in a country with equivalent legislation.

(c) Professional Intermediaries in Countries with Equivalent Legislation

3.86 It may be possible to rely on another's due diligence procedures when the *Introducer* is:

a) a lawyer or accountant, or firm of lawyers or accountants, which is regulated in a country with equivalent legislation (See Schedule 3 of the Regulations, Appendix C), or
b) a member of a professional body both of which are in a Schedule 3 country and which is subject to disciplinary procedures for failure to conduct relevant financial business in accordance with equivalent rules and guidelines to these Guidance Notes, or
c) a lawyer or certified or chartered accountant or firm of lawyers or chartered or certified accountants, carrying on business in a country with equivalent legislation.

In all of the above cases:

(i) The Introducer should complete the Eligible Introducers Form or its functional equivalent (See Appendix F) , and;

(ii) senior management is satisfied that it is reasonable to rely on the Eligible Introducer Form.

When considering whether it is reasonable to rely on the Eligible Introducer Form, senior management must consider the following:

a) whether the intermediary is a member of and in good standing within the professional body to which it belongs;
b) whether there is a pre-existing client relationship between the Cayman FSP and the introducer and/or between the introducer and the client and the length of that relationship;
c) whether the nature of the business of the intermediary and client are appropriate to the business being introduced; and
d) whether the intermediary is itself established and reputable.

The Cayman FSP should maintain a written record of the basis on which it determines to rely on the Eligible Introducer Form.

3.87 In the above cases the *Introducer* should complete the Eligible Introducer's Form in Appendix F or its functional equivalent.

(d) General

3.88 If an Introducer fails or is unable to provide a written confirmation or undertaking of the sort required above, the relationship must be reassessed and a judgment made as to what other steps to verify identity are appropriate or whether or not the relationship should be discontinued.

3.89 Following introduction by an *Eligible Introducer*, it will not usually be necessary to re-verify identity or duplicate records in respect of each transaction or piece of business.

(e) Payment on an Account in a Bank in the Cayman Islands or Country with Equivalent Legislation

3.90 As provided for in Regulation 8 of the Money Laundering Regulations, when a financial transaction involves payment by the client and he does so by remitting funds from an account held in his name at a bank in the Cayman Islands or a bank regulated in a Schedule 3 country, it may be unnecessary to take any further steps to verify client identity. The *Financial Services Provider* should however, have evidence identifying the branch or office of the Bank and verifying that the account is in the name of the client.

3.91 It may be reasonable for example, to take no further steps to verify identity when payment is made by cheque or electronically and sent either by mail or electronically from an account (or joint account) in the client's name at a bank in a Schedule 3 country if it does not fall within the following categories:

a) the circumstances of the payment are such that a person handling the transaction knows or suspects that the applicant for business is engaged in money laundering,

or that the transaction is carried out on behalf of another person engaged in money laundering; or

b) the payment is made for the purpose of opening a relevant account with a bank in the Cayman Islands; or

c) onward payment is to be made in such way that it is not or does not result in-

i) a reinvestment on behalf of the applicant with the same institution engaged in relevant financial business, or

ii) a payment directly to the applicant.

3.92 If the payment does fall into one of the above categories then the evidence of identity of the applicant must be obtained in accordance with the full identification procedures as outlined in this chapter of the guidance notes unless the payment is being made by operation of law (i.e. the payment of the proceeds requires to be made to a trustee in bankruptcy, a liquidator, a trustee for an insane person or a trustee of the estate of a deceased person).

3.93 When payment does not fall in one of the categories set out above, and is made with no additional verification undertaken, a record should usually be retained indicating how the transaction arose in addition to a record of the relevant branch or office and the account name. In addition, the *Financial Services Provider* should take steps to ensure that, in relation to any reinvestment or repayment, there is no apparent variation between the name on the initial payment instrument and the form or request related to any reinvestment or repayment.

EXCEPTIONS TO VERIFICATION REQUIREMENTS

3.94 Unless a transaction is a suspicious one, documentary evidence of identity is not normally required in the following circumstances. In the event of any knowledge or suspicion that money laundering has or is occurring, the exemptions and concessions set out below do not apply and the case should be treated the same as one requiring verification and reporting.

Exempted Categories

(a) One-off transactions and Exempted one-off transactions

3.95 As defined in the Regulations, a "one-off transaction" means any transaction other than a transaction carried on in the course of an established business relationship formed by a person acting in the course of relevant financial business.

3.96 As defined in the Regulations, an "exempted one-off transaction" means a one-off transaction (whether a single transaction or a series of linked transactions) where the amount of the transaction or the aggregate of a series of linked transactions is less than CI$15,000 or the equivalent in any other case.

3.97 *Financial Services Providers* need to be vigilant at all times that the total of a series of linked transactions does not exceed the exempted limit of CI$15,000.

3.98 As a matter of best practice, a time period of 12 months for the identification of linked *transactions* is normally acceptable. However there is some difficulty in defining an absolute time scale that linked transactions may fall within. Therefore the relevant procedures for linking will ultimately depend on the characteristics of the product rather than relating to any arbitrary time limit. For example, *Financial Services Providers* should be aware of any obvious connections between sender of funds and the recipient.

3.99 Verification of identity will not normally be needed in the case of an exempted one off transaction referred to above. If, however, the circumstances surrounding the exempted one off transaction appear to the *Financial Services Provider* to be unusual or questionable, it is likely to be necessary to make further enquiries. Depending on the result of such enquiries, it may then be necessary to take steps to verify the proposed client's identity. If money laundering is known or suspected, the *Financial Services Provider* should not refrain from making a report in line with Section 7(1) of the Regulations simply because of the size of the transaction.

(b) Postal, telephonic and electronic business

3.100 In the following paragraph the expression "non-paying account" is used to mean an account or investment product which does not provide:

- cheque or other money transmission facilities, or
- the facility for transfer of funds to other types of account which do provide such facilities, or
- the facility for repayment or transfer to a person other than the *Applicant for Business* whether on closure or maturity of the account, or on realization or maturity of the investment, or otherwise.

3.101 Given the above definition, where an *Applicant for Business* pays or intends to pay monies to an institution by post, or electronically, or by telephoned instruction, in respect of a non-paying account and:

- it is reasonable in all the circumstances for payment to be made by such means; and

- such payment is made from an account held in the sole ot joint name of the *Applicant for Business* at another regulated financial institution or foreign regulated institution in a Schedule 3 country, and

- the name(s) of the *Applicant for Business* corresponds with the name(s) of the paying account-holder; and

- the receiving institution keeps a record of the applicant's account details with that other institution; and

- there is no suspicion of money laundering,

3.102 The receiving institution is entitled to rely on verification of the *Applicant for Business* by that other institution to the extent that it is reasonable to assume that verification has been carried out and completed. If however, the *Financial Services Provider* has grounds to believe that the identity of the customer has not been previously verified by the regulated financial institution it should, utilizing a risk based approach, take additional measures to verify identity.

(c) Exempted Clients (where documentary evidence of identity is not normally required)

3.103 Documentary evidence of identity will not normally be required if the client:

(a) is a central or local government, statutory body or agency of government;

(b) is regulated by the *Monetary Authority* or is a broker member of the Cayman Islands Stock Exchange as defined in the Cayman Islands Stock Exchange Membership Rules;

(c) is a *Financial Institution* or *Authorised Person* in a country with equivalent legislation as listed in Schedule 3 of the Regulations (Appendix C);

(d) is a company quoted or fund listed on the Cayman Islands Stock Exchange or other market or exchange approved by the *Monetary Authority*. These are listed in Appendix H. This list is subject to review and may be updated periodically;

(e) is a subsidiary of a company or a *Financial Services Provider* referred to in sub-paragraphs (a), (b), (c) and (d) above or has common ownership. In such cases it may be appropriate to obtain written confirmation of the relationship from the holding or parent company or the partnership;

(f) is a pension fund for a professional association, trade union or is for employees of an entity referred to in subparagraphs (a), (b), (c) and (d) above. Satisfactory evidence that the fund falls within this category may be provided by a copy of a certificate of registration, approval or regulation by a government, regulatory or fiscal authority in the jurisdiction in which the fund is established. In the absence of such certificate, *Financial Services Providers* are recommended to obtain the names and addresses of the trustees of the fund (if a trust) or otherwise those empowered to take decisions in respect of it;

3.104 If reliance is to be placed on the fact that a client is an exempted client the *Financial* Services *Provider* should satisfy himself appropriately that he does in fact fall within this category. The *Financial Services Provider* should record the basis upon which he is so satisfied.

3.105 Changes to the list of countries in Schedule 3 of the Regulations will not create new obligations to verify the identity of clients acquired since the coming into effect of the Regulations i.e. September 2000.

TREATMENT OF BUSINESS RELATIONSHIPS EXISTING PRIOR TO ENACTMENT OF THE REGULATIONS

3.106 Section 17 of the Money Laundering Regulations required that verification of the identity of persons with whom a business relationship was formed before 1st September 2000 be completed by 30th September 2003.

3.107 It is clear that certain business relationships established prior to the enactment of the Regulations (1st September, 2000) can still present a major threat of money laundering, and indeed, it is a widely recognised tactic for money launderers to establish seemingly legitimate and normally-run accounts which are then used for laundering money at a later date.

3.108 Prior to 30th September 2003 *Financial Services Providers* are encouraged to adopt the following procedures to ensure that the necessary information is obtained on all existing customers:

a) Establish what constitutes satisfactory evidence of identity for its existing clients to be in compliance with these Guidance Notes.
b) Conduct a risk assessment of the clients, and make a distinction between

high and low risk cases.

c) Give immediate priority to obtaining the information required by these Guidance Notes for the identified high-risk cases.
d) Conduct the necessary due diligence on the remaining low risk cases over a longer term.

3.109 In addition *Financial Services Providers* should develop and implement the following policies and procedures where information on existing customers is not obtained:

a) Make a record of their non-compliant business relationships and note in each case what information or documentation is missing and the reason or supposed reason for its absence. The record will be available to The Monetary Authority for the purposes of its carrying out its responsibility for monitoring compliance with the Money Laundering Regulations.
b) Establish procedures to deal with the business relationship in those situations where satisfactory evidence is not obtained by September 30th 2003 and continue to make reasonable efforts to secure compliance.
c) Where the *Financial Services Provider* is unable to satisfy the verification required by Regulation 17 it should consider appropriate measures to ensure compliance, by for example, refusing to accept further funds from that person or provide further services to that person or by freezing funds held on his behalf or by terminating the business relationship altogether. Any such action should be carried out if and to the extent that it can properly be done by the *Financial Services Provider,* without prejudicing third parties (including clients who have verified their identity) and without exposing the *Financial Service Provider* to liability, loss or prejudice.

3.110 The Monetary Authority will be examining the extent to which institutions are following the above procedures during the course of onsite inspections and may take appropriate action as authorized by the regulatory laws where warranted. In determining what action to take, the Monetary Authority will take into account the overall circumstances including the seriousness of the non-compliance, the number of instances of non-compliance and the failure to respond to any previous recommendations or warnings given by the Monetary Authority.

3.111 *Financial Services Providers* are reminded of the suspicion reporting duties imposed by the Proceeds of Crime Law and that non-cooperation with the verification required by regulation 17 is a circumstance that should put the financial services provider on enquiry, to ask itself the question whether the reason for non-cooperation may be that the business relationship is being used for money laundering purposes.

3.112 In those cases where persons do not have standard identification documents some flexibility is suggested in paragraph 3.17 above. For existing clients an introduction from

a respected customer personally known to a Director, Manager or senior member of staff, will often provide comfort provided that the conditions of para 3.17 are satisfied and that the introduction can never replace the address verification procedures described in these Guidance Notes. Details of who initiated the account and authorized the introduction must be kept. Directors/Senior Managers should take a common sense approach in determining whether certain documents should be waived in any particular situation but it must ensure that normal identification procedures are not waived as a favour to the applicant. Where specific documentation of a client is waived, management must make a record of why the waiver was granted.

3.113 When an existing customer closes one account and opens another, or enters into a new agreement to purchase products or services, there is no need to verify identity or address. However, the opportunity should be taken to confirm the relevant customer information. This is particularly important if there has been no recent contact or correspondence with the customer e.g. within the last 12 months or when a previously dormant account has been reactivated.

NO SIMPLIFIED DUE DILIGENCE FOR HIGHER-RISK SCENARIOS

3.114 Simplified customer due diligence should be unacceptable for specific higher-risk scenarios. Higher-risk scenarios may include, but are not limited to the following:

- a customer is not physically present for identification purposes; or
- the relevant person proposes to have a business relationship or carry out a a one-off transaction with a PEP; or
- the prospective customer holds a deposit-taking licence and proposes to establish a correspondent banking relationship with the *Financial Services Provider*; or
- the nature of the situation is such, or a risk assessment reveals, that a higher risk of money laundering is likely.

CORRESPONDENT BANKING

3.115 *Financial Services Providers* should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

c.) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

d.) Assess the respondent institution's anti-money laundering and terrorist financing controls.

e.) Obtain approval from senior management before establishing new correspondent relationships.

f.) Document the respective responsibilities of each institution.

g.) With respect to "payable-through accounts[1]", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

3.116 *Financial Services Providers* should not enter into, or continue, a correspondent relationship with a "shell bank[2];" and should take appropriate measures to ensure that it does not enter into, or continue a corresponding banking relationship with a bank which is known to permit its accounts to be used by a shell bank. Neither should Financial Services Provides set up anonymous accounts or anonymous passbooks for new or existing customers.

3.117 *Financial Services Providers* should satisfy themselves that the respondent financial institutions in foreign countries do not permit their accounts to be used by shell banks.

[1] Payable-through accounts are correspondent accounts that are used directly by third parties to transact business on their own behalf.

2 A" Shell Bank" is a bank that is incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

SECTION 4 - ON-GOING MONITORING OF BUSINESS RELATIONSHIPS

4.1 Once the identification procedures have been completed and the client relationship is established, the *Financial Services Provider is required to* monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened.

4.2 *Financial Services Providers* should develop and apply written policies and procedures for taking reasonable measures to ensure that documents, data or information collected during the "Identification" process are kept up-to-date and relevant by undertaking routine reviews of existing records. This does not mean that there needs to be automatic renewal of expired identification documents (e.g. passports) where there is sufficient information to indicate that the identification of the customer can readily be verified by other means

4.3 The relevancy of the documentation underlying the Financial Services Provider's records will be determined according to circumstances of the client, the nature and risk of the transaction or relationship. Particular attention should be paid to higher risk categories of customers and business relationships. In circumstances where customer documentation standards change substantially or there have been significant changes in the business relationship, *Financial Services Providers* should use these as opportunities to update records. These include, but are not limited to, the following:

- New products or services being entered into,
- A significant increase in a customer's salary being deposited,
- The stated turnover or activity of a corporate client increases,
- A person has just been designated as a PEP,
- The nature, volume or size of transactions increases.

However, if a *Financial Services Provider* becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible

MONITORING

4.4 *Financial Services Providers,* either directly or in accordance with paragraph 3.43, are expected to have systems and controls in place to monitor on an ongoing basis the relevant activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for *Financial Services Providers* to be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be: -

(a) transaction type
(b) frequency
(c) amount

(d) geographical origin/destination
(e) account signatories

4.5 It is recognised that the most effective method of monitoring of accounts is achieved through a combination of computerised and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring method as a matter of course. Computerised approaches may include the setting of “floor levels" for monitoring by amount.

4.6 Whilst some *Financial Services Providers* may wish to invest in expert computer systems specifically designed to assist the detection of fraud and money laundering, it is recognized that this may not be a practical option for many *Financial Services Providers* for the reasons of cost, the nature of their business, or difficulties of systems integration, in such circumstances institutions will need to ensure they have alternative systems in place. Appendix K includes examples of suspicious activities.

4.7 Financial services providers should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when the financial services provider has doubts about the veracity or adequacy of previously obtained customer identification data.

4.8 The customer due diligence measures mentioned in paragraph 4.7 do not imply that financial services providers have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction, or when a document evidencing identification expires. An institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer’s account is operated which is not consistent with the customer’s business profile.

"HOLD MAIL" ACCOUNTS

4.9 "Hold Mail" accounts are accounts where the accountholder has instructed the *Financial Services Provider* not to issue any correspondence to the accountholder's address. Although this is not necessarily a suspicious act in itself, the such accounts do carry additional risk to *Financial Services Providers*, and they should exercise due caution as a result.

4.10 Regardless of the source of "Hold Mail" business, it is recommended on a best practice basis that evidence of identity of the accountholder should be obtained by the *Financial*

Services Provider, even where the client was introduced by a *Eligible Introducer*. "Hold Mail" accounts should be regularly monitored and reviewed.

4.11 It is recommended that *Financial Services Providers* have controls in place for when existing accounts change status to "Hold Mail", and that the necessary steps to obtain the identity of the account holder are taken where such evidence is not already on the *Financial Services Providers* file.

4.12 Accounts with a "c/o" address should not be treated as "Hold Mail" accounts, as mail is being issued, albeit not necessarily to the accountholder's address. There are of course many genuine innocent circumstances where a "c/o" address is used, but Financial *Services Providers* should monitor such accounts more closely as they represent a higher risk.

4.13 *Financial Services Providers* should incorporate procedures to check the current permanent address of hold mail customers wherever the opportunity arises.

WIRE TRANSFERS

(a) General

4.14 To facilitate the identification and reporting of suspicious transactions and bearing in mind that the full traceability of transfers of funds can be a particularly important and valuable tool in the prevention, investigation and detection of money laundering or terrorist financing, the Cayman Islands Government enacted amendments to the MLRs on 1 June 2007 to comply with FATF Special Recommendation (SR) VII. The FATF issued SR VII, with the objective of enhancing the transparency of electronic payment transfers (wire transfers) of all types, domestic and cross border.

4.15 Specifically, its aim is to ensure that basic accurate and meaningful information on the originator of wire transfers is immediately available to (1) the appropriate authorities to assist them in investigating, prosecuting money launderers and terrorists and tracing the assets of money launderers and terrorists, (2) the FRA for analysing suspicious or unusual activity and disseminating information as necessary, and (3) beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions.

4.16 The June 2007 MLR amendments are not intended to impose rigid requirements or mandate a single operating process that would negatively impact the payment system. Guidance provided here is intended to assist financial services providers in outlining their obligations with respect to wire transfers. The character of the Cayman Islands industry dictates that the vast majority of transfers will be cross border in nature.

Scope of the Regulations

4.17 The amendments to the MLRs are intended to apply to any transaction (domestic or cross boarder) carried out on behalf of a payer through a payment service provider by electronic means, with a view to making funds available to the payee at a payment service provider, irrespective of whether the payer and the payee are the same person.

4.18 The amendments to the MLRs also apply where the payment service provider of the payer is situated outside the Cayman Islands and the intermediary payment service provider is situated within the Cayman Islands, for transfers of funds by the intermediary payment service provider within the Cayman Islands.

4.19 Recognising, and in keeping with international standards, that certain transfers of funds represent a low risk of money laundering or terrorist financing, the regulation exempts the following types of funds transfers:

- where the payer withdraws cash from his own account;
- where truncated checks (electronically imaged copies of original checks) are used;
- for fines, duties and levies within the Cayman Islands;
- where there is a debit transfer authorisation (standing order) between two parties permitting payments between them through accounts, if a unique identifier accompanies the transfer of funds, allowing the person to be traced back;
- where both the payer and the payee are payment service providers acting on their own behalf;
- by credit or debit card or similar payment instrument, providing that the payee has an agreement with the payment service provider permitting payment for goods or services and that the transfer is accompanied by a unique identifier permitting the transaction to be traced back to the payer;
- within the Islands for the provision of goods and services to a payee account if (a) the payment service provider of the payee, by means of a unique reference number, is able trace back the transfer of funds to the person who has an agreement with the payee for the provision of goods and services, and (b) in the case of two or more one-off transactions, that these transactions do not appear to be linked and that the total amounts of these transactions are under fifteen thousand dollars;

Information Requirements and Record Keeping

4.20 The MLRs require, except where permitted in Regulation 17 of the MLRs as amended and outlined above in paragraph 4.15, complete payer information to accompany all wire transfers. The complete payer information applies to transfers where the destination payment service provider is outside of the Cayman Islands.

4.21 Section 2 of the MLRs as amended define “complete information” for the purpose of wire transfers. In essence three items of information are required:-

4.22 In the case of natural persons:

1. his name; and
2. his account number or a unique identifier (which allows the transaction to be traced back to the payer) and
3. Either his address or date and place of birth, or customer identification number, or the number of a government issued document, evidencing identity (e.g. passport or drivers licence).

4.23 In the case of legal persons:

1. the name; and
2. the account number or a unique identifier (which allows the transaction to be traced back to the payer) and
3. Either the address or customer identification number, or the number of a government issued document, evidencing identity.

4.24 The payment service provider of the payer should keep complete information on the payer, which accompanies wire transfers for a period of five years. The Payment service provider of the payee and the intermediary service provider should also keep records of any information received on the payer for a period of five years.

(b) Transfer of funds within the Cayman Islands (Domestic Transfers)

4.25 Where both the payment service provider of the payee and the payment service provider of the payer are situated within the Cayman Islands, transfer of funds need only be accompanied by the account information or a unique identifier which will allow the information to be traced back to the payer.

4.26 If the payment service provider of the payee requests complete information on the payer, then such information should be provided by the payment service provider of the payer within three working days of such request.

Batch Transfers

4.27 For batch file transfers from a single payer where the payment service provider of the payee is located outside of the Cayman Islands, there is no need for complete payer information for each transfer bundled together if (a) that batch contains the complete payer information and (b) the individual transfers carry the account number of the payer or a unique identifier.

Incomplete and Missing Information on Incoming Wire Transfers

4.28 The payment service provider of the payee should have effective risk based procedures in place to detect missing or incomplete information from the messaging or payment and settlement system used to effect the transfer of funds. In order not to disrupt straight-through processing, it is not expected that monitoring should be undertaken at the time of processing the transfer.

4.29 The payment service provider of the payee shall consider missing or incomplete information on the payer as a risk factor in assessing whether the transfer funds or any related transaction is suspicious and whether it must be reported to the FRA.

Detection Upon Receipt

4.30 Where the payment service provider of the payee detects, when receiving transfer of funds, the required payer information that is missing or incomplete, then it shall either reject the transfer, or ask for or otherwise obtain, complete information on the payer. This may include the acquisition of the information from a source other than the service provider of the payer.

Post-Event Monitoring

4.31 The payment service provider should subject incoming wire transfers to an appropriate level of post event random sampling that is risk-based. The sampling may be weighted toward transfers from :

- non schedule 3 countries or a countries deemed to be high-risk for money laundering and/or terrorist financing; and
- payment service providers of payers who are identified from such sampling as having previously failed to comply with the relevant information requirements.

4.32 This does not obviate the obligation to report suspicious actions in accordance with normal suspicious transaction reporting procedures.

Where the payment service provider regularly fails to supply the required payer information and the payment service provider of the payee has taken reasonable measures to have the payment service provider of the payer correct the failures, then the payment service provider of the payee should either reject any future transfers of funds from the payment service provider;

- restrict its business relationship with the payment service provider; or
- terminate its business relationship with the payment service provider;

and report to the FRA and the Monetary Authority any such decision to restrict or terminate the relationship

Payments via Intermediaries and Technical Limitations

4.33 Where the payment service provider of the payer is situated outside the Cayman Islands and the intermediary payment service provider is situated within the Cayman Islands, then the intermediary payment service providers should ensure that all information received on the payer that accompanies a transfer of funds is kept with the transfer.

4.34 The intermediary payment service provider may use a payment system with technical limitations that prevent information on the payer from accompanying the transfer, to send transfer of funds to the payment service provider of the payee, provided that it is able to provide the payment service provider of the payee with the complete information using a mutually acceptable means of communication.

4.35 Where the intermediary payment service provider receives a transfer of funds without complete information on the payer, then it may use the a payment system with technical limitations if it is able to provide the payment service provider of the payee with the complete information using a mutually acceptable means of communication.

4.36 Where the intermediary payment service provider uses a payment system with technical limitations, it is obligated to make available within three working days to the payment service provider of the payee upon request, all information on the payer which it has received. This is irrespective of whether the information is complete or not.

(c) Cooperation with the FRA

4.37 Payment service providers are obligated to respond fully and without delay to enquiries made by the FRA concerning information on the payer accompanying transfer of funds and corresponding records.

SECTION 5 – INTERNAL REPORTING PROCEDURES FOR SUSPICIOUS ACTIVITIES

5.1 *Financial Services Providers* must establish a written internal procedures manual so that, in the event of a suspicious activity being discovered, all staff are aware of the reporting chain and the procedures to follow. Such manuals should be periodically updated to reflect any legislative changes.

APPOINTING AN *MLRO* TO WHOM ALL REPORTS OF KNOWLEDGE OR SUSPICION OF MONEY LAUNDERING ARE MADE.

5.2 *Each Financial Services Provider* should designate a suitably qualified and experienced person as Money Laundering Reporting Officer (MLRO) at management level, to whom suspicious activity reports must be made by staff. It is generally expected that the *MLRO* would be carrying out a Compliance, Audit or Legal role within the *Financial Services Providers*' business. It is also recommended that *Financial Services Providers* identify a Deputy, who should be a staff member of similar status and experience to the *MLRO.*

5.3 The *MLRO* should be well versed in the different types of transaction which the institution handles and which may give rise to opportunities for money laundering. Appendix K gives examples of common transaction types which may be relevant. These are not intended to be exhaustive.

5.4 It is recognised that where a *Financial Services Provider* has no employees in the Cayman Islands it may not be possible for a senior member of staff to be the *MLRO*. In these circumstances the *Financial Services Provider* may;

a. Identify someone else as the appropriate person to whom a report is to be made, provided that that person has the following characteristics:
   i. is a natural person; and
   ii. is autonomous (meaning the *MLRO* is the final decision maker as to whether to file an SAR); and
   iii. is independent (meaning no vested interest in the underlying activity); and
   iv. has and shall have access to all relevant material in order to make an assessment as to whether the activity is or is not suspicious.

b. Delegate the *MLRO* function consistent with paragraph 3.55 and in accordance with the principles set out in these Guidance Notes.
c. Where the *Financial Service Provider* is a mutual fund or mutual fund administrator regulated in the Cayman Islands, utilise the further options set out in Sector 8 of the Guidance Notes.

5.5 Where a *Financial Service Provider* has no staff, the provisions of Regulations 5(1)(b) and (c) regarding awareness and training will not apply. However, the *Financial Service Provider* is responsible for ensuring vigilance systems are in place to ensure that any staff involved in the relevant activities of the *Financial Service Provider* are aware of the identity of the *MLRO* and that all internal SARs are submitted to the *MLRO*

5.6 Where the MLRO that is located outside of the Islands files a suspicious activity report with the appropriate authority under the laws and regulations of his home country, it would be appropriate, where permitted by such laws and regulations, for the MLRO to simultaneously report such suspicious activity to the Reporting Authority in the Cayman Islands

IDENTIFYING THE *MLRO* AND REPORTING CHAINS

5.7 All staff engaged in the business of the *Financial Services Providers* at all levels must be made aware of the identity of the *MLRO* and his Deputy, and the procedure to follow when making a suspicious activity report. All relevant staff must be aware of the chain through which suspicious activity reports should be passed to the *MLRO*.

A suggested format of an internal report form is set out in Appendix I.

5.8 *Financial Services Providers* should ensure that staff report all suspicious activities to the MLRO, and that "any such report be considered in the light of all other relevant information by the MLRO, or by another designated person, for the purpose of determining whether or not the information or other matter contained in the report does give rise to a knowledge or suspicion." See section 14(b) of the Regulations.

5.9 Where staff continue to encounter suspicious activities on an account which they have previously reported to the *MLRO*, they should continue to make reports to the *MLRO* whenever a further suspicious transaction occurs, and the *MLRO* should determine whether a disclosure in accordance with the legislation is appropriate.

5.10 All reports of suspicious activities must reach the MLRO and only the MLRO should have the authority to determine whether a disclosure in accordance with the legislation is appropriate. However the line/relationship manager can be permitted to add his comments to the suspicion report indicating any evidence as to why he/she believes the suspicion is not justified.

IDENTIFYING SUSPICIONS

5.11 A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. Therefore, the first key to the recognition is knowing enough about the customer and the customer's

normal expected activities to recognize when a transaction, or series of transactions, is unusual.

5.12 Although these Guidance Notes tend to focus on new business relationships and transactions, institutions should be alert to the implications of the financial flows and transaction patterns of existing customers, particularly where there is a significant, unexpected and unexplained change in the behaviour of an account.

5.13 As the types of transactions which may be used by money launderers are almost unlimited, it is difficult to define a suspicious transaction. However, it is important to properly differentiate between the terms "unusual" and "suspicious".

5.14 Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction must be considered *unusual*, and the staff member put "on enquiry". Complex transactions or structures may have entirely legitimate purposes. However, *Financial Services Providers* should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should as far as possible be examined and documented by the *Financial Service Provider*. Findings regarding enquiries about complex, unusual large transactions, and unusual patterns of transactions should be kept by the *Financial Service Provider,* and be available to help competent authorities and auditors for at least five years.

5.15 Where the staff member conducts enquiries and obtains what he considers to be a satisfactory explanation of the complex or unusual large transaction, or unusual pattern of transaction, he may conclude that there are no grounds for suspicion, and therefore take no further action as he is satisfied with matters. However, where the enquiries conducted by the staff member do not provide a satisfactory explanation of the transaction, he may conclude that there are grounds for *suspicion* requiring disclosure. Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result should be properly documented and made available to the relevant authorities upon request. Enquiries to check whether complex or unusual transactions or structures have legitimate economic or lawful purpose, where conducted properly and in good faith, are not regarded as tipping off.

5.16 Activities which should put staff on enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive.

- any unusual financial activity of the customer in the context of his own usual activities;

- any unusual transaction in the course of some usual financial activity;
- any unusually-linked transactions;
- any unusual employment of an intermediary in the course of some usual transaction or financial activity;
- any unusual method of settlement;
- any unusual or disadvantageous early redemption of an investment product;
- any unwillingness to provide the information requested.

QUESTIONS TO ASK YOURSELF

5.17 The following factors should be borne in mind when seeking to identify a suspicious transaction. This list is not meant to be exhaustive.

(a) Is the customer known personally?
(b) Is the transaction in keeping with the customer's normal activity known to the *Financial Services Provider*, the markets in which the customer is active and the customer's own business? (i.e. does it make sense?)
(c) Is the transaction in keeping with normal practice in the market to which it relates i.e. with reference to market, size and frequency?
(d) Is the role of the agent involved in the transaction unusual?
(e) Is the transaction to be settled in the normal manner?
(f) Are there any other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries? And,
(g) Can you understand the reasons for the transaction i.e. might there be an easier, cheaper or more convenient method available?

CASH TRANSACTIONS

5.18 Given the international nature of the business conducted by many *Financial Services Providers*, cash transactions may be relatively uncommon, whereas for banks, building societies or money services businesses offering services to local customers, cash transactions may be a normal every-day service to many customers.

5.19 Where cash transactions are being proposed by customers, and such requests are not in accordance with the client's known reasonable practice, many *Financial Services*

Providers will need to approach such situations with caution and make further relevant enquiries.

5.20 Depending on the type of business each *Financial Services Provider* conducts and the nature of its client portfolio, each may wish to set its own parameters for the identification and further investigation of cash transactions. Where the staff member of the *Financial Services Provider* has been unable to satisfy himself that any cash transaction is reasonable activity, and therefore he considers it suspicious, he should make a disclosure as appropriate.

5.21 Whilst certain cash transactions may lead the *Financial Services Providers* to make further enquiries to establish or dispel suspicion, it goes without saying that equal vigilance must be applied to transactions which do not involve cash.

ROLE OF STAFF MEMBERS

5.22 Staff should be required to report any suspicion of laundering either directly to their MLRO or, if the institution so decides, to their line manager for preliminary investigation in case there are any known facts which may negate the suspicion subject to paragraph 5.8.

5.23 Employees should comply at all times with the vigilance systems of their institution and will be treated as having met appropriate standards of vigilance if they disclose their suspicions to their *MLRO* or other appropriate senior colleague according to the vigilance systems in operation in their institution.

THE ROLE OF THE *MLRO*

5.24 On receipt of a report concerning a suspicious customer or suspicious activity the *MLRO* should determine whether the information contained in such report supports the suspicion. He should investigate the details in order to determine whether in all the circumstances he in turn should submit a report to the *Reporting Authority*.

5.25 If the *MLRO* decides that the information does substantiate a suspicion of laundering, he must disclose this information promptly. If he decides that the information does not substantiate a suspicion, he would nevertheless be well advised to record fully the reasons for his decision not to report to the *Reporting Authority.*

5.26 It is for each institution (or group) to consider whether its vigilance systems should require the *MLRO* to report suspicions within the institution (or group) to the inspection or compliance department at head office.

5.27 Failure by the *MLRO* to diligently consider all relevant material may lead to vital information being overlooked and the suspicious activity not being disclosed to the *Reporting Authority* in accordance with the requirements of the legislation. Alternatively, it may also lead to vital information being overlooked which may have made it clear that a disclosure would have been unnecessary. As a result, it is recommended that the *MLRO* should establish and maintain a register of money laundering referrals made to him by staff.

5.28 Staff members should note that in the event of suspicion of money laundering, a disclosure should be made even where there has been no transaction by or through the *Financial Services Provider*. Staff members should ensure that they do not commit the offence of tipping off the customer who is the subject of the disclosure.

REPORTING SUSPICIONS TO THE REPORTING AUTHORITY

5.29 If the MLRO decides that a disclosure should be made, a report, in standard form (see Appendix J), should be sent to the Reporting Authority. The Form should be completed in its entirety and any fields that are not applicable should be so indicated. It is important that the MLRO fill in the form to the fullest extent possible providing as much relevant information and detail as they have available. This will provide more assurance that the information provided is of benefit to the FRA.

5.30 The Reason for Suspicion section of the Form is a key part of the report. It is important for the MLRO to explain why there are suspicions about a specific transaction or transactions. Information about the subject and why there is a suspicion in the context of the business relationship should be included. Other useful information that should be provided includes how the transaction and/or business relationship was initiated, relevant dates, the amount of funds involved, the current status of the account if applicable and what action if any the FSP intends to take or may have taken.

5.31 If the *MLRO* considers that a report should be made **urgently** (e.g. where the account is already part of a current investigation), initial notification to the *Reporting Authority* should be made by telephone, email, or other means and must be followed up in writing as soon as is reasonably practicable.

5.32 The receipt of a report will be promptly acknowledged by the *Reporting Authority*. The report is forwarded to trained financial investigation officers who alone have access to it. They may seek further information from the reporting institution and elsewhere. It is important to note that after a reporting institution makes an initial report in respect of a specific suspicious activity, that initial report does not relieve the institution of the need to report further suspicions in respect of the same customer or account and the institution should report any further suspicious activity involving that customer.

5.33 Vigilance systems should require the maintenance of a register of all reports made to the *Reporting Authority* pursuant to this paragraph. Such registers should contain details of:

- the date of the report;
- the person who made the report;
- the person(s) to whom the report was forwarded; and
- a reference by which supporting evidence is identifiable.

5.34 The *Reporting Authority* will keep the reporting institution informed of the interim and final result of investigations following the reporting of a suspicion to it. The *Reporting Authority* will endeavour to issue an interim report to the institution at regular intervals and in any event to issue the first interim report within one month of the report being made. In addition, at the request of the reporting institution, the *Reporting Authority* will promptly confirm the current status of such an investigation. Suspicious activity disclosure should be sent directly to the *Reporting Authority* at the following address:

The Reporting Authority
P.O. Box 1054
George Town, Grand Cayman
Telephone: (1345) 945-6267
Facsimile: (1345) 945-6268

REPORTING DECLINED BUSINESS

5.35 It is normal practice for Financial Services Providers to turn away business that they suspect might be criminal in intent or origin. Where an applicant for business or a customer fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration should be given to filing a SAR. Also, where an attempted transaction gives rise to knowledge or suspicion of money laundering or terrorist financing, that attempted transaction should be reported to the Reporting Authority.

5.36 Reporting of such events will allow the *Reporting Authority* to build a clearer picture of the money laundering threat to the Island, and to use such intelligence on a proactive basis. Furthermore, the *Financial Services Provider* should refrain from referring such business to other *Financial Services Providers.*

5.37 The reporting of declined business is consistent with developing international best practice.

SECTION 6 – PROGRAMMES AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

6.1 *Financial Services Providers* should develop programmes against money laundering and terrorist financing. These programmes should include:

a. the development of internal policies, procedures and controls, including appropriate compliance management arrangement, and adequate screening procedures to ensure high standards when hiring employees;

b. an appropriate employee training programme; and

c. an audit function to test the system

6.2 The type and extent of measures to be taken should be appropriate to the risk of money laundering and terrorist financing, and to the size of the *Financial Services Provider*.

COMPLIANCE MANAGEMENT

6.3 For *Financial Services Providers* compliance management should include the appointment of a Compliance Officer, who may also be the MLRO, at the management level who:

- has sufficient skills and experience;
- reports directly to the Board;
- has sufficient seniority and authority so that the Board reacts to and acts upon any recommendations made;
- has regular contact with the Board so that the Board is able to satisfy itself that statutory obligations are being met and that sufficiently robust measures are being taken to protect itself against the risk money laundering ant terrorist financing;
- has sufficient resources, including sufficient time and (where appropriate) a Deputy Compliance Officer and support staff;
- has unfettered access to all business lines, support departments and information necessary to appropriately perform the function;

6.4 Financial Services Providers may demonstrate clearly apportioned roles for countering money laundering and the financing of terrorism, where the Compliance Officer (or other audit, compliance, review function):

- Develops and maintain systems and controls (including documented policies and procedures) in line with evolving requirements;
- Ensures regular audits of the AML/CFT programme;

- Advises the Board of AML/CFT compliance issues that need to be brought to its attention;
- Reports periodically, as appropriate, on the Financial Services Provider's systems and controls; and
- Responds promptly to request for information by the relevant authorities.

AUDIT FUNCTION

6.5 *Financial Services Provider* should, on a regular basis, conduct an AML/CFT audit to

- attest to the overall integrity and effectiveness of the AML/CFT systems and controls;
- assess its risks and exposures with respect to size, business lines, customer base and geographic locations.
- assess the adequacy of internal policies and procedures including
    i. Customer identification and verification,
    ii. Record keeping and retention ,
    iii. Reliance relationships and supporting documentation, and
    iv. Transaction monitoring;
- test compliance with the relevant laws and regulations;
- test transactions in all areas of the *Financial Services Provider*, with emphasis on high –risk areas, products and services;
- assess employees' knowledge of the laws, regulations, guidance, and policies & procedures;
- assess the adequacy, accuracy and completeness of training programmes; and
- assess the adequacy of the Financial Services Provider's process of identifying suspicious activity.

EMPLOYEE SCREENING

6.6 The extent of employee screening should be proportionate to the potential risk associated with money laundering or terrorist financing in relation to the business in general, and to the particular risks associated with the individual positions.

EMPLOYEE TRAINING

6.7 Where *Financial Services Providers* have staff they should ensure that all appropriate staff, (in accordance with Section 5(1) of the Regulations), receive training on money

laundering prevention on a regular basis, ensure all staff fully understand the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation.

The timing and content of training programmes

6.8 Although general provisions are made in Section 5(1) of the Regulations, they do not specify the exact nature of training to be given to staff, and therefore each *Financial Services Provider* can tailor its training programmes to suit its own needs, depending on size, resources and the type of business they undertake. Smaller organisations with no in-house training function may wish to approach third parties such as specialist training agencies, firms of attorneys or legal practitioners, or the major firms of accountants or management consultants. Training should be structured to ensure compliance with all of the requirements of the applicable legislation.

Where the Financial Service Provider has delegated the performance of relevant functions to a person or an institution in a Schedule 3 country, it must be satisfied that equivalent training and education procedures are in place in relation to the law and regulations of such country.

Staff awareness

6.9 Staff should appreciate the serious nature of the background against which the Regulations have been issued. They should be aware of their own personal obligations and of their personal liability under the legislation should they fail to report information in accordance with internal procedures and legislation. All staff should be encouraged to co-operate fully and provide a prompt and adequate report of any suspicious activities.

6.10 All staff need to be fully educated in the "Know Your Customer" requirements for the prevention of money laundering. Training should therefore cover not only the need to know the customer's true identity, but also, where a business relationship is being established, the need to know enough about the type of business activity expected in relation to the customer at outset (and on an ongoing basis) so that suspicious activity can be identified in the future.

New employees

6.11 Irrespective of seniority, all new employees should be given a general introduction to the background to money laundering and the procedures for reporting suspicious activities to the *MLRO,* prior to them becoming actively involved in day to day operations. New employees should also receive a clear indication of the importance placed on money laundering issues by the organisation, of the legal requirement to report, and of their personal legal obligations in this regard.

Operations staff

6.12 Staff who deal with the public such as cashiers, dealers, sales persons etc., are the first point of contact with potential money launderers, and their efforts are vital to an organisation's effectiveness in combating money laundering. Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer's identity, for new and existing customers and be aware of the procedures for treatment of declined business as outlined in these Guidance Notes. Training should be given on the factors which may give rise to suspicions about a customer's activities, and on the procedures to be adopted when a transaction is considered to be suspicious.

6.13 Staff involved in the processing of deals or transactions should receive relevant training in the processing and verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. Staff should be aware of the types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed. Staff should also be aware of the correct procedure to follow in such a circumstance.

6.14 All staff should be vigilant in circumstances where a known, existing customer opens a new and different type of account, or makes a new investment e.g. a banking customer with a personal account opening a business account. Whilst the *Financial Services Provider* may have previously obtained satisfactory identification evidence for the customer, the *Financial Services Provider* should take steps to learn as much as possible about the customer's new activities.

Training for supervisors and managers

6.15 Although Executive Directors and Senior Managers may not be involved in the day-to-day procedures for handling transactions that may relate to money laundering, it is important that they understand the statutory duties placed on them, their staff and the firm itself given that these individuals are involved in signing off procedures.

6.16 Supervisors and managers should receive a higher level of training covering all aspects of money laundering procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, the procedures relating to dealing with production and restraint orders and the requirements for verification of identity and retention of records.

Training for Money Laundering Reporting Personnel (*MLRO*)

6.17 *MLROs* (and also Deputy *MLROs)* should receive in-depth training on all aspects of the primary legislation, the Regulations and internal policies. They should also receive appropriate initial and ongoing instruction on the determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity.

Continuing vigilance and refresher training

6.18 Over time, due to the multiple demands placed on their time, there is a danger that staff may become less vigilant concerning money laundering, and therefore it is vital that all staff receive appropriate refresher training to maintain the prominence that money laundering prevention requires, and that they fully appreciate the importance that their employer places on it and their obligations arising from it.

SECTION 7 - RECORD KEEPING PROCEDURES

GENERAL

7.1 *Financial Services Providers* should maintain, for at least 5 years, all necessary records on transactions to be able to comply swiftly with information requests from the competent authorities. Such records should be sufficient to permit the reconstruction of individual transactions, so as to provide, if necessary, evidence for prosecution of criminal activity. *Financial Services Providers* should also keep records of identification data obtained through the customer due diligence process, account files and business correspondence that would be useful to an investigation for a period of 5 years after the business relationship has ended. This includes records pertaining to enquiries about complex, unusual large transactions, and unusual patterns of transactions. Identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

7.2 Where there has been a report of a suspicious activity or the *Financial Services Provider* is aware of a continuing investigation into money laundering relating to a client or a transaction, records relating to the transaction or the client should be retained until confirmation is received that the matter has been concluded.

7.3 Records relating to verification of identity will generally comprise:

- a description of the nature of all the evidence received relating to the identity of the verification subject;

- the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

7.4 Records relating to transactions will generally comprise:

- details of personal identity, including the names and addresses, of:
  (1) the customer;
  (2) the beneficial owner of the account or product;
  (3) any counter-party;
- details of securities and investments transacted including:
  (4) the nature of such securities/investments;
  (5) valuation(s) and price(s);
  (6) memoranda of purchase and sale;

(7) source(s) and volume of funds and bearer securities;

(8) destination(s) of funds and bearer securities;

(9) memoranda of instruction(s) and authority(ies);

(10) book entries;

(11) custody of title documentation;

(12) the nature of the transaction;

(13) the date of the transaction;

(14) the form (e.g. cash, cheque) in which funds are offered and paid out.

GROUP RECORDS

7.5 There may be circumstances in which group records are stored centrally off island. However, *Financial Services Providers should* ensure that appropriate records are maintained and can be retrieved promptly on request.

TRAINING RECORDS

7.6 So that *Financial Services Providers* can demonstrate that they have complied with the provisions of Section 5(1) of the Regulations concerning staff training, they should maintain records which include:-

(i) details of the content of the training programmes provided;
(ii) the names of staff who have received the training;
(iii) the date on which the training was delivered;
(iv) the results of any testing carried out to measure staff understanding of the money laundering requirements; and
(v) an on-going training plan.

ESTABLISHMENT OF REGISTERS

7.7 A *Financial Services Provider* should maintain a register of all enquiries made to it by the *Reporting Authority* and all disclosures to the *Reporting Authority*. The register should be kept separate from other records and contain as a minimum the following details:

- the date and nature of the enquiry,
- details of the account(s) involved; and
- be maintained for a period of at least 5 years.

Equivalency

7.8 Where the Financial Service Provider has delegated any or all of the foregoing functions to a person or institution in a Schedule 3 jurisdiction then it must be satisfied that the relevant records will be maintained in accordance with such regulation and will be available to the Monetary Authority on request and to the FRU or law enforcement authorities in accordance with the relevant procedures.

SECTION 8 –SECTOR SPECIFIC GUIDANCE

This section is intended to deal with specialised areas of relevant financial business which require more explanation and raise more complex issues than are dealt with in the general body of these Guidance Notes. This section must be read in conjunction with the other sections of these Guidance Notes.

The following types of relevant financial business are covered by these sector specific guidance notes:

- Mutual funds
- Banking
- Company formation and management
- Creation and administration of Trusts
- Insurance
- Real estate

MUTUAL FUNDS AND FUND ADMINISTRATORS

i) In this section:

a "Mutual Fund" or "Fund" is as defined in the Mutual Funds Law (2003 Revision) (the "Law") and may include a unit trust. Reference may also be made to the separate guidance in the Notes in the section on Trusts and Fiduciary Services and paragraph 3.37 of the Guidance Notes in relation to unit trusts.

A "Mutual Fund Administrator" or "An Administrator" is a person providing mutual fund administration as defined in the Law; that is: a person managing or administering a Mutual Fund (including controlling all or substantially all of its assets); a person providing the principal office of a Mutual Fund in the Cayman Islands or providing an operator to the Mutual Fund as defined in section 2 of the Law (a trustee of the unit trust, a general partner of a partnership or a director of a company).

A "Promoter" is as defined in section 2 of the Mutual Funds Law (as amended); namely, any person who causes the preparation or distribution of an offering document in respect

of a Mutual Fund or proposed Fund. An attorney at law or accountant acting on behalf of such person is not a Promoter.

ii) Who should be treated as the Applicant for Business?

	FSP	Applicant for Business
3	The Mutual Fund.	Investors should be treated as such for the purposes of the Guidance Notes.
4	A FSP incorporating a company/setting up a limited partnership/unit trust as part of a Mutual Fund structure (including acting as investor, shareholder and/or providing initial registered office).	Promoters. Where the mutual fund is a unit trust, the trustees. Where the mutual fund is a limited partnership, the general partner. Where the mutual fund is a corporation see the section on Company Formation and Management.
5	FSP providing registered office for Mutual Fund/general or limited partner (other than at the date of incorporation). FSP providing a principal office for an Administrator.	The Mutual Fund. The Administrator
6	Mutual Fund Administrator.	The Mutual Fund (the trustees of a unit trust; a general partner). When the Mutual Fund for which documentary evidence should be obtained is a limited partnership it will usually be sufficient to obtain evidence of the identity of the controlling General Partner. Given the special circumstances of mutual funds, it is recommended as good practice that an Administrator should not rely on the Mutual Fund falling into the exempted category by virtue of it being subject to the Regulations. However, the Administrator may be satisfied that the Mutual Fund, if not itself carrying out client identification or record keeping, has in place appropriate

		safeguards to ensure that its obligations under the Regulations are met. Promoters: Whilst promoters are not to be treated as applicants for business for the purposes of these Guidance Notes, it is industry best practice to ascertain the identity and background of any promoter relied upon.
7	FSP otherwise issuing and administering subscriptions/redemptions.	The Mutual Fund.

Company formation and opening of Bank accounts for Funds is provided for elsewhere in Section 8 of these Guidance Notes.

iii) When must the identity be verified?

The Regulations provide that there should be procedures in place requiring, as soon as reasonably practicable after contact is first made with an applicant for business, either satisfactory evidence of the applicants identity or that steps are taken which will produce satisfactory evidence of identity (Regulation 7(1)).

The time span in which satisfactory evidence has to be obtained depends on the particular circumstances and the practicalities of obtaining evidence before commitments are entered into between parties and before money passes (Regulation 11(2)).

In the Fund context, situations may arise in which satisfactory identification procedures have not been completed prior to the receipt of subscription funds or redemption settlement requests. Whether or not it is appropriate to transfer funds to a brokerage or similar account in the name of the Fund may depend on the nature of the investment. Mutual Funds and Administrators should ensure that they have in place tightly controlled procedures to ensure that shares/units/interests are not applied to investors and that redemption proceeds are not settled without senior management approval, the basis for such approval to be recorded and such records retained.

iv) How might identification of existing clients be carried out?

Refer to paragraphs 3.103 to 3.113 of the Guidance Notes.

If, after having conducted a risk assessment in accordance with paragraph 3.80 of the Guidance Notes, verification procedures or identification of an investor have not been completed prior to the date on which redemption is due to take place, the Fund should use the opportunity of redemption to seek satisfactory evidence of identity. It is industry best practice that, save in exceptional circumstances, payment of the redemption proceeds

should be made only to the investor and not to a third party. If payment is to be made to or from an account in the name of the investor with a regulated bank in the Islands or in a Schedule 3 country and the criteria set out in para. 3.90-3.93 are adhered to, that will be sufficient evidence of identity.

v) Particular issues on verification of identity of investors

a. One-off transactions.
For the purpose of the Guidance Notes a subscription to a mutual fund should not be treated as a one-off transaction (for which see paragraph 3.95-3.99) of the Guidance Notes).

b. *If the investor is a fund domiciled outside a Schedule 3 country but is administered in a Schedule 3 country*.
In such a case, the investor may fall within a category of exempted client. Evidence may also be satisfactory if the investor's administrator:

i) is subject to the Anti-Money Laundering regime of the Schedule 3 country.

ii) confirms in writing that it has obtained and maintains client verification evidence in accordance with the procedures of the Schedule 3 country.

c. Payment on an Account in a Bank in the Cayman Islands or a Schedule 3 Country
When redemption proceeds are paid into an account held in the name of an investor] at a bank in the Cayman Islands or a bank regulated in a Schedule 3 country, evidence identifying the branch or office of the bank and verifying that the account is in the name of the investor is satisfactory evidence of the investors identity and it will generally be unnecessary to obtain other documentary evidence. See para 3.90-3.94 of these Guidance Notes.

d. Corporate Group Introduction
It will not be necessary for identity to be re-verified or records duplicated if the identity of an investor has been verified by another entity within a group in a manner compatible with the Regulations and provided that written confirmation is obtained that the identification records will upon request be provided (see paragraphs 3.84 of the Guidance Notes). This is so even in circumstances when neither the investor nor the Bank from which he sends funds or investment is located in a Schedule 3 country.

vi) When may a successor administrator rely on the client verification evidence obtained by its predecessor?
Where a successor firm is acquiring administration of an existing mutual fund, the successor must ensure that the necessary due diligence has been performed prior to performing the administration. It may be possible to rely upon the evidence of identity obtained by a predecessor administrator provided that the original files, or certified copies of the original files, are transferred to the successor administrator and the

successor firm has assessed the quality of the evidence on investor identity. Where insufficient evidence exists, it may be appropriate to supplement with additional evidence to meet the standards required by these Guidance Notes.

At no time would it be appropriate to rely upon an eligible introducer exemption.

vii) What specific records should be kept and where?

Refer to paragraph 7.1 to 7.8 of the Guidance Notes.

It may be impractical for a regulated Fund itself to maintain records but it must ensure that all appropriate records are maintained on its behalf. Mutual Fund Administrators must ensure that they have client verification evidence appropriate to the administration of funds and, if the function is delegated to them, must maintain records on behalf of the fund for the requisite period.

viii) When procedures required by the Regulations may be maintained by a party not based in the Cayman Islands.
Maintenance by a person or institution regulated in a Schedule 3 country of all records and compliance with the procedures of such a Schedule 3 jurisdiction will be regarded as compliance with the Regulations and the Guidance Notes, subject to compliance with the provisions of paragraphs 3.91 to 3.94 and Section 7 of the Guidance Notes.

Procedures for reporting of suspicious activity

Regulated financial service providers must have internal reporting procedures in place to identify and report suspicious activity. Both Mutual Funds and their Administrators subject to the Regulations, have separate obligations to have such reporting procedures in respect of their relevant financial business. Although ultimate responsibility for having satisfactory procedures remains with the financial service provider, the obligation may be met in *two* ways other than by the appointment of an MLRO directly for the fund.

Where a Fund has no staff in the Islands and the issuance and administration of subscriptions and redemptions is done by a person subject to the regulatory regime of the Cayman Islands or a Schedule 3 country, compliance by that person with the procedures of such jurisdiction will be regarded by the Monetary Authority as compliance with the Regulations and the Guidance Notes.

Where a Fund or a Fund Administrator has delegated the reporting function to a regulated person in the Islands or a Schedule 3 country, consistent with the requirements of paragraph 3.56 of these Guidance Notes, the Monetary Authority will regard compliance with the procedures of such jurisdiction as compliance with the Regulations and the Guidance Notes.

A Fund or a Fund Administrator may also appoint a suitable third party as its MLRO, whether within or outside the Islands, provided that such appointment is consistent with the requirements of paragraph 5.4 a of these Guidance Notes.

The directors of the Fund or Fund Administrator should document, either as a board resolution or otherwise, the manner in which the entity has met its obligations for ensuring internal reporting procedures are in place to identify and report suspicious activity.

BANKING

1. Who is the applicant for business?

The applicant for business may be one of the following:

Example	Applicant for Business
1.	Direct Personal Clients
2.	Corporate clients (including trust and fiduciary clients)
3.	Partnerships / Unincorporated Businesses

2. Whose identity must be verified (subject to possible exceptions in 6 below)?

Example	Applicant for Business	Evidence of identity required for
1.	Direct Personal Clients	• Beneficial owners of accounts • Assets bought, sold or managed through the relationship • Satisfactory evidence, confirmed by using one or more of the verification methods outlined in section 3.19 of the Guidance Notes • Current, satisfactory bank reference from at least one bank with whom the prospective customer has had a relationship for not less than 3 years. If one is not forthcoming, satisfactory reference from a person or entity who has personal knowledge of the prospective customer and which establish his bona fides and integrity. • References confirmed for genuineness • For non face to face verification, suitably certified or authenticated documents

2.	Corporate clients (including trust and fiduciary clients)	• The company, that it exists
		• Consistent with that required for direct personal clients, documentary evidence of identity for all directors; all those with signing powers, including third parties; and beneficial owners. (See section 3.31, 3.35 and 3.39-3.41 in the Guidance Notes)
		• Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of direct personal relationships
		• Satisfactory evidence, confirmed by at least one of the following independent checks, of company's existence:
		  • Memorandum of Association and articles and Certificate of Incorporation
		  • Information about the identity of controlling shareholders and directors, e.g., Register of Directors, Register of Members
		  • Understanding of all relevant party and inter-company relationships
		  • It may be appropriate to obtain information relating to customers or suppliers and the background of major shareholders and directors

3.	Partnerships / Unincorporated Businesses	• The entity, that it exists
		• Consistent with that required for direct personal clients, documentary evidence of identity required for partners/managers; all those with signing powers, including third parties; and beneficial owners as defined in the Guidance Notes, Section 3.31
		• Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of direct personal relationships
		• Satisfactory evidence, confirmed by at least one of the following independent checks, of existence of partnership / unincorporated business:
		  • Partnership agreement or excerpt if relevant
		  • Certificate of Registration
		  • Information about the identity of controlling partners / shareholders, e.g., excerpt from partnership document
		  • Establish all relevant party relationships

3. When must identity be verified?

Client verification information should be obtained prior to opening account or establishing business relationship. If it is not forthcoming at the outset or within a reasonable time the relationship should be re-evaluated and transactions should not proceed. For exceptions, refer to the Guidance Notes, "Timing and Duration of Verification", Sections 3.62 – 3.65.

4. When might it be possible to rely on third parties to verify identity?

Bankers should use their judgment in determining whether or not in the context of banking they should place reliance on the due diligence procedures for intermediaries. In cases in which reliance is placed on the intermediary, senior management must make a judgement as to whether or not it would be prudent to obtain appropriate evidence of client verification either by provision by the Introducer of primary documentation relating to this or by written confirmation from the Introducer that it has satisfied itself as to the bona fides and integrity of the client. For guidance on whether an entity qualifies as an Eligible Introducer refer to the Guidance Notes, "Procedures for Introduced Business", Sections 3.66 – 3.94.

5. When might it be possible for identity to be verified by a party not based in the Cayman Islands?

Reliance on exemption (and therefore dispensation of the need to obtain normal evidence of client identity) when conducting mainstream banking business will be rare. Due diligence should be performed in accordance with the Guidance Notes, "Procedures for Introduced Business", Sections 3.62 – 3.94.

6. When may there be no need or might it not be practicable for identity to be verified?

Refer to the Guidance Notes, "Exceptions to Verification Requirements", Sections 3.94 – 3.105.

7. What information should be obtained in relation the proposed transaction, business and source of assets?

In addition to those listed in the main body of the Guidance Notes:

Example	Applicant for Business	Information which should be obtained
1.	Direct Personal Clients	• Full details regarding Source of Funds

		• Sufficient information to anticipate normal business activity, including type of products required and general level of likely activity
2.	Corporate clients	• Full details regarding Source of Funds • Sufficient information to anticipate normal business activity, including type of products required and general level of likely activity • Sufficient information regarding intra-group relationships, if any; clients; service providers; and trading partners to establish a trading profile which can be monitored against transactions
3.	Partnerships/ Unincorporated Businesses	• Full details regarding Source of Funds • Sufficient information to anticipate normal business activity, including type of products required and general level of likely activity • Sufficient information regarding intra-group relationships, if any; clients; service providers; and trading partners to establish a trading profile which can be monitored against transactions

8. How should the business of the client be monitored?

Refer to the Guidance Notes, "On-Going Monitoring of Business Relationships", Sections 4.1-4.10.

9. What warning signs or "red flags" should service providers be alert to?

Refer to Appendix K of the Guidance Notes

10. How might identification of existing clients be carried out?

As indicated in the Guidance Notes, sections 3.88-3.95, banks should conduct a risk assessment. Those clients assessed as high risk should be actioned first. The bank should ensure the information on file identifies the party and enables the bank to effectively monitor the account.

11. What specific records should be kept and where?

Refer to the Guidance Notes, Sections 7.1-7.8. (to be provided)

12. When should enhanced due diligence be applied?

It is recommended that enhanced due diligence be applied in situations where the bank is particularly exposed to reputational risk. Reference to Section 3 of the Guidance Notes – paragraphs 3.42 – 3.47 provides information on procedures for Associations Not for Profit (Including Charities), Politically Exposed Persons (PEPS) and High-Risk Countries. Additional examples would include cases whereby a client is confidentiality-driven, or presents a multi-layered structure of beneficial ownership.

COMPANY FORMATION AND MANAGEMENT

Who is the Applicant for business?

Company formation

In the case of forming a company, the applicant for business is the client upon whose instructions the company is formed. This may or may not be a proposed shareholder. In addition to obtaining identification evidence for the client, it will normally be necessary to obtain:

i. An explanation of the nature of the proposed company's business, and the source of funds.
ii. Satisfactory evidence of the identity of each of the proposed principal beneficial owners (see paras 3.31 and 3.35)

In some circumstances reliance may be placed on the due diligence of other persons. Refer to the section on Introduced business in the Guidance Notes.

Company management

Where a company manager provides corporate services to a company, the client may or not be the company itself. However one must look behind the company for due diligence purposes and, depending upon the circumstances, investigate and obtain proof of identity of any or all of the following:

a) the shareholders (or beneficial owners if different from the registered shareholders);
b) the directors and officers;
c) anyone who is giving instructions to the company manager on behalf of the company;
d) anyone who introduces any of the above persons to the company manager.

However it is recognized that obtaining due diligence on all of the above in every case could be onerous and could lead to a duplication of procedures, unnecessary complication and eventual loss of legitimate business. The money laundering regulations and the notes therefore allow for reliance, in certain circumstances, on third party intermediaries. For guidance in this area see section on *Introduced Business* in the guidance notes.

The following will therefore apply:

1. Where the company manager is approached by a shareholder, beneficial owner or directors and officers as the applicant for business, the company manager should do appropriate due diligence on the shareholders and beneficial owners, the directors and anyone who gives instructions to the company manager on behalf of the company, the directors, officers or the shareholders in accordance with the sections of these guidance notes dealing with corporate clients (see section 3.31 to 3.37).

2. Where the company manager is approached by a person who gives instructions to the company manager on behalf of the company, the company manager should do appropriate due diligence on that person, the shareholders, and the directors and officers accordance with the sections of these guidance notes dealing with corporate clients (see section 3.31 to 3.37). However it may, in certain circumstances, be acceptable to rely solely on the due diligence of the person giving those instructions. (See section on introduced business)

Where the company manager relies upon the due diligence of an introducer such a decision must be made by senior management and the reasons for the decision must be documented. In addition the company manager must carry out appropriate due diligence on the introducer or intermediary to ensure their eligibility and ensure that written undertakings are received from the intermediary in accordance with the guidance notes.

Structured Finance Companies

Where a company is established to undertake one or more structured finance transactions, it may be established by a trustee for that transaction or generally. In such cases, the Financial Service Provider must identify the parties and the commercial purpose and conduct enquiry on any or all of the following persons and entities as appropriate in the circumstances, with a view to ensuring that appropriate due diligence and anti-money laundering compliance is applied to the identity of the investors and the flow of funds in accordance with the Regulations and Guidance Notes, or in accordance with the regulatory regime of a Schedule 3 country.

Such enquiry may extend to any or all of the following:
i) the arranger; or
ii) the originator; or
iii) where relevant, the promoter; and
iv) investors in the securities of the company;

Discontinued Relationships

Funds held to the order of a client or prospective client should only be returned to the source

from which they came and not to a third party.

Ongoing Monitoring

In order to be alert for instances of money laundering company managers must continue monitoring the activities of their client companies for signs of unusual or suspicious activities. Changes in transaction type, frequency, unusually large amounts, geographical origins and destinations attributes and change in account signatories all warrant special attention.

Hold Mail and c/o Addresses

Sometimes the directors or beneficial owners of client companies request that mail not be forwarded but held at the registered office for storage or later collection. These are not necessarily suspicious acts but do carry higher risk and should warrant special attention. Evidence of identity of the beneficial owners should be obtained even where the client is introduced by eligible introducers. Clients who request "c/o" addresses should also receive additional attention.

Bearer Shares

The Cayman Islands company law allows the issue of bearer shares. Bearer shares can be used to conceal the identity of beneficial owners. Company managers should therefore only be a party to the issue of bearer shares where the shares are physically held by the company manager or by a custodian authorized or recognised by the Monetary Authority to the order of the beneficial owner. Such shares should not be released to the beneficial owner and may only be physically transferred to another entity authorised or recognised to act as a custodian under the companies law. If any such shares are in issue prior to these Guidance Notes company managers should ensure that such shares are lodged with a custodian within the period prescribed under the law.

Changes in service provider

Clients have the right to choose which management company should manage their affairs and to change to others if they so desire. However company managers who are asked by a prospective client to take over the management of a company which is being managed by another service provider should communicate with that service provider and make appropriate enquiries as to the reason for the transfer of business.

Provision of Directors and Officers

Where a company manager provides directors and officers to a managed company he should ensure that all statutory requirements with regard to keeping and filing details of the shareholders, directors and officers as required by law, are complied with within the period allowed by statute.

TRUSTS

1. Creation and Administration of Trusts

"Trust business" may be divided into three categories for the purposes of the Regulations and these Guidance Notes:-

(a) unit trusts which are therefore covered by the mutual funds part of this section in relation to their creation and administration;
(b) bare trusts or nomineeships where the trustee is acting both as a trustee and as an agent and Regulation 9 will apply;
(c) all other trusts, where the trust is not a mutual fund and the trustee is a principal as a matter of law.

This section deals solely with the creation and administration of trusts falling within category (c).

2. Competent Staff

FSPs and the Monetary Authority are expected to pay particular attention to ensuring that staff working in these areas are properly competent, qualified (where necessary or appropriate) and have the requisite experience for a person in their position within the organisation.

3. Creation of a Trust

3.1. Settlor
Where a new trust is being created, the Applicant for Business will be the settlor (or all of the settlors if more than one).

3.2. Settled Assets
FSPs should also make appropriate inquiry as to the source of the assets a settlor intends to settle. This will necessarily vary from case to case and depend on many factors, such as the type of trust intended to be created, the relative and absolute value of the assets intended to be settled, the objectives of the settlor in creating the trust and the timeframe within which the parties are working.

3.3. Ongoing Obligations
FSPs must recognise the need to adopt ongoing procedures in relation to trusts. In particular, each time assets are added to the trust by a new or existing settlor the same procedures should be followed.

4. Transfer of an Existing Trust

Where an FSP is approached to become an additional or successor trustee, it is recognised that the concept of an "Applicant for Business" as used in the Regulations does not apply easily.

4.1. Previous Due Diligence

Trustees act as a body. Additional or successor trustees "step into the shoes" of the existing or predecessor trustees. An FSP who is an additional or successor trustee should inquire of the existing or predecessor trustees whether appropriate inquiries were made of the settlor or settlors at the time of creating the trust and at the time of addition of any assets to the trust, and seek to obtain the originals or copies of the relevant due diligence documentation (e.g. verification of the settlor's identity and source of funds). Having done so, the FSP should consider whether it is adequate, according to the circumstances of the particular case. However, in some cases such documentation may not be available or upon review may not be adequate. In such cases the FSP should make reasonable inquiries of its own:-

(a) Where the Settlor is Alive
Where the settlor is still alive, the FSP should make the relevant inquiries of the settlor.

(b) Where the Settlor is Dead
Where the settlor is dead, the FSP should make reasonable inquiries about the settlor of such persons as may be appropriate in the circumstances of the particular case e.g. the existing or predecessor trustees or the beneficiaries. In particular, if the beneficiaries are relatives of the deceased settlor, as will often be the case, appropriate inquiry of the oldest beneficiaries may be the most fruitful.

5. Trusts Established Prior to 1 September 2000

In order to comply with the regulations on the treatment of existing business, the FSP should review existing trusts in the same way as if it were being invited to act as a successor or additional trustee of such trusts.

6. Possible Abuse of Trusts by Money Launderers

There appears to be limited potential for trusts to be used at the initial or placement stage of the money laundering process. Indeed, criminally derived funds would normally already have to have been inserted into the financial system before such assets could be placed into a trust. At the layering and integration stages of money laundering, however, there is greater potential for the misuse of trusts. Once the illegal proceeds have already entered the banking system, trusts could be exploited to further confuse the links between these proceeds and the illicit activity that generated them. The FATF have expressed concerns that this process may be even more effective if it is carried out in a number of countries and through legal professionals able to claim professional secrecy.

7. Circumstances Prompting Increased Vigilance

FSPs are urged to be particularly vigilant in the following areas:

7.1 Links with High Risk Countries

[See Sections 3.52 – 3.54 High risk Countries]

7.2 Total Changes of Beneficiaries

Where all of the existing beneficiaries are removed and different beneficiaries are added, or where this is intended, or where the trust is intentionally structured to permit this.

There may be perfectly legitimate reasons for this occurring or for this to be possible, but FSPs should endeavour to ascertain what these are.

7.3 Unexplained Requests for Anonymity

Where the settlor's stated reason for establishing a trust is the need for anonymity or confidentiality in relation to himself or the beneficiaries.

It should not be automatically inferred that this in itself is an illegitimate need. There are many instances where a settlor may desire that the extent or nature of his wealth is not known to third parties – such as children, the media, business or industry colleagues, potential kidnappers, industry competitors etc. The legitimate need for privacy is acknowledged and supported in the Cayman Islands as in other countries and may be a reason for establishing a trust. However, FSPs are encouraged to adopt a conservative and cautious approach in this area. In particular, where the reasons given by the settlor for the need for anonymity or confidentiality are not clear or are unconvincing, FSPs should take appropriate further action.

7.4 Beneficiaries with no apparent connection to the settlor

Where there is no readily apparent connection or relationship of the settlor to the beneficiaries. Since the economic nature of a trust is a mechanism for the settlor to benefit a beneficiary, typically not in return for any consideration (payment, transfer of assets or provision of services), FSPs should endeavour so far as possible to ascertain the settlor's reasons for wanting to benefit a beneficiary with whom he seemingly has no connection. This can be a matter of great sensitivity (for example, where the beneficiary turns out to be an illegitimate child of the settlor) and FSPs are encouraged to take this into account while pursuing necessary or appropriate inquiries.

7.5 Unexplained Urgency

FSPs are encouraged to inquire as to the reasons for any urgency, especially where the settlor is indicating that some of the due diligence process can or will be completed after the trust has been established or a transaction has been entered into by the trustees or an underlying company owned by the trust.

7.6 Potentate risk
[See section 3.48-3.51 – Politically exposed persons]

INSURANCE

Note that a significant amount of the following guidance was extracted from the International Association of Insurance Supervisors Guidance Paper on Anti Money Laundering ("AML") and Combating the Financing of Terrorism ("CFT") Oct 2004

SCOPE OF THE MONEY LAUNDERING REGULATIONS AND PURPOSE OF THIS SECTOR SPECIFIC GUIDANCE

1. The Money Laundering Regulations (2008 Revision) are applicable to insurance business as listed in the First Schedule of the Regulations which includes life and annuity business, and all of which are described as long term insurance.

2. In addition Regulation 4 includes within the types of relevant financial business, the business of an insurance manager, an insurance agent, or an insurance broker within the meaning of the Insurance Law (2004 Revision).

3. This sector specific guidance seeks to provide practical assistance to insurers and insurance intermediaries in complying with the Regulations, interpreting and applying the general provisions of these Guidance Notes but also for all insurers to adopt sound risk management and internal controls for its operations.

4. The principal obligation to perform AML procedures under the Regulations falls on each FSP in respect of the parties with which it directly transacts, that is to say its own applicants for business. For example, in the case of an insurance manager, its applicants for business will largely be insurance companies, which themselves, as licensees also will have their own independent obligations to perform AML checks as appropriate on policyholders or others with whom they conduct relevant financial business. As a practical matter, however, many insurers, particularly those without their own dedicated staff, may often delegate the operation of AML procedures to managers, but each FSP retains ultimate responsibility for ensuring that appropriate steps are taken in respect of its own applicants for business. Where an insurer is un-staffed, section 5.4 of the Guidance Notes as to the MLRO will be applicable.

5. In relation to insurance business, significant factors that will affect the level of risk of any transaction or business relationship include:

- The applicants for business,
- The product to be underwritten or sold,
- The nature of the business relationship formed, and
- The method of payment of the premium.

CLASS A AND CLASS B INSURERS, BROKERS AND AGENTS

NATURE OF PRODUCTS UNDERWRITTEN/SOLD

GENERAL (NON-LIFE)

6. A significant factor determining the level of AML or CFT risk in any product is the level of premium payable on the policy and method of payment. For example, a motor policy with an annual premium of $1000 will present a much lower risk than one on a luxury car or car fleet in the case of a commercial motor policy, which commands a much higher premium and value at risk. Premium payments made in cash are generally a concern. For example, premiums for property and casualty policies in the case of condominium developments may be significant and insurers should be especially vigilant when requests are made for large premiums to be paid in cash. Sound claims management is essential as money laundering or terrorist financing can occur through inflated or bogus claims, e.g. by arson or other means causing a fraudulent claim to be made.

7. FEATURES OF HIGH RISK AND LOW RISK GENERAL INSURANCE PRODUCTS WITH EXAMPLES

Low risk	Low premiums, inability to make claims without substantial reliable evidence of loss. Note that products rated as low AML/CFT risk may also be rated a low fraud risk, but not always.
Example of low risk	A single, individual travel policy may be considered low risk simply because the premium is low and the term date is short. Other travel policies however, for example, annual or group, may be considered to pose a relatively increased risk and thus controls should be applied appropriately.
High risk	High premium amounts and the ability to pay in cash, to overpay premiums, and to cancel the policy to seek a premium refund. Also the greater risk of fraud will generally mean a greater risk of AML/CFT.
Example of high risk	May include Cash-In-Transit policies or Fidelity Guarantees where the likelihood of manipulation and conspiracy is greater.

LONG TERM (LIFE)

8. FEATURES OF HIGH RISK AND LOW RISK LONG TERM (LIFE) INSURANCE PRODUCTS WITH EXAMPLES

Low	1. Life insurance policies where the premium payable annually is no more than CI$800 or a single premium of no more than CI$2000.
	2. Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral
	3. A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.
High	1. Unit-linked or with profit single premium contracts
	2. Single premium life insurance policies that store cash value
	3. Fixed and variable annuities
	4. (Second hand) endowment policies.

APPLICANTS FOR BUSINESS - ESTABLISHING A BUSINESS RELATIONSHIP

9. Before an insurance contract is concluded between customer and insurer there is already a pre-contractual business relationship between the customer and the person selling the policy, be that the insurer or an intermediary. After a policy is taken out:

- the insurer covers a certain risk described in the contract and policy conditions
- certain transactions may take place such as premium payments, payments of advance or final benefits, and
- certain events may occur such as a change in cover or a change of beneficiaries.

10. The insurer will need to carefully assess the specific background, and other conditions and needs of the customer. This assessment is already being carried out for commercial purposes (determining the risk exposure of the insurer and setting an adequate premium) as well as for reasons of active client management. This will lead to a client profile, which could serve as a reference to establish the purpose of the contract and to monitor subsequent transactions and events.

11. The insurer should realise that creating a customer profile is also of importance for AML/CFT purposes and therefore for the protection of the integrity of the insurer and its business. Generally, it will be appropriate to obtain information as outlined below, but other circumstances may require alternative information.

12. INSURANCE SPECIFIC INFORMATION THAT MAY BE REQUESTED TO SUPPLEMENT AS NECESSARY THAT OUTLINED IN SECTION 3 OF THESE GUIDANCE NOTES

Applicant for business (proposer)	Insurance specific information
Personal	▪ That the person is the proposer and has an insurable interest in the risk to be insured ▪ The property or other risk to be insured and its valuation. ▪ Any other beneficiaries with insurable interests and/or claim on the policy. ▪ The source of funds for the payment of the premium.
Corporate	▪ That the person proposing represents and is authorised to represent the company, which has an insurable interest in the risk to be insured ▪ The property or other risk to be insured, and its valuation. ▪ Any other beneficiaries with insurable interest and/or claim on the policy. ▪ Source of funds for the payment of the premium.

13. When must identity be verified?

In principle, identification and verification of customers and beneficial owners should take place when the business relationship with that person is established. This means that the policyholder (or its owner / controller) needs to be identified and their identity verified before, or at the very latest at the moment when, the insurance contact is concluded. That said, identification and verification of the beneficiary may take place after the insurance contract has been concluded with the policyholder, provided the money laundering risks and financing of terrorism risks are

not significantly high and are effectively managed. However, identification and verification must occur at or before the time of claims settlement, premium refunds or the time when the beneficiary intends to exercise vested rights under the policy.

14. When might it be possible to rely on third parties to verify identity?
When introduced by an Eligible Introducer (see and follow guidance in sections 3.66-3.93).

15. When may there be no need or might it not be practicable for identity to be verified?
Where a Class A insurer effects insurance business directly or a Class B insurer writes third party business, which are not long-term business as per Schedule I of the Regulations, there would not be a need to verify the identity of a proposing policyholder. However, the need for internal controls in particular those designed to deter and detect fraud should be present in all licensed insurers as per the Insurance Law. That said a risk based approach set out in the guidance above may lead an insurer to conclude that minimal verification is required in certain cases.

16. What additional information might be requested and when?
In insurance, various transactions or 'trigger events' occur after the contract date and indicate where due diligence may be required. These trigger events include claims notification, surrender requests and policy alterations, including changes in beneficiaries. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors. In this respect "transactions" should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, requests for changes in cover, redemption, cancellation, claim submission premium payments, requests for changes in benefits, beneficiaries, duration, etc.

17. How should the business of the client be monitored?
In general the insurer should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. It should assess if the change/transaction does not fit the profile of the customer and/or beneficial owner or is for some other reason unusual or suspicious.

18. What warning signs or "red flags" should service providers be alert to?

1. Requests for a return of premium to be remitted to persons other than policy holder.
2. Claims payments paid to persons other than policyholders and beneficiaries.
3. Unusually complex holding company or trust ownership structure.
4. Claims fraud.
5. A change in beneficiaries (for instance, to include non-family members).
6. A change/increase of the premium payment (for instance, which appear unusual in the light of the policyholder's income or where there are several overpayments of policy premiums after which the policyholder requests that reimbursement is paid to a third party).
7. Use of cash and/or payment of large single premiums.
8. Payment/surrender by a wire transfer from/to foreign parties.
9. Payment by banking instruments, which allow anonymity of the transaction.

10. Change of address and/or place of residence of the policyholder.
11. Lump sum top-ups to an existing life insurance contract.
12. Lump sum contributions to personal pension contracts.
13. Requests for prepayment of benefits.
14. Use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution).
15. Change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment).
16. Early surrender of the policy or change of the duration (including where this causes penalties).
17. Requests for multiple policies to be taken out for premiums slightly below any publicised limits for performing checks, such as checks on the source of wealth or cash payments.

The above list is not exhaustive. Insurers should consider other types of transactions or trigger events, which are appropriate to their type of business.

19. What specific AML/CFT records should be kept and where?
See 7.1–7.8. Where reliance is placed on an eligible introducer the requirements of section 3.66-3.94 must be followed. All records, including discharge documents must be "readily accessible".

INSURANCE MANAGERS

NATURE OF THE PRODUCTS UNDERWRITTEN/SOLD

20. Money laundering and the financing of terrorism can occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, and fronting arrangements, or by the misuse of normal reinsurance transactions. Examples include:

- the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds
- the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding
- the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers.

21. For Class B insurers the line of business or risk assumed is much less relevant to the assessment of AML/CFT risk, than the persons or applicants for business involved. This is because even the typically lowest risk product could potentially be used for money laundering for example, workers compensation schemes may be established for fictitious personnel or be funding mechanisms for terrorists awaiting assignment. One factor that should help to mitigate this risk is the involvement of independent third parties e.g. medical practitioners, claims

adjusters and government agencies to substantiate claims. In the international market the scope for lines of business in insurers is unlimited. The focus for financial service providers entering into relationships with Class B insurers, should be the operators and owners of the insurer, the business rationale for the insurer, its relationships and source of funding.

APPLICANTS FOR BUSINESS

22. The applicant for business to insurance managers may be either an existing insurer, possibly already under management and regulated, or it may be a company or group of individuals seeking to establish a new insurer. (The following guidance regarding due diligence and documentation to be obtained falls outside and is separate from that which the manager may necessarily obtain in preparing a licence application for a insurer or insurer to be formed as per the Insurance Law and Regulations there under.)

EXISTING INSURER TO BE MANAGED

23. It is recognized that where insurers already formed and licensed are transferred to an Insurance Manager, although the insurer, as an applicant for business, may be regarded as an exempted client regarding the verification of identity as per 3.103, the nature of the relationship between the manager and the insurer may require that additional commercial due diligence is obtained and maintained in order to discharge its obligations as manager and for on-going monitoring. See in particular 3.60 and 3.66.

24.Verification Subjects
For Class B insurers see the general guidance in the Guidance Notes section 3.31, Directors, Officers and Controllers, which is applicable according to the circumstances. In addition, Class B insurance entities can take various legal forms such as limited partnerships thus the due diligence should be tailored accordingly. Class B insurers can also be established as segregated portfolio companies under the Companies Law (2004 Revision). In that case 3.31 applies to both the core company and the individual cell where the ownership or control is different.

NEW CLASS B INSURER TO BE FORMED

25. For Insurance Managers acting for clients in the formation of a Class B insurer, note the general guidance in this section 8 on company formation and the relevant sections of the GN including 3.31, 3.3, 3.9 and 3.38. In the case of company formation it may be necessary to consider any sponsor, initiator, broker or promoter who instructs the creation of the Class B insurer, and its identity verified. In addition, note the specific guidance in 3.52-3.54 where the underlying business is from high-risk countries.

26. When must identity be verified?
As soon as is reasonably practicable after the business relationship is established, by necessity no later than the time of application for licensing under the Insurance Law, ideally before the receipt

of any funds and always before the return of any premium paid or other capital amount received on behalf of the insurer.

27. When might it be possible to rely on third parties to verify identity?
When introduced by an Eligible Introducer (see and follow guidance in section 3.66-3.94).

28. What additional information might be requested and when?
All changes subsequent to licensing should be monitored and in particular changes to the ownership or control or the business plan may require further information and verification.

29. How should the business of the client be monitored?
All changes to the nature of the business of the Class B insurer should be assessed and a decision made whether such constitutes a trigger requiring further verification or investigation/information. At a minimum the Annual Statement of Operations filed with the Cayman Islands Monetary Authority provides a periodic opportunity to review the relationship and the business of the client, or upon renewal of the service agreement.

30. What warning signs or "red flags" should service providers be alert to?

1. Requests for a premium refund to be remitted to persons other than the policy holder.
2. Dividends paid to persons other than shareholders.
3. Unusually complex holding company or trust ownership structure.
4. Concealment of identity of client or the beneficial owner; of the ownership of funds.
5. Incomplete application details and lack of willingness to provide evidence to answers required.
6. Unexplained changes in investment pattern; investment taken against advice or not appropriate to insurer's real needs;
7. Sudden changes in intermediary transaction pattern;
8. Unexplained receipt of bulk premiums from intermediary accounts.
9. Third party transactions (payments or withdrawals);
10. Multiple sources of payment or cross jurisdiction funding for payment;
11. Payment of premiums from early surrender of another investment in unusual circumstances;
12. Payment from obscure or unregulated organisations;
13. Unnecessarily complex transactions or intentions;
14. Requests for part investment and return of surplus funds;
15. Immediate interest in surrender penalties or requests for large withdrawals or policy loans;
16. Early surrender of a contract;
17. Receipt of unexplained wire transfers and requests to return wire transfers;
18. Requests for no correspondence to go to client.

31. What specific AML/CFT records should be kept and where?

See 7.1 –7.8 and in addition, all documentation listed above together with initial and subsequent information necessary for on-going monitoring should be held, whether as duplicate or back up by the Manager at its office in Cayman. Where reliance is placed on an eligible introducer the requirements of section 3.66-3.94 must be followed. All records, including discharge documents must be "readily accessible".

SECURITIES AND INVESTMENT BUSINESSES

Introduction

Investment businesses are less likely than banks to be at risk during the initial placement stage of money laundering because cash settlement of investment transactions is relatively rare. Instead, in the securities and investment business, it is more likely that a *Financial Services Provider* will come into contact with the layering and integration stages of a money laundering operation than the placement of cash. Often the money launderers' intention will be simply to carry out transactions for their own sake, to complicate the audit trail in the event of an investigation at a later stage.

Layering and integration of laundered money tend to occur in the securities and investment businesses because the liquidity of many investment products attracts sophisticated money launderers, as it allows them the opportunity to move funds quickly and easily from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy. Investment businesses are also able to transfer monies across borders quickly and efficiently. Complex and sophisticated new investment products that are constantly being introduced, and the lack of order in emerging markets, offer considerable potential to the money launderer.

Procedures and records maintained by investment businesses constitute an important audit trail and play an important part in combating money laundering.

12. Who is the applicant for business?

The applicant for business may be one of the following:

Where the *Financial Services Provider*	Applicant for Business is
acts as agent in buying, selling, managing, subscribing for or underwriting securities	the principal
acts as principal or makes arrangements in buying, selling, managing, subscribing for or underwriting securities	the counterparties
advises an investor or potential investor on the merits for buying, selling, managing subscribing for or underwriting securities	the investor or potential investor

13. How is identity of Applicant for Business verified (subject to possible exceptions in 6 below)?

If the Applicant for Business is a natural person (irrespective of his or her capacity as the principal, counterparty, or investor), apply the guidance contained at sections 3.9 to 3.29 of the Guidance Notes.

If the Applicant for Business is a not a natural person, apply the guidance contained at sections 3.31 to 3.47 of the Guidance Notes.

14. When must identity be verified?

Client verification information should be obtained prior to opening account or establishing business relationship. If it is not forthcoming at the outset or within a reasonable time, the relationship should be re-evaluated and transactions should not proceed. For exceptions, refer to the Guidance Notes, "Timing and Duration of Verification," sections 3.62 – 3.65.

If the *Financial Services Provider* acquires the clients/accounts of another *Financial Services Provider*, if the money laundering procedures previously undertaken have not been in accordance with Cayman Islands requirements, or the procedures cannot be checked by the *Financial Services Provider* acquiring the new customer, or the customer records are not available to the acquiring *Financial Services Provider*, then verification of identity procedures will need to be undertaken for all transferred customers as soon as is practicable.

15. When might it be possible to rely on third parties to verify identity?

Financial Services Providers should use their judgment in determining whether or not in the context of the intended business relationship they should place reliance on the due diligence procedures of intermediaries. In cases in which reliance is placed on the intermediary, senior management must make a judgement as to whether or not it would be prudent to obtain appropriate evidence of client verification either by provision by the Introducer of primary documentation relating to confirm identity, or by written confirmation from the Introducer that it has satisfied itself as to the bona fides and integrity of the client. For guidance on whether an entity qualifies as an Eligible Introducer refer to the Guidance Notes, "Procedures for Introduced Business," sections 3.66 – 3.93.

16. When might it be possible for identity to be verified by a party not based in the Cayman Islands?

Financial Services Providers may rely on an Eligible Introducer's Form in accordance with these Guidance Notes. In general, in all other situations, reliance on exemption (and therefore

dispensation of the need to obtain normal evidence of client identity) will be rare. Due diligence should be performed in accordance with the Guidance Notes, "Procedures for Introduced Business," sections 3.66 – 3.93.

17. What information should be obtained in relation to the proposed transaction, business and source of assets?

In addition to those listed in these Guidance Notes:

Example	Applicant for Business	Information which should be obtained
5.	Where the principal, counterparty(ies), or investor or potential investor is a person	Sufficient information to anticipate normal business activity, including type of products required and general level of likely activity and investment goals.
6.	Where the principal, counterparty(ies), or investor or potential investor is a company, or otherwise	Sufficient information to anticipate normal business activity, including type of products required and general level of likely activity and investment goals; and Sufficient information regarding intra-group relationships, if any; clients; service providers; and trading partners to establish a trading profile which can be monitored against transactions.

18. How should the business of the client be monitored?

For each investment transaction, the *Financial Services Provider* should record the information required under section 7.4 of the Guidance Notes. In addition, the *Financial Services Provider* should consider whether the transaction is consistent with the client profile and client's stated investment goals and expectations, and should also be alert to the "red flags" listed in section 9 below.

In addition, the review of the client's transactions should be in accordance with sections 4.1 - 4.13 of the Guidance Notes, "On-Going Monitoring of Business Relationships," and sections 5.11 – 5.16, "Identifying Suspicions".

19. When might enhanced due diligence be appropriate?

Enhanced due diligence may also be applied in situations where the *Financial Services Provider* is particularly exposed to reputational risk. Section 3 of the Guidance Notes – (sections 3.38 –

3.50) provides information on procedures for Associations Not for Profit (Including Charities), Politically Exposed Persons (PEPs), and High-Risk Countries.

Additional examples would include cases whereby a client is confidentiality-driven, or presents a multi-layered structure of beneficial ownership for no apparent business reason, or when "red flags" are noticed.

20. What warning signs or "red flags" should service providers be alert to?

Appendix K of the Guidance Notes contains examples of "red flags" for which a *Financial Services Provider* must be alert. The following list contains additional "red flags" which may indicate a money laundering scheme. As stated at Appendix K, the presence of any of the following behaviours does not necessarily indicate an inappropriate or illegal act, but the *Financial Services Provider* should be on enquiry and be satisfied with any explanation, especially as more and more of the these activities are present.

- clients who are unknown to the *Financial Services Provider* and verification of identity / incorporation proves difficult;
- clients who wish to deal on a large scale but are completely unknown to the *Financial Services Provider*;
- clients who wish to invest or settle using cash;
- clients who use a cheque that has been drawn on an account other than their own;
- clients who change the settlement details at the last moment;
- clients who insist on entering into financial commitments that appear to be considerably beyond their means;
- clients who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
- clients who have no obvious reason for using the services of the *Financial Services Provider* (eg: clients with distant addresses who could find the same service nearer their home base; clients whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere);
- clients who refuse to explain why they wish to make an investment that has no obvious purpose;
- clients who are introduced by an overseas agent based in a country noted for drug production or distribution or a client introduced by an overseas branch, affiliate or other service provider based in a non Schedule 3 country;
- clients who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from a non Schedule 3 country;

- clients who transfer funds or shares to accounts in a non Schedule 3 country;
- clients who make back to back deposit/loan transactions with subsidiaries or affiliates of overseas financial services businesses;
- clients who want to transfer funds overseas or make payment in foreign currency which appear to have no commercial objective;
- clients who indulge in much activity with little or no profit over a number of jurisdictions;
- clients who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;
- clients who purchase low grade securities in an overseas jurisdiction, sell locally and then purchase high grade securities with the proceeds;
- clients who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
- clients who wish to maintain a number of trustee or clients' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
- any transaction involving an undisclosed party;
- transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral;
- significant variation in the pattern of investment with reasonable or acceptable explanation.

Financial Services Providers also need to be aware that its employees could be targeted by money launderers and therefore should be aware of:

- changes in employee characteristics, (eg: lavish life styles or avoiding taking holidays), and
- changes in employee or agent performance, (eg: a dealer has remarkable or unexpected increase in performance).

21. How might identification of existing clients be carried out?

As indicated in the Guidance Notes, sections 3.106-3.113, *Financial Services Providers* should conduct a risk assessment. Those clients assessed as high risk should be actioned first. The *Financial Services Provider* should ensure the information on file identifies the party and enables the bank to effectively monitor the account.

MONEY SERVICES BUSINESS

1. Section 2 of the Money Services Law defines "money services business" (MSB) as
   (a) the business of providing (as a principal business) any or all of the following services -
      (i.) money transmission;
      (ii.) cheque cashing;
      (iii.) currency exchange;
      (iv.) the issuance, sale or redemption of money orders or traveller's cheques; and
      (v.) such other services as the Governor in Council may specify by notice published in the Gazette; or
   (b) the business of operating as an agent or franchise holder of a business mentioned in paragraph (a).

SCOPE OF MONEY LAUNDERING REGULATIONS AND PURPOSE OF THIS SECTOR SPECIFIC GUIDANCE

2. This sector specific guidance seeks to provide practical assistance to MSBs in complying with the Regulations, interpreting and applying the general provisions of these Guidance Notes, and for MSBs to adopt sound risk management and internal controls for their operations.

3. The Money Laundering Regulations (MLRs) apply to MSBs as indicated in the list of activities falling within the definition of "Relevant Financial Business" in the Second Schedule of the MLRs.

4. It is the responsibility of each MSB to have systems and training in place to prevent money laundering. This means that each MSB must maintain identification procedures, record-keeping procedures, and such other procedures and controls and communications appropriate for the purposes of forestalling and preventing money laundering.

Vulnerability of MSBs to Money Laundering & Terrorist Financing

5. The fleeting relationship with its customers makes MSBs vulnerable to money laundering and the financing of terrorism. Whereas a person would typically have to be a customer with an account at a bank, for example, to be able to access the services of that bank, a person does not have that type of relationship with the MSB and can repeatedly use different MSBs to transact business. The money transmission part of the MSB is particularly vulnerable, given the high volume of cash handled on a daily basis and the ability to transmit funds instantly to any part of the globe.

6. While the international remittance system is typically used by expatriate workers to send a part of their earnings back home, it can also be used to transmit the illegal proceeds of criminal activities and the financing of terrorism. The rapid movement of funds across

multiple jurisdictions presents a challenge to investigators, particularly if the identity of the originator is unclear. For this reason, international standards have been developed with respect to payer information that should accompany wire transfers to mitigate the above-mentioned risk.

7. Apart from money transmission, cheque cashing is another important segment of the business for some MSBs. MSBs should be aware that endorsed third party cheques from overseas are a money laundering risk. Even where a CI cheque, endorsed by a third party, is presented to the MSB for cashing, the MSB should take appropriate steps to ascertain the economic purpose behind the endorsement to that person presenting the cheque. Large cheques originating from unknown individuals present a greater money laundering risk compared to small cheques originating from well-established businesses.

ASSESSMENT OF RISK

8. MSBs should adopt a risk-based approach to managing money laundering and terrorist financing risks. In so doing, MSBs should develop a profile of its customers, thereby familiarising themselves to clients' personal or business needs for the services provided. The MSB's risk assessment should take into consideration the factors such as

   - types of products and services offered;
   - its customer types (customer occupation or type of business operated);
   - geographical location of clients or where funds are transmitted; and
   - average cash value of typical transactions and the $15,000 customer identification threshold as per the Money Laundering Regulations (MLRs).

9. As much as possible, MSBs should use computer technology to conduct the risk assessment. Customers, products and services should be ranked as "high," "medium," or "low" risk. The transfer of a part of an expatriate worker's weekly wage to his family in his home country should be less risky compared to the transmission of a large sum by a visitor to numerous recipients. Higher risk customers, products and services should be subject to enhanced customer due diligence checks and transaction monitoring. The risk model should be documented, with its rationale clearly stated, and should be updated on a regular basis to keep in line with changes in the business or the threats.

ESTABLISHMENT OF CUSTOMER RELATIONSHIPS

10. Sound customer identification and verification polices and procedures are effective weapons against money laundering. Requiring appropriate identification, verifying the information in certain cases, and being alert to unusual or suspicious transactions can help an MSB deter and detect money laundering and terrorist financing schemes.

11. A customer identification and verification policy tailored to the operations of a particular business:

- helps detect suspicious activity in a timely manner;
- promotes compliance with the relevant laws, regulations and guidance;
- promotes safe and sound business practices;
- minimises the risk that the MSB will be used for illegal activities;
- reduces the risk of government seizure and forfeiture of funds associated with customer transactions (such as out standing money orders/traveller's cheques and outstanding money transfers) when the customer is involved in criminal activity; and
- protects the reputation of the MSB.

12. Whose identity must be verified?

The applicant for businesses may be an individual, a corporate client, a partnership or unincorporated business.

Reasonable measures should be taken to distinguish between someone who is acting on his own behalf and someone who is acting on behalf of another. If it is determined that the person is acting on behalf of another, then the procedures for verifying the identity of the ultimate applicant for business apply. Customers may fall within the following categories:

Example	Applicant for Business	Requirements
1.	Direct Personal Client	• Beneficial owner of funds • Third Party sending funds Satisfactory evidence, confirmed by using one or more of the verification methods: o Current valid passport; o Armed Forces ID card; o Any uniquely numbered government-issued ID card showing the photograph of the applicant, such as a driver's licence or a voter's registration card; and o A Cayman Islands employer ID card bearing the photograph and signature of the applicant.
2.	Corporate Client	• The company (evidence that it exists) • Consistent with that required for direct personal clients, documentary evidence of identity for all directors; all those with signing powers, including

		third parties; and beneficial owners. (See section 3.31, 3.35 and 3.39-3.41 in the Guidance Notes) • Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required for direct personal relationships Satisfactory evidence, confirmed by at least one of the following independent checks, of company's existence: o Memorandum and Articles of Association and Certificate of Incorporation o Information about the identity of controlling shareholders and directors, e.g., Register of Directors, Register of Members o Understanding of all relevant party and inter-company relationships o It may be appropriate to obtain information relating to customers or suppliers and the background of major shareholders and directors
3.	Partnerships / Unincorporated Businesses	• The entity, evidence that it exists • Consistent with that required for direct personal clients, documentary evidence of identity required for partners/managers; all those with signing powers, including third parties; and beneficial owners as defined in the Guidance Notes, Section 3.31 • Documentary evidence of identity of the new owner/controller where there is a change in ownership or control, in accordance with that required of direct personal relationships Satisfactory evidence, confirmed by at least one of the following independent checks, of existence of partnership / unincorporated business: o Partnership agreement or excerpt if relevant o Certificate of Registration o Information about the identity of controlling partners / shareholders, e.g., excerpt from partnership document o Establish all relevant party relationships

13. For which customers must MSBs obtain identification documentation?

Section 7 of the MLRs stipulates the cases where identification documentation is to be obtained:

- Any case where the parties form a business relationship between them;
- Any case where it is known or suspected the customer is engaged in money laundering;
- Any case in respect of a one off transaction where payment is equal to or exceeds CI$15,000, or;
- Any case where, in respect of two or more one-off transactions, it appears at the outset or at a later stage, that the transactions are linked and the total amount, in respect to all of the transactions is CI$15,000 or more.

Notwithstanding the above, proper identification documentation is required for **all** money transmissions, which is one of the major services offered by MSBs. The requirement for specific pieces of payer information that are to accompany each wire transfer applies to money transmissions. MSBs must therefore request and obtain identification documentation for money transmissions, in line with the payer information requirements in 23 below (***Wire Transfers***). The fact that the vast majority of remitters are from the expatriate community means that this should not result in unnecessary hardship on their part, for providing appropriate identification at the beginning of the relationship.

For other services other than money transmissions, it would be ***prudent best practice*** to have more diligent thresholds than the $15,000 required under Section 7 of the MLRs. The threshold should be derived from the risk assessment, bearing in mind what 1) the amount that the average customer and would transact and 2) the reporting threshold of US$3,500 on the quarterly MSB form reported to the Authority.

Given the fleeting nature of the customer relationship, MSBs should obtain identification information where the customer, product or geography is deemed to be high risk in the risk assessment.

14. When must identification documentation be obtained?

Customer identification information should be obtained **prior** to a transaction being carried out. If identification information is not obtained, the transaction should not proceed.

15. What should be done if there are doubts as to the identity of an existing customer?

If in the process of reviewing identification documentation, the MSB has doubts about the veracity or adequacy of previously obtained customer identification data, then the MSB should take reasonable steps to verify the data. Depending on the money laundering risk of the customer, the MSB could either wait for the customer to transact business again if he is a regular customer, or it can contact the individual by phone requesting that he submit the relevant documentation. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering or terrorist financing in relation to that customer, or where the customer's pattern of transactions changes from what is deemed to be "normal" for that customer.

16. What information should be obtained in relation to expected amount of transactions and source of funds for "regular customers"[3]?

Refer to the Guidance Notes, "Direct Personal Clients", Paragraphs 3.9 – 3.13.

17. What is considered to be an appropriate description of "source of funds"?

The appropriate description of a customer's "source of funds" would be as follows:

- Salary
- Sale of property including documentation evidencing the sale
- Loan proceeds including documentation evidencing the grant of the loan

The following on their own would not be considered appropriate descriptions of the ultimate "source of funds":

- Partner
- Savings

Partner and savings are considered immediate sources of funds, for which the proof of the either salary, dividends, sale proceeds, or loan (ultimate sources) should be provided. In the case of ***Partners***[4], additional enquiries such as confirmation from the treasurer would be an appropriate requirement, while in the case of ***Savings***, a bank statement should be provided.

18. Why is it important to establish the purpose of the transaction?

It is important to establish the purpose for those transactions that are large, complex or unusual (see further details on complex and unusual transactions at 20). The threshold for large transactions should be determined from the MSB's risk assessment, but

[3] Regular Customer for the purpose of this Guidance would be one who has established a pattern of conducting transactions whether it be on a daily basis, weekly basis, monthly basis, quarterly basis, semi-annual basis, or annual basis. Any transaction conducted by the same customer less often than once per year would fall into the "one-off transaction" category for the purpose of this Guidance.

[4] Partners is an informal saving and credit scheme in the Caribbean in which a group of people regularly deposit a fixed amount of money with a main organiser, the 'banker', into a central fund. The banker distributes the total sum (the 'hand') to members in a pre-arranged order. This system of credit operates almost completely on trust, in that each person who collects his/her lump sum must be trusted to continue paying in the contributions until all members have collected their 'hand.' This scheme operates usually with no written agreement.

certainly transactions over $15,000 should fall in that category. In the same way a bank would ask its customer about the purpose for which an account is being established, an MSB should ask the customer about the purpose of the transaction that is beyond the MSB's threshold. In that way, the MSB is able to establish if the purpose is lawful and whether the transaction will be a one-off event or part or a regular occurrence. Asking about the purpose of the transaction helps the MSB to develop a profile of "normal" activity for that customer. If the MSB is unable to establish what "normal" activity is, then it is hard to separate the unusual activities for further analysis to determine which ones are suspicious.

TRANSACTION MONITORING

19. How should the business of a customer be monitored?

Because of the large number of customers involved and the relative small amounts transacted, it is imperative for MSBs to have adequate systems in place to collate relevant information and monitor customers' activities. In the money services business, the amount of information collected may be broadened to include details of the recipient of the funds. This information will assist MSBs to determine whether there is any risk that the customer is utilising multiple recipients to facilitate money laundering or whether multiple customers are remitting multiple small sums that are accumulated with one recipient.

20. What to do about complex and unusual transactions?

Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction must be considered *unusual*, and the staff member put "on enquiry". Complex transactions or structures may have entirely legitimate purposes. However, the MSB should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should as far as possible be examined and documented by the MSB.

An example of an unusual pattern of transactions would be where an MSB's database reveals that several seemingly unrelated individuals are remitting small amounts of money to one individual abroad. In that case, the MSB may conduct an Internet search to find out more about the recipient before making further enquiries with one or two of the senders.

Where enquires and/or research establish that there is a logical and lawful explanation to an unusual transaction or pattern of transactions, then the MSB may conclude that there is no need for further action. But if the enquiry and/or research lead to suspicion, then the MSB must file a SAR with the FRA. In either case it is important to document the

entire process of moving from "complex/unusual" to "suspicious/not suspicious" to "File SAR/No need to file SAR."

21. What specific records should be kept and where?

The MSB must keep adequate records of the identity of its clients and all transactions conducted by that client for a period of 5 years following the last transaction, the closing of an account, or the termination of the business relationship.

Refer to the Guidance Notes, "Record Keeping Procedures", Paragraphs 7.1 – 7.8 for further information.

22. What warning signs or "red flags" should service providers be alert to?

- Deposit of cheques or funds transferred to/from high-risk jurisdictions or from different jurisdictions than expected or typically seen in the account;
- Unusually large or frequent deposits or fund transfers;
- Use of multiple transactions and multiple recipients, including structuring of transactions to avoid identification threshold of $15,000 or whatever enhanced due diligence threshold that the MSB may have;
- Multiple customers remitting multiple small sums to one recipient where the aggregate amount exceeds the reporting threshold requirements;
- A single customer remitting to several persons overseas where the aggregate sum exceeds reporting thresholds;
- Multiple large remittances over a short period of time, executed by the same sender or for the benefit of the same recipient;
- A customer or group of customers attempting to hide the size of a large cash transaction
    - at different times on the same day;
    - with different MSB cashiers on the same day or different days;
    - at different branches/offices of the same MSB;
- Large volumes of cash received or remitted to one or more recipients over a period of time;
- A customer purchases money transfers, money orders, traveller's cheques, etc, with large amounts of cash
- Business customer reluctant to provide complete information regarding the type of business, the purpose of the transaction, or any other information requested by the MSB; and
- Lack of adequate client identification or source of funds being provided.

Refer to Appendix K of the Guidance Notes noting that not all examples given in this appendix will be applicable to MSBs.

WIRE TRANSFERS

23. What information should accompany the transfer of funds?

The MLRs require complete information on the payer to accompany the transfer of funds. Complete information on the payer consists of

1. his name; and
2. his account number (where one exists) or a unique identifier; and
3. either his address or his date and place of birth or his customer identification number or the number of a Government-issued document evidencing his identity.

For further guidance, see paragraphs 4.14 to 4.47 of the GN.

FILING A SAR

24. When should a SAR be filed?

Refer to Guidance Notes, "Role of Staff Members", Paragraphs 5.22 – 5.23, "The Role of the MLRO", Paragraphs 5.24 – 5.28, and "Reporting Suspicions to the Reporting Authority", Paragraphs 5.29 – 5.37.

It is important to note that SARs must be filed with the Financial Reporting Authority (FRA) on a suspicious transaction even if the transaction did not proceed.

TRAINING

25. What staff members should receive training in AML?

Staff should be educated in the "Know Your Customer" requirements for the prevention of money laundering and terrorist financing. Training should therefore cover not only the need to know the customer's true identity, but also, where a business relationship is being established, the need to know enough about the type of business activity expected in relation to the customer at outset (and on an ongoing basis) so that "normal" activity can be distinguished from suspicious activity in the future, at it relates to that person.

Although Executive Directors and Senior Managers may not be involved in the day-to-day procedures for handling transactions that may relate to money laundering and terrorist financing, it is important that they understand the statutory duties placed on them, their staff and the firm itself given that these individuals are involved in signing off procedures.

Supervisors and managers should receive a higher level of training covering all aspects of money laundering procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, the procedures relating to dealing with production and restraint orders and the requirements for verification of identity and retention of records.

MLROs and Deputy MLROs should receive in-depth training on all aspects of the primary legislation, the Regulations and internal policies. They should also develop and maintain up-to-date knowledge on the development and/or implementation of AML policies and procedures, including AML risk assessment, transaction monitoring, investigation of complex and unusual activates, reporting of suspicious activities, staff AML training, and staff screening. They should also keep up-to-date with new trends of criminal activity.

For further details, refer to the Guidance Notes, "Training and Awareness", Section 6.

INDEPENDENT AUDIT FUNCTION

26. Does the MSB need an internal audit function?

MSBs should have procedures of internal control including an appropriate internal audit function for the prevention of money laundering and terrorist financing. The internal audit function serves to test the MSB's system of internal control and should be appropriate to the MSB's size and to the nature of its operations. Testing should be risk-based, with particular emphasis on high-risk operations. It should be independent, conducted periodically, and reported directly to the Board. The audit report should include, but not be limited to, the following:

- review of high risk accounts, transactions, and customers;
- one-off transactions in excess of $15,000 and suspicious activity reporting;
- money remittance and check cashing transactions are in accordance with the relevant laws, regulations and guidance;
- adequacy of customer identification information and customer due diligence; and
- complex and unusual transactions.

DOCUMENTATION

27. What policies and procedures should be documented?

MSBs should document its AML policies and procedures. At the very least, MSBs should have documented policies and procedures on:

- the assessment of risks;
- customer identification;
- transaction monitoring, including complex and unusual transactions;
- suspicious activity reporting; and
- staff training.

REAL ESTATE

1. Who is the applicant for business?

The applicant for business may be one of the following:

Example	Applicant for business
1.	Purchaser - Personal – better known as the "customer" in real estate terms, this is the ultimate individual who would submit offers to purchase property
2.	Vendor - Personal – better known as the "client" in real estate terms, this is the ultimate individual who is listing their property
3.	Purchaser – Corporate – better known as the "customer" in real estate terms, this is the ultimate corporation who would submit offers to purchase property
4.	Vendor - Corporate – better known as the "client" in real estate terms, this is the ultimate corporation that is listing its property

2. Whose identity MUST be verified?

Applicant for business	Evidence of identification required for
1. Purchaser - Personal	• That the person is the contracting party and proposed registered title-holder of the property • Source of funds for the purchase of the property • Satisfactory evidence, confirmed by using one or more of the verification methods outlined in section 3.19 of the Guidance notes.
2. Vendor - Personal	• That the person is the contracting party and current registered title-holder of the property
3. Purchaser - Corporate	• That the corporation is the contracting party and proposed registered title-holder of the property • Source of funds for the purchase of the property • The company, that it exists

	• Documentary evidence of all directors and all those with signing powers including third parties and beneficial owners (See Section 3.31, 3.35 and 3.39-3.41 in the GN) • Satisfactory evidence, confirmed by at least one of the following independent checks of company's existence: 1. Memorandum of association and articles and certificate of incorporation 2. Information about the identity of controlling shareholders and directors e.g. Register of Directors, Register of Members 3. It may be appropriate to obtain information relating to customers and suppliers and the background of major shareholders and directors. • Normally no need to repeat due diligence on corporate clients/customers if the same beneficial owner each time.
4. Vendor - Corporate	• That the corporation is the contracting party and current registered title-holder of the property • The company, that it exists • Documentary evidence of all directors and all those with signing powers including third parties and beneficial owners •

3. When must identity be verified?

The real estate industry has a history of being utilized by money launderers and fraudsters to place criminal proceeds in the financial system, conceal the original source of funds and legitimise such funds. As such, persons involved in financial, estate agency and legal services provided in the course of business relating to the sale, purchase or mortgage of land or interests in land on behalf of clients or customers must be alert to such risks. Collecting evidence of identification and the source of funds assists those providing relevant financial business in ensuring the prospective customer is who he/she claims to be and that the nature of the business that the customer expects to undertake is legitimate.

It is recognized that real estate agents and brokers' involvement in the sale and purchase of land or property may extend from being significant (direct contact with the customer and the funds are transacted in their escrow account) to relatively peripheral (collection of commission on the sale), to nominal (real estate listing). The risk to the real estate agents or brokers will differ

depending on the extent to which they are involved, in that the more they are involved with the customer and/or in handling the funds, the more risk they will assume. Therefore the amount of evidence the real estate agents or brokers collect should be correlated to the risks.

Real estate agents and brokers who are directly involved with the prospective customers or whose escrow account is being utilized to transfer funds from the purchaser to the vendor should perform full verification in accordance with the Guidance Notes. As the risk of money laundering arises primarily from the purchase of a property, the principal focus of real estate agents and brokers' due diligence efforts should be directed to the identification of the purchaser and the source of funds.

To the extent that the funds being transacted through the escrow account are payments to and from an account in the name of the purchaser and vendor in a regulated bank in the Cayman Islands or a Schedule 3 country, or the purchaser or vendor are managed or registered with an entity regulated in the Cayman Islands (which can be verified on www.cimoney.com.ky), it may be unnecessary to take any further steps to verify client identity.

It may be reasonable for example, to take no further steps to verify identity when payment is made by cheque or electronically and sent either by mail or electronically from an account (or joint account) in the purchaser's/vendor's name at a bank in the Cayman Islands or a Schedule 3 country if it does not fall within the following categories:

a) the circumstances of the payment are such that a person handling the transaction knows or suspects that the applicant for business is engaged in money laundering, or that the transaction is carried out on behalf of another person engaged in money laundering; or

b) the payment is made for the purpose of opening a relevant account with a bank in the Cayman Islands.

If the payment does fall into one of the above categories then the evidence of identity of the applicant must be obtained in accordance with the full identification procedures as outlined in the Guidance Notes.

Similarly, it may be reasonable for example, to take no further steps to verify identity, when the purchaser or vendor is a corporate entity managed or registered with an entity regulated in the Cayman Islands unless the person handling the transaction knows or suspects that the applicant for business is engaged in money laundering, or that the transaction is carried out on behalf of another person engaged in money laundering.

If the purchaser or vendor is a corporate entity that is not managed by or registered with an entity regulated in the Cayman Islands or the person handling the transaction knows or suspects the purchaser or vendor is involved in money laundering, then the evidence of identity of the

applicant must be obtained in accordance with the full identification procedures as outlined in the Guidance Notes.

Real estate agents and brokers who are only peripherally or nominally involved should only collect information as to the names of the parties involved in the transactions, and/or those who acted on their behalf. This will assist the Reporting Authority if it should wish to perform an investigation of the transactions.

4. What documentary evidence of source of funds is required?

In those circumstances identified in paragraph 3 where verification of identity may not be necessary, it may also not be necessary to obtain documentary evidence of source of funds, as long as the criteria in paragraph 3 are met. In other circumstance, however, then the documentary evidence of source of funds must be obtained.

The extent to which such documentary evidence is required or the information is verified with an outside source will depend upon (a) the risk associated with the response and (b) how easy the source is to verify. Below is a table which attempts to give some examples of considerations when a response if received:

	Source of Funds	Considerations
1.	Savings/ Employment Income	• Price of property consistent with expectations of income earner; • Age of the income earner
2.	Business Income	• Type of business and expectations of earnings; • Details of the business (name, address, website, and whether it has public earnings information)
3.	Sale of Business	• Public information (eg. News clippings) or other evidence of sale
4.	Inheritance	• Evidence of death; • Original source of funds of the deceased
5.	Sale of investments or property	• Information of original source (income, business) is required and considered as above

5. When might it be possible to rely on third parties to verify identity?

In addition to those circumstances identified in paragraph 3 where verification of client identity may not be necessary, it may be appropriate for real estate agents and brokers to rely upon the

due diligence procedures performed by others who conducted client verification procedures substantially in accordance with the Guidance Notes. Those situations are identified under section 3.66 –3.89 of the Guidance Notes. Realtors should use their judgement in determining whether or not in the context of real estate they should place reliance on the due diligence procedures for intermediaries. In cases where the reliance is placed on the intermediary, senior management must make a judgement as to whether or not it would be prudent to obtain appropriate evidence of client verification. In most cases it may be more appropriate to seek a confidentiality waiver from the client/customer in order that the documentation held by third parties on the customer/ client may be copied and retained by the realtor.

In addition to the scenarios envisaged in sections 3.66-3.89 of the Guidance Notes on introduced business, it is also common in real estate business for co-agency relationships to arise. When the prospective client is introduced by one CIREBA member to another, it is not necessary for identity to be re-verified or for the records to be duplicated provided that the identity of the client has been verified by the introducing member of CIREBA in a manner compatible with the Regulations and provided that written confirmation is obtained that the identification will on request be provided. CIREBA members relying on another CIREBA member's introduction must be satisfied that the *CIREBA Rules and Regulations* are absolutely adhered to and is at least as high a standard as detailed in these Guidance Notes.

In all cases where reliance is being placed on an eligible introducer, other than a CIREBA member, for documentary evidence of client identification of a purchaser (personal or corporate), information regarding source of funds would still need to be obtained.

6. How should a realtor deal with relationships prior to enactment of the regulations?

Given the nature of real estate transactions, the length of time of the relationship between the realtor and the customer or client as it pertains to any one property is relatively short, and usually does not last over a year, before the listing is renewed or continued. As such, it is not expected that Section 3.103 to 3.113 will pertain to real estate agents and brokers.

7. How should the business of the client be monitored?

Given the nature of real estate transactions, it is uncommon that a customer or client will have more than one transaction, i.e. the purchase or sale of a property. Two exceptions exist:

(a) Local developers or investors who are involved in more than one property. In this case the realtors should refer to the Guidance Notes "*On-Going Monitoring of Business Relationships*" Sections 4.1-4.8; and,

(b) The original purchaser of a property uses the realtor to subsequently sell the same property. In this case, it is not necessary for the realtor to obtain documentary evidence of customer identity again, however, the realtor should ensure that the proceeds

are being remitted to an account that is consistent with the understanding and expectation of the client.

8. What warning signs or 'red flags' should service providers be alert to?

Real estate agents and brokers should be alert to transactions that fall outside the standard industry practice, which may include but are not limited to the following:

- Customer wishing to purchase property with cash or bearer instruments;
- Client seeks proceeds of sale to be remitted to a third party other than the current owner or to an account other than where the client resides;
- Customer is not concerned with losing deposit when he has a right to recover it; and,
- Any irregularity in the ownership structure or the activities surrounding a transaction may require further or broader investigation.

9. Who should be appointed MLRO?

Since most real estate companies are relatively small, it is appropriate for such organizations to have the broker also be the MLRO.

10. What specific records should be kept and where?

Refer to the Guidance Notes, sections 7.1-7.8.

SECTION 9 -APPENDICES

Appendix A - Background Information on Money Laundering

What is money laundering?

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If they are successful, it also allows them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of income.

Money laundering is a global phenomenon that affects all countries to varying degrees. By its very nature it is a hidden activity, and therefore the scale of the problem and the amount of criminal money being generated either locally or globally each year is impossible to measure accurately. Failure to prevent the laundering of the proceeds of crime allows criminals to benefit from their actions, making crime a more attractive proposition.

The need to combat money laundering

In recent years there has been a growing recognition that it is essential to the fight against crime that criminals be prevented, wherever possible, from legitimising the proceeds of their criminal activities by converting funds from "dirty" to "clean".

The laundering of the proceeds of criminal activity through the financial system is vital to the success of criminal operations. Those involved must exploit the facilities of the world's Financial Institutions if they are to benefit from the proceeds of their activities. The increased integration of the world's financial systems, and the removal of barriers to the free movement of capital, have meant it is potentially easier for criminals to launder dirty money, and more complicated for the relevant authorities to trace. The long-term success of any of the world's financial sectors depends on attracting and retaining legitimately earned funds. The unchecked use of the financial system for laundering money has the potential to undermine individual Financial Institutions, and ultimately the entire financial sector.

Money laundering in various forms has existed since time immemorial. The effect of legislation is to criminalise the activity and create a number of specific offences. It is inevitable that in all countries, some existing customers, including those of long-standing, are already engaged in money laundering.

Although these Guidance Notes focus upon new business relationships and transactions, Financial Institutions should also be alert to the financial flows and transaction patterns of existing customers, particularly where there is a significant and unexplained change in the behaviour of the account. (See Appendix K, Examples of Suspicious Activities).

The Money Laundering Regulations, requires Financial Institutions to establish systems to detect money laundering, and therefore assist in the prevention of abuse of their financial products and services. This is also in Financial Institutions' own commercial interest, and it also protects the reputation of the Cayman Islands.

Because of the international nature and both market and geographical spread of business on the Cayman Islands, local institutions which are less than vigilant may be vulnerable to abuse by money launderers, particularly in the 'layering' and 'integration' stages (see below). Banks, Building Societies, Investment Business and Money Service Providers which, albeit unwittingly, become involved in money laundering risk prosecution and substantial costs both in management time and money, as well as face the severe consequences of loss of reputation.

The stages of money laundering

There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a car, or jewellery), to passing money through a complex international web of legitimate businesses or 'shell' companies. Initially, however, in the case of drug trafficking and some other serious crimes such as robbery, the proceeds usually take the form of cash which needs to enter the financial system by some means. Street purchases of drugs are almost always made with cash.

Despite the variety of methods employed, the laundering process is accomplished in three stages. These may include numerous transactions by the launderers that could alert a *Financial Service* to criminal activity:-

a) Placement - the physical disposal of cash proceeds derived from criminal activity.

b) Layering - separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

c) Integration - the provision of apparent legitimacy to wealth derived from crime. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic steps may or may not occur as separate and distinct phases. They may occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organisations. The table below provides some typical examples.

The stages of money laundering

Placement Stage	**Layering stage**	**Integration Stage**
Cash paid into bank* (Sometimes with staff complicity or mixed with proceeds of legitimate business)	Wiring transfer abroad(often using shell companies or funds disguised as proceeds of legitimate business)	False loan repayments forged invoices used cover for laundered money.
Cash exported	Cash deposited in overseas banking system	Complex web of domestic and international) makes tracing source of funds virtually impossible
Cash used to buy high value items	Resale of goods or assets	Income from property or legitimate business assets appears 'clean'

'bank' includes all deposit-taking institutions, those which exchange or remit cash, and the client accounts of professional intermediaries, such as accountants, regulators and trustees.

Certain points of vulnerability have been identified in the laundering process which the money launderer finds difficult to avoid, and where his activities are therefore more susceptible to being recognised, such as:-

- entry of cash into the financial system;
- cross-border flows of cash;
- acquisition of financial assets;

- transfers within and from the financial system;
- incorporation of companies; and
- establishment of financial vehicles (e.g. ostensible pooled investment funds, merchanting and barter companies).

Appendix B – Background to the Guidance Notes

Basle Statement of Principles

In December 1988 the Basle Committee on Banking Regulation and Supervisory Practices ("the Basle Committee") issued a Statement of Principles. This Statement was endorsed by Cayman Islands Monetary Authority and circulated to all banking institutions licensed by it at the time. The statement set out the following basic principles:-

Customer Identification - when establishing a relationship by opening an account or providing any other service, including safe custody and safe deposit box facilities, reasonable efforts should be made to determine the true identity of the customer requesting the service;

Compliance with Legislation and Regulation Enforcement Agencies - business should be conducted in conformity with high ethical standards and local regulations and regulations pertaining to financial transactions. Institutions should cooperate fully with national regulation enforcement authorities to the extent permitted without breaching customer confidentiality; and

Record Keeping and Systems - institutions should implement specific procedures for retaining internal records of transactions and establish an effective means of testing for general compliance with the Statement.

The Financial Action Task Force ("FATF")

In June 1989 the Heads of Government of the Group of Seven ("G7") countries established the Financial Action Task Force, commonly referred to as "FATF".

FATF Member countries have thus been introducing legislation to combat money laundering. Such legislation generally includes equivalent offences and compliance obligations for companies established and operating within the Member countries and, as such, seeks to create consistent regulations and prevention practices. This international initiative will therefore create similar obligations for all companies operating within the international financial

market place and thereby reduce the likelihood of discriminatory practices between Members, and between Members and non-Members.

The Caribbean Financial Action Task Force ("CFATF")

In June 1990 15 Caribbean states plus five members of the Financial Action Task Force with affiliations in the region met in conference in Aruba and produced 21 recommendations, 19 of which were eventually adopted as CFATF recommendations. In June 1992 a second regional meeting addressed the areas of legal, financial, political and technical assistance in combating money laundering. It provided detailed recommendations, which were presented at a ministerial meeting convened in Kingston, Jamaica in November 1992. 20 Caribbean states plus the FATF affiliates participated. An accord was agreed embodied in the Kingston Declaration on money laundering endorsing the implementation of the 1988 United Nations Vienna Convention, the Organisation of American States Model Regulations, the 40 FATF Recommendations and the 19 Regional Specific Objectives.

In October 1996 21 countries signed a Memorandum of Understanding and a Mission Statement formulating its mission, organisation and membership requirements.

The CFATF also has a rolling programme of mutual evaluations.

The EU Money Laundering Directive

As part of this initiative, the UK and other countries of the European Union are implementing a Council Directive on the prevention of the use of the financial system for the purposes of money laundering (No 91/308/EEC).

Appendix C – The Money Laundering Regulations

Note that this appendix provides the provision of the Regulations but not in the gazetted format, as at the date of issue and persons should check the current Regulations to ensure that the specific provisions are not outdated.

Supplement No. 3 published with Gazette No. 15 of2lst July, 2008.

PROCEEDS OF CRIMINAL CONDUCT LAW

(2007 Revision)

MONEY LAUNDERING REGULATIONS

(2008 Revision)

Revised under the authority of the Law Revision Law (1999 Revision).

The Money Laundering Regulations, 2000 made the 2nd April, 2000,
consolidated with the -

Money Laundering (Amendment) (Client Identification) Regulations, 2001 made the 26th April, 2001
Money Laundering (Amendment) (Electronic Payments) Regulations, 2001 made the 24th May, 2001
Money Laundering (Amendment) Regulations, 2001 made the 2nd October, 2001
Money Laundering (Amendment) Regulations, 2002 made the 30th April, 2002
Money Laundering (Amendment) (No.2) Regulations, 2002 made the 17th December, 2002
Money Laundering (Amendment) Regulations, 2003 made the 17th June, 2003
Money Laundering (Amendment) Regulations, 2004 made the 1st September, 2004
Money Laundering (Amendment) Regulations, 2005 made the 25th October, 2005
Money Laundering (Amendment) Regulations, 2007 made the 1st June, 2007
Money Laundering (Amendment) (No. 2) Regulations, 2007 made the 7th August, 2007,

and as amended by the -
Cayman Islands (Constitution) (Amendment) Order 2003 (U.K.S.I. 2003 No. *1515)* made the 12th day of June, 2003.
Consolidated and revised this 13th day of May, 2008.

Note (not forming part of the Regulations): This revision replaces the 2006 Revision which should now be discarded.

MONEY LAUNDERING REGULATIONS

(2008 Revision)

ARRANGEMENT OF REGULATIONS

PART I - Introductory

MONEY LAUNDERING REGULATIONS

(2008 Revision)

PART I - Introductory

I. These regulations may be cited as the Money Laundering Regulations (2008 Revision).

2. (1) In these regulations-

"applicant for business" means a person seeking to form a business relationship, or carry out a one-off transaction, with a person who is carrying out relevant financial business in the Islands;

"Authority" means the Cayman Islands Monetary Authority;

"batch file transfer" means several individual transfers of funds which are bundled together for transmission;

"business relationship" has the meaning given by regulation 3;

"Case 1", "Case 2", "Case 3" and "Case 4" have the meanings given in regulation 7;

"insurance business" means business of any of the classes of business specified in the First Schedule;

"intermediary payment service provider" means a payment service provider, neither of the payer nor of the payee, that participates in the execution of transfers of funds;

"money laundering" means doing any act which constitutes an offence under section 47 or 48 of the Misuse of Drugs Law (2000 Revision), sections 19 to 22 of the Terrorism Law, 2003 or sections 32 to 34 of the Law or, in the case of an act done otherwise than in the Islands, would constitute such an offence if done in the Islands;"

"one-off transaction" means any transaction other than a transaction carried out in the course of an established business relationship formed by a person acting in the course of relevant financial business;

"payee" means a person who is the intended final recipient of transferred funds; "payer" means either a person who holds an account and allows a transfer of funds from that account, or, where there is no account, a natural or legal person who places an order for a transfer of funds;

"payment service provider" means a person whose business includes the provision of transfer of funds services;

"relevant financial business" has the meaning given by regulation 4;

"terrorist financing" means doing any act which constitutes an offence under sections 19 to 22 of the Terrorism Law, 2003 or, in the case of an act done otherwise than in the Islands, would constitute such an offence if done in the Islands;

"transfer of funds" means any transaction carried out on behalf of a payer through a payment service provider by electronic means, with a view to making funds available to a payee at a payment service provider, irrespective of whether the payer and the payee are the same person; and

"unique identifier" means a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used to effect the transfer of funds.

(2) For the purposes of Part VII, complete information on a payer shall consist of-

(a) his name;
(b) (i) his address; or
(ii) his date and place of birth;
(iii) his customer identification number; or
(iv) the number of a Government-issued document evidencing his identity; and

(c) his account number or a unique identifier which allows the transaction to be traced back to the payer.

(3) The reference, in the definition of "money laundering", to doing any act which would constitute an offence under the Law shall, for the purposes of these regulations, be construed as a reference to doing any act which would constitute an offence under the Law if, for the definition of "criminal conduct" in section 22(10) of the Law, there were substituted -

"(10) In this Law "criminal conduct" means -

(a) conduct which constitutes an offence to which this Law applies; or

(b) conduct which

(i) would constitute such an offence if it had occurred in the Islands; and

(ii) contravenes the law of the country in which it occurred.".

(3) For the purposes of this regulation, a business relationship formed by a person acting in the course of relevant financial business is an established business relationship where that person has obtained, under procedures maintained by him in accordance with regulation 7, satisfactory evidence of the identity of the person who, in relation to the formation of that business relationship, was the applicant for business.

3. (1) Any reference in this regulation to an arrangement between two or more persons is a reference to an arrangement in which at least one person is
acting in the course of a business.

(2) For the purposes of these regulations-

"business relationship" means any arrangement between two or more persons where -

(a) the purpose of the arrangement is to facilitate the carrying out of transactions between the persons concerned on a frequent,
habitual or regular basis; and

(b) the total amount of any payment or payments to be made by any person to any other in the course of that arrangement is not known or capable of being ascertained at the time the arrangement is made.

4. (1) For the purposes of these regulations-

"relevant financial business", subject to subregulation (2), means the business of engaging in one or more of the following -

(a) banking or trust business carried on by a person who is for the time being a licensee under the Banks and Trust Companies Law (2007 Revision);

(b) acceptance by a building society of deposits made by any person (including the raising of money from members of the society by the issue of shares);

(c) business carried on by a co-operative society within the meaningof the Co- operative Societies Law (2001 Revision);

(d) insurance business and the business of an insurance manager an insurance agent, an insurance sub-agent or an insurance broker within the meaning of the Insurance Law (2008 Revision);

(e) mutual fund administration or the business of a regulated mutual fund within the meaning of the Mutual Funds Law (2007 Revision);

(f) the business of company management as defined by the Companies Management Law (2003 Revision), except that the services specified in section 3(4)(a) of that law shall not be excluded for the purposes of these regulations from the provision of the specified services as defined in subsection (2) of that section; and

(g) any of the activities set out in the Second Schedule, other than an activity falling within paragraphs (a) to (f) of this subregulation.

(2) In this regulation -

"banking business" has the same meaning as in the Banks and Trust Companies Law 2007 Revision); and

"building society" means a society incorporated under section 3 of the Building Societies Law (2001 Revision).

PART II - Systems and Training to Prevent Money Laundering

5. (1) A person shall not, in the course of relevant financial business carried on by him in or from the Islands, form a business relationship, or carry out a one-

off transaction, with or for another unless he -

(a) maintains the following procedures established in relation to that business -
  (i) identification procedures in accordance with regulations 7 and 9;
  (ii) record-keeping procedures in accordance with regulation 12;
  (iii) except where the person concerned is an individual who in the course of relevant financial business does not employ or act in association with any other person, internal reporting procedures in accordance with regulation 14; and
  (iv) such other procedures of internal control (including an appropriate internal audit function) and communication as may be appropriate for the purposes of forestalling and preventing money laundering;
(b) complies with the identification and record keeping requirements of Part VII;
(c) takes appropriate measures from, time to time, for the purposes of making employees whose duties include the handling of relevant financial business aware of
  (i) the procedures under paragraph (a) which are maintained by him and which relate to the relevant financial business in question; and
  (ii) the enactments relating to money laundering; and
(d) provides such employees from time to time with training in the recognition and handling of transactions carried out by, or on behalf of, any person who is, or appears to be, engaged in money laundering.

(2) Whoever contravenes this regulation is guilty of an offence and liable -(a) on summary conviction, to a fine of five thousand dollars; or

(b) on conviction on indictment, to a fine and to imprisonment for two years.

(3) In determining whether a person has complied with any of the requirements of subregulation (1) -

(a) a court shall take into account any relevant supervisory or regulatory guidance which applies to that person; and
(b) a court may take into account any other relevant guidance issued by a body that regulates, or is representative of, any trade, profession, business or employment carried on by that person.

(4) In proceedings against a person for an offence under this regulation, it shall be a defence for that person to show that he took all reasonable steps and exercised all due diligence to avoid committing the offence.

(5) In this regulation-

"enactments relating to money laundering" means the enactments referred to in regulation 2(2) and the provisions of these regulations; and

"supervisory or regulatory guidance" means guidance issued, adopted or approved by the Authority or contained in regulations or a code of practice issued under the principal Law.

6. (1) Where an offence under regulation *5* committed by a body corporate is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a director, manager, secretary or other similar officer of the body corporate or a person who was purporting to act in any such capacity he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by the members, subregulation (1) shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of a body corporate.

(3) Where an offence under regulation *5* committed by a partnership, or by an unincorporated association other than a partnership, is proved to have been committed with the consent or connivance of, or is attributable to any neglect on the part of, a partner in the partnership or a person concerned in the management or control of the association, he, as well as the partnership or association, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

PART III - Identification Procedures

7. (1) Subject to regulations 8 and 10, identification procedures maintained by a person are in accordance with this regulation if in Cases I to 4 they require, transactions as soon as is reasonably practicable after contact is first made between that person and an applicant for business concerning any particular business relationship or one-off transaction -

(a) the production, by the applicant for business, of satisfactory evidence of his identity; or
(b) the taking of such measures specified in the procedures as will produce satisfactory evidence of his identity,

and the procedures are, subject to subregulation (6), in accordance with this regulation if they require that where that evidence is not obtained the business relationship or one-off transaction in question shall not proceed any further.

(2) Case 1 is any case where the parties form or resolve to form a business relationship between them.

(3) Case 2 is any case where, in respect of any one-off transaction, a person handling the transaction-

(a) knows or suspects that the applicant for business is engaged in money laundering other than terrorist financing, or that the transaction is carried out on behalf of another person engaged in money laundering other than terrorist financing; or
(b) knows or has reasonable cause to suspect that the applicant for business is engaged in terrorist financing, or that the transaction is carried out on behalf of another person engaged in terrorist financing.

(4) Case 3 is any case where, in respect of any one-off transaction, payment is to be made by or to the applicant for business of the amount of fifteen thousand dollars or more.

(5) Case 4 is any case where, in respect of two or more one-off transactions -

(a) it appears at the outset to a person handling any of the transactions -
(i) that the transactions are linked; and
(ii) that the total amount, in respect of all of the transactions, which is

payable by or to the applicant for business is fifteen thousand dollars or more; or

(b) at any later stage, it comes to the attention of such a person that sub-paragraphs (i) and (ii) of paragraph (a) are satisfied.

(6) The procedures referred to in subregulation (1) are in accordance with this regulation if, when a report is made in circumstances falling within Case 2 (whether in accordance with regulation 14 or directly to the Reporting Authority), they provide for steps to be taken in relation to the one-off transaction in question in accordance with any directions that may be given by the Reporting Authority.

(7) In these regulations, references to satisfactory evidence of a person's identity shall be construed in accordance with regulation 11(1).

8. (1) Where satisfactory evidence of the identity of an applicant for business would, apart from this regulation, be required under identification procedures in accordance with regulation 7 but -

(a) the circumstances are such that a payment is to be made by the applicant for business; and
(b) it is reasonable in all the circumstances -
(i) for the payment to be sent by post or delivered by hand or by any electronic means which is effective to transfer funds;

or

(ii) for the details of the payment to be sent by post or delivered by hand, to be given on the telephone or to be given by any other electronic means,

then, subject to subregulation (2), the fact that the payment is debited from an account held in the applicant's name at a licensee under the Banks and Trust Companies Law (2007 Revision) or at a bank that is regulated in, and either based or incorporated in or formed under the laws of, a country specified in the Third Schedule (whether the account is held by the applicant alone or jointly with one or more other persons) shall be capable of constituting the required evidence of identity.

(2) Subregulation (1) shall-

(a) not have effect to the extent that the circumstances of the payment fall within Case 2;
(b) not have effect to the extent that the payment is made by a person for the purpose of opening a relevant account with a licensee under the Banks and Trust Companies Law (2007 Revision); and
(c) cease to have effect in relation to an applicant for business where onward payment is to be made in any way other than results in -
(i) a reinvestment on behalf of the applicant with the same institution engaged in relevant financial business; or
(ii) a payment made directly to the applicant,

so that the evidence of identity of the applicant which would have been required but for the operation of subregulation (1) shall be obtained before payment of the proceeds is made (unless by operation of law the payment of the proceeds requires to be made to a trustee in bankruptcy, a liquidator, a trustee for an insane person or a trustee of the estate of a deceased person).

(3) For the purposes of subregulation (l)(b), it shall be immaterial whether the payment or its details are sent or given to a person who is bound by regulation *5(1)* or to some other person acting on his behalf.

(4) In this regulation-

"relevant account" means an account from which a payment may be made by any means to a person other than the applicant for business, whether such a payment -

(a) may be made directly to such a person from the account by or on behalf of the applicant for business; or

(b) may be made to such a person indirectly as a result of
(i) a direct transfer of funds from an account from which no such direct payment may be made to another account; or
(ii) a change in any of the characteristics of the account.

9. (1) This regulation applies where, in relation to a person who is bound by r regulation 5(1), an applicant for business is or appears to be acting otherwise than as principal.

(2) Subject to regulation 10, identification procedures maintained by a person are in accordance with this regulation if, in a case to which this regulation applies, they require reasonable measures to be taken for the purpose of establishing the identity of any person on whose behalf the applicant for business is acting,

(3) In determining, for the purposes of subregulation (2), what constitutes reasonable measures in any particular case, regard shall be had to all the circumstances of the case and, in particular, to best practice which, for the time being, is followed in the relevant field of business and which is applicable to those circumstances.

(4) Without prejudice to subregulation (3), if the conditions mentioned in subregulation *(5)* are fulfilled in relation to an applicant for business who is, or appears to be, acting as an agent for a principal (whether undisclosed or disclosed for reference purposes only) it shall be reasonable for a person bound by regulation 5(1) to accept a written assurance from the applicant for business to the effect that evidence of the identity of any principal on whose behalf the applicant for business may act in relation to that person will have been obtained and recorded under procedures maintained by the applicant for business; but a person bound by regulation 5(1) remains liable for any failure to so obtain and record satisfactory evidence of such identity.

(5) The conditions referred to in subregulation (4) are that, in relation to the business relationship or transaction in question, there are reasonable grounds for believing that the applicant for business -

(a) acts in the course of a business in relation to which an overseas regulatory authority exercises regulatory functions; and
(b) is based or incorporated in, or formed under the law of, a country specified in the Third Schedule.

(6) In subregulation *(5)* and regulation 10-

"overseas regulatory authority" means an authority which, in a country outside the Islands, exercises a function corresponding to a statutory function of the Authority in relation to relevant financial business in the Islands.

10. Subject to subregulation (2), identification procedures under regulations 7 and 9 shall not require any steps to be taken to obtain evidence of any person's identity-

(a) where there are reasonable grounds for believing that the applicant for business is a person who is bound by regulation 5(1);
(b) where there are reasonable grounds for believing that the applicant for business is himself
(i) acting in the course of a business in relation to which an overseas regulatory authority, as defined in regulation 9(6), exercises regulatory functions; and
(ii) is based or incorporated in, or formed under the law of, a country specified in the Third Schedule;
(c) where a one-off transaction is carried out with or for a third party pursuant to an introduction effected by a person who has provided an assurance that evidence of the identity of all third parties introduced by him will have been obtained and recorded under procedures maintained by him, where that person identifies the third party and where
(i) that person falls within paragraph (a); or
(ii) there are reasonable grounds for believing that the conditions mentioned in

regulation 9(5)(a) and (b) are fulfilled in relation to him;

(d) where the person who would otherwise be required to be identified, in relation to a one-off transaction, is the person to whom the proceeds of that transaction are payable but to whom no payment is made because all of those proceeds are directly reinvested on his behalf in another transaction
   (i) of which a record is kept; and
   (ii) which can result only in another reinvestment made on that person's behalf or in a payment made directly to that person;

(e) in relation to insurance business consisting of a policy of insurance in connection with a pension scheme taken out by virtue of a person's contract of employment or occupation where the policy -
   (i) contains no surrender clause; and
   (ii) may not be used as collateral for a loan;

(f) in relation to insurance business in respect of which a premium is payable in one installment of an amount not exceeding two thousand dollars; or

(g) in relation to insurance business in respect of which a periodic premium is payable and where the total payable in respect of any calendar year does not exceed eight hundred dollars.

(2) Nothing in this regulation shall apply in circumstances falling within Case 2.

(3) In this regulation-

"calendar year" means a period of twelve months beginning on the 31st December.

11. (1) For the purposes of these regulations, evidence of identity is satisfactory if

(a) it is reasonably capable of establishing that the applicant is the person he claims to be; and

(b) the person who obtains the evidence is satisfied, in accordance with the procedures maintained under these regulations in relation to the relevant financial business concerned, that it does establish that fact.

(2) In determining for the purposes of regulation 7(1) the time span in which satisfactory evidence of a person's identity has to be obtained, in relation to any particular business relationship or one-off transaction, all the circumstances shall be taken into account including, in particular -

(a) the nature of the business relationship or one-off transaction concerned;
(b) the geographical locations of the parties;
(c) whether it is practical to obtain the evidence before commitments are entered into between the parties or before money passes; and
(d) in relation to Case 3 or 4, the earliest stage at which there are reasonable grounds for believing that the total amount payable by an applicant for business is fifteen thousand dollars or more.

PART IV - Record-keeping Procedures

12. (1) Record-keeping procedures maintained by a person are in accordance with this regulation if they require the keeping, for the prescribed period, of the procedures following records -

(a) in any case where, in relation to any business relationship that is formed or one-off transaction that is carried out, evidence of a person's identity is obtained under procedures maintained in accordance with regulation 7 or 9, a record that indicates the nature of the evidence and –
   (i) comprises a copy of the evidence;
   (ii) provides such information as would enable a copy of it to be obtained; or
   (iii) in a case where it is not reasonably practicable to comply with sub-paragraph (i) or (ii), provides sufficient information to enable the details as to a person's identity contained in the relevant evidence to be re-obtained; and

(b) a record containing details relating to all transactions carried out by that person in the

course of relevant financial business.

(2) For the purposes of subregulation (1), the prescribed period is, subject to subregulation (3), the period of at least five years commencing with -

(a) in relation to such records as are described in paragraph (a), the date on which the relevant business was completed within the meaning of subregulation (4); and
(b) in relation to such records as are described in paragraph (b), the date on which all activities taking place in the course of the transaction in question were completed.

(3) Where a person who is bound by regulation *5(1)* -

(a) forms a business relationship or carries out a one-off transaction with another person;
(b) has reasonable grounds for believing that that person has become insolvent; and
(c) after forming that belief, takes any step for the purpose of recovering all or part of the amount of any debt payable to him by that person which has fallen due,

the prescribed period for the purposes of subregulation (1) is the period of at least five years commencing with the date on which the first such step is taken.

(4) For the purposes of subregulation (2)(a), the date on which relevant business is completed is -

(a) in circumstances falling within Case 1, the date of the ending the business relationship in respect of whose formation the under subregulation (l)(a) was compiled;
(b) in circumstances falling within Case 2 or 3, the date of the completion of all activities taking place in the course of the one-off transaction in respect of which the record under (1)(a) was compiled; or
(c) in circumstances falling within Case 4, the date of the completion of all activities taking place in the course of the last one-off transaction in respect of which the record under subregulation (l)(a) was compiled,

and where the formalities necessary to end a business relationship have not been approved, but a period of five years has elapsed since the date on which the last transaction was carried out in the course of that relationship, then the date of the completion of all activities taking place in the course of that last transaction shall be treated as the date on which the relevant business was completed.

13. (1) For the purposes of regulation 12(3)(b), a person shall be taken to be Insolvent, but only if

(a) he has been adjudged bankrupt or has made a composition or arrangement with his creditors;
(b) he has died and his estate falls to be administered in accordance with an order under section 66 of the Bankruptcy Law (1997 Revision); or
(c) where that person is a company, a winding up order or an administration order has been made or a resolution for voluntary winding up has been passed with respect to it, or a receiver or manager of its undertaking has been duly appointed, or possession has been taken, by or on behalf of the holders of any debentures secured by a floating charge, of any property of the company comprised in or subject to the charge, or a voluntary arrangement has been sanctioned under section 86 of the Companies Law (2007 Revision).

(2) Where a person bound by regulation 5(1) -

(a) is an appointed representative; and
(b) is not -

(i) a licensee under the Banks and Trust Companies Law (2007 Revision);
(ii) a licensee under the Insurance Law (2008 Revision);
(iii) a licensed mutual fund administrator under the Mutual Funds Law (2007 Revision); or
(iv) the holder of a licence under the Companies Management 2003 Revision Law (2003 Revision),

it shall be the responsibility of the appointed representatives' principal to ensure that record-keeping procedures in accordance with regulation 12 are maintained in respect of any relevant financial business carried out by the appointed representative which is investment business carried on by him for which the principal has accepted responsibility.

(3) Where record-keeping procedures in accordance with regulation 12 are not maintained in respect of business relationships formed, and one-off transactions carried out, in the course of such relevant financial business as is referred to in subregulation (2), an appointed representative's principal shall be regarded as having contravened regulation 5 in respect of those procedures and he, as well as the appointed representative, shall be guilty of an offence and shall be liable to be proceeded against and punished accordingly.

(4) In this regulation-

"appointed representative" means a person -

(a) who is employed by a person under a contract for services which
  (i) requires or permits him to carry on relevant financial business; and
  (ii) either prohibits him from giving advice about entering into investment agreements with persons other than his principal, or enables his principal to impose such a restriction or to restrict or prohibit the kinds of advice which he may give; or
  (iii) either prohibits him from procuring persons to enter into investment agreements with persons other than his principal, or enables his principal to impose such a prohibition or to restrict the kinds of investment to which the agreements may relate or the other persons with whom they may be entered into; and
(b) for whose activities in carrying on the whole or part of that relevant financial business his principal has accepted
responsibility in writing,

and the relevant financial business carried on by the appointed representative as such is the relevant financial business for which his principal has accepted responsibility.

PART V - Internal reporting procedures

14. Internal reporting procedures maintained by a person are in accordance with this regulation if they include provisions-

(a) identifying a person ("the appropriate person") to whom a report is to be made of any information or other matter which comes to the attention of a person handling relevant financial business and which, in the opinion of the person handling that business, gives rise to -
  (i) a knowledge or suspicion that another person is engaged in money laundering other than terrorist financing; or
  (ii) a knowledge or reasonable suspicion that another person is engaged in terrorist financing;
(b) requiring that any such report be considered in the light of all other relevant information by the appropriate person, or by another designated person, for the purpose of determining whether or not the information or other matter contained in the report does give rise to such a knowledge or suspicion;
(c) for any person charged with considering a report in accordance with paragraph (b) to have reasonable access to other information which may be of assistance to him and which is available to the person responsible for maintaining the internal reporting procedures

concerned; and

(d) for securing that the information or other matter contained in a report is disclosed to the Reporting Authority where the person who has considered the report under the procedures maintained in accordance with the preceding provisions of this regulation -

(i) knows or suspects that another person is engaged in money laundering other than terrorist financing; or

(ii) knows or has reasonable cause to suspect that another person is engaged in terrorist financing.

PART VI - Duty to Report Evidence of Money Laundering Other Than Terrorist Financing

15. (1) Subject to subregulation (2), this Part applies to the Authority and to a minister or official member in the exercise, in relation to any person carrying on relevant financial business, of his statutory or official functions.

(2) This Part does not apply to any disclosure of information to which Part 2 of Schedule 1 to the Terrorism Law, 2003 relates.

16. (1) Subject to subregulation (2), where the Authority, a minister or official Member -

(a) obtains any information; and

(b) is of the opinion that the information indicates that any person has or may have been engaged in money laundering, he shall, as soon as is reasonably practicable, disclose that information to the Reporting Authority.

(2) Where any person is a secondary recipient of information obtained by the Authority, a minister or official member, and that person forms such an opinion as is mentioned in subregulation (l)(b), that person may disclose the information to the Reporting Authority.

(3) Where any person employed by the Authority, appointed by the Authority to act as the Authority's agent, employed by any such agent or employed by the Government in the ministry or portfolio of a minister or official-

(a) obtains any information whilst acting in the course of any investigation, or discharging any functions, to which his appointment or authorisation relates; and

(b) is of the opinion that the information indicates that a person has or may have been engaged in money laundering,

that person shall, as soon as is reasonably practicable, either disclose that information to the Reporting Authority or disclose that information to the Authority, minister or official member by whom he was appointed or authorised.

(4) Any disclosure made by virtue of subregulations (1) to (3) shall not be treated as a breach of any restriction imposed by statute or otherwise.

(5) Any information -

(a) which has been disclosed to the Reporting Authority by virtue of subregulations (1) to (4); and

(b) which would, apart from subregulation (4), be subject to such a restriction as is mentioned in that subregulation,

may be disclosed by the Reporting Authority, or any person obtaining the information directly or indirectly from the Reporting Authority, in connection with the investigation of any criminal offence or for the purposes of any criminal proceedings, but not otherwise.

(6) In this regulation "secondary recipient", in relation to information obtained by the Authority, a minister or official member, means any person to whom that information has been passed by the Authority, a minister or official member.

PART VII - Identification and Record Keeping Requirements Relating to Wire Transfers

17. (1) Subject to subregulations (2) and (3), this Part applies to transfers of funds, in any currency, which are sent or received by a payment service provider carrying on business in or from within the Islands.

(2) This Part does not apply to transfers of funds carried out using a credit or debit card, if-

(a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services; and
(b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies such transfer of funds.

(3) This Part does not apply to transfers of funds -

(a) where the payer withdraws cash from his or her own account;
(b) where there is a debit transfer authorisation between two parties permitting payments between them through accounts, if a unique identifier accompanies the transfer of funds, enabling the person to be traced back;
(c) where truncated cheques are used;
(d) for fines, duties or other levies within the Islands; or
(e) where both the payer and the payee are payment service providers acting on their own behalf.

18. (1) Subject to regulation 19, a payment service provider of a payer shall ensure that transfers of funds are accompanied by complete information on the payer.

(2) The payment service provider of the payer shall, before transferring the funds, verify the complete information on the payer on the basis of documents, data or information that meet the requirements of regulation 11(1).

(3) In the case of transfers of funds from an account, verification may be deemed to have taken place if-

(a) the payer's account is held at a licensee under the Banks and Trust Companies Law (2007 Revision); or
(b) the payer is a person who is bound by regulation 5(1), but regulation 8(2)(a) and (b) shall, with necessary changes, apply.

(4) The payment service provider of the payer shall, for five years, keep records of complete information on the payer which accompanies transfers of funds.

19. Where both the payment service provider of the payer and the payment service provider of the payee are situated in the Islands, transfers of funds shall be required to be accompanied only by the account number of the payer or a unique identifier allowing the transaction to be traced back to the payer; but, if so requested by the payment service provider of the payee, the payment service provider of the payer shall make available to the payment service provider of the payee complete information on the payer, within three working days of receiving that request.

20. In the case of batch file transfers from a single payer where the payment service providers of the payees are situated outside the Islands, regulation 18(1) shall not apply to the individual transfers bundled

together therein, if the batch file contains that information and the individual transfers carry the account number of the payer or a unique identifier.

21. The payment service provider of a payee shall have effective procedures in place in order to detect whether, in the messaging or payment and settlement system used to effect a transfer of funds, the following information on the payer is missing -

(a) for transfers of funds where the payment service provider of the payer is situated in the Islands, the information required under regulation 19;
(b) for transfers of funds where the payment service provider of the payer is situated outside the Islands, complete information on the payer, or where applicable, the information required under regulation 26; and
(c) for batch file transfers where the payment service provider of the payer is situated outside the Islands, information on the payer as referred to in regulation 20 in the batch file transfer only, but not in the individual transfers bundled therein.

22. Where the payment service provider of the payee detects, when receiving transfers of funds, that information on the payer required under this Part is missing or incomplete it shall either reject the transfer or ask for complete payer information on the payer; and, in any event, the payment service provider of the payee shall comply with the Law, the Terrorism Law, 2003 and these regulations.

(2) Where a payment service provider regularly fails to supply the required information on the payer, the payment service provider of the payee shall adopt reasonable measures to have the payment service provider of the payer correct the failures, before -

(a) rejecting any future transfers of funds from that payment service provider;

(b) restricting its business relationship with that payment service provider; or
(c) terminating its business relationship with that payment service provider,

and the payment service provider of the payee shall report to the Reporting Authority and to the Authority any such decision to restrict or terminate its business relationship with that payment service provider.

23. The payment service provider of the payee shall consider missing or incomplete information on the payer as a factor in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether it must be reported to the Reporting Authority, in accordance with the Law and these regulations.

24. The payment service provider of the payee shall, for five years, keep records of any information received on the payer.

25. Intermediary payment service providers shall ensure that all information received on the payer that accompanies a transfer of funds is kept with the transfer.

26. (1) This regulation applies where the payment service provider of the payer is situated outside the Islands and the intermediary payment service provider is situated within the Islands, in respect of transfers of funds by the intermediary payment service provider within the Islands.

(2) Subject to subregulation (3), the intermediary payment service provider may use a payment system with technical limitations which prevent information on the payer from accompanying the transfer of funds to send transfers of funds to the payment service provider of the payee.

(3) Where the intermediary payment service provider receives a transfer of funds that does not have complete information on the payer as required under this Part, it shall only use a payment system with technical limitations if it is able to inform the payment service provider of the payee thereof, using a manner of communication accepted by, or agreed between, both payment service providers.

(4) Where the intermediary payment service provider uses a payment system with technical limitations, the intermediary payment service provider shall, upon request from the payment service provider of the payee, make available to the payment service provider of the payee all the information on the payer which it has received, irrespective of whether it is complete or not, within three working days of receiving that request.

(5) In the cases referred to in subregulations (2) and (3), the intermediary payment service provider shall, for five years, keep records of all information received.

27. Payment service providers shall respond fully and without delay to enquiries from the Reporting Authority concerning the information on the payer accompanying transfers of funds and corresponding records.

28. Where there is an inconsistency between the provisions of this Part and any Conflicts other provision of these regulations, the provisions of this Part shall prevail, to the extent of the inconsistency.

FIRST SCHEDULE

regulation 2

CLASSES OF LONG TERM BUSINESS

Number	Description	Nature of Business
I	Life and annuity	Effecting and carrying out contracts of insurance on human life or contracts to pay annuities on human life, but excluding (in each case) contracts within Class III below.
II	Marriage and birth	Effecting and carrying out contracts of insurance to provide a sum on marriage or on the birth of a child, being contracts expressed to be in effect for a period of more than one year.
III	Linked long term	Effecting and carrying out contracts of insurance on human life or contracts to pay annuities on human life where the benefits are wholly or partly to be determined by reference to the value of, or the income from, property of any description (whether or not specified in the contracts) or by reference to fluctuations in, or in an index of, the value of property of any description (whether or not so specified).
IV	Permanent health	Effecting and carrying out contracts of insurance providing specified benefits against risks of persons becoming incapacitated in consequence of sustaining injury as a result of an accident, of an accident of a specified class or of sickness or infirmity, being contracts that- (a) are expressed to be in effect for a period of not less than five years or until the normal retirement age for the persons concerned, or without limit of time; and (b) either are not expressed to be terminable by the insurer, or are expressed to be so terminable only in special circumstances mentioned in the contract.
V	Tontines	Effecting and carrying out tontines.
VI	Capital redemption	Effecting and carrying out capital redemption contracts.
VII	Pension fund management	Effecting and carrying out- (a) contracts to manage the

investments of pension funds; or
(b) contracts of the kind mentioned in paragraph (a) that are combined with contracts of insurance covering either conservation of capital or payment of a minimum interest.

SECOND SCHEDULE

regulation 4(1)(g)

LIST OF ACTIVITIES FALLING WITHIN THE DEFINITION OF "RELEVANT FINANCIAL BUSINESS"

1. Acceptance of deposits and other repayable funds from the public.

2. Lending.

3. Financial leasing.

4. Money transmission services.

5. Issuing and administering means of payment (e.g. credit cards, travellers

cheques and bankers drafts).

6. Guarantees and commitments.

7. Trading for own account or for account of customers in -

(a) money market instruments (cheques, bills, CD5, etc.);
(b) foreign exchange;
(c) financial futures and options;
(d) exchange and interest rate instruments; or
(e) transferable securities.

8. Participation in securities issues and the provision of services related to such issues.

9. Advice to undertakings on capital structure, industrial strategy and related questions and advice and services relating to mergers and the purchase of undertakings.

10. Money broking.

11. Portfolio management and advice.

12. Safekeeping and administration of securities.

13. Safe custody services.

14. Financial, estate agency and legal services provided in the course of business relating to the sale, purchase or mortgage of land or interests in land on behalf of clients or customers.

15. The services of listing agents and broker members of the Cayman Islands Stock Exchange as defined in the CSX Listing Rules and the Cayman Island Stock Exchange Membership Rules respectively.

16. The conduct of securities investment business.

17. Dealing in precious metals or precious stones, when engaging in a cash transaction of fifteen thousand dollars or more.

THIRD SCHEDULE

regulation 9(5)(b)

COUNTRIES AND TERRITORIES WITH EQUIVALENT LEGISLATION

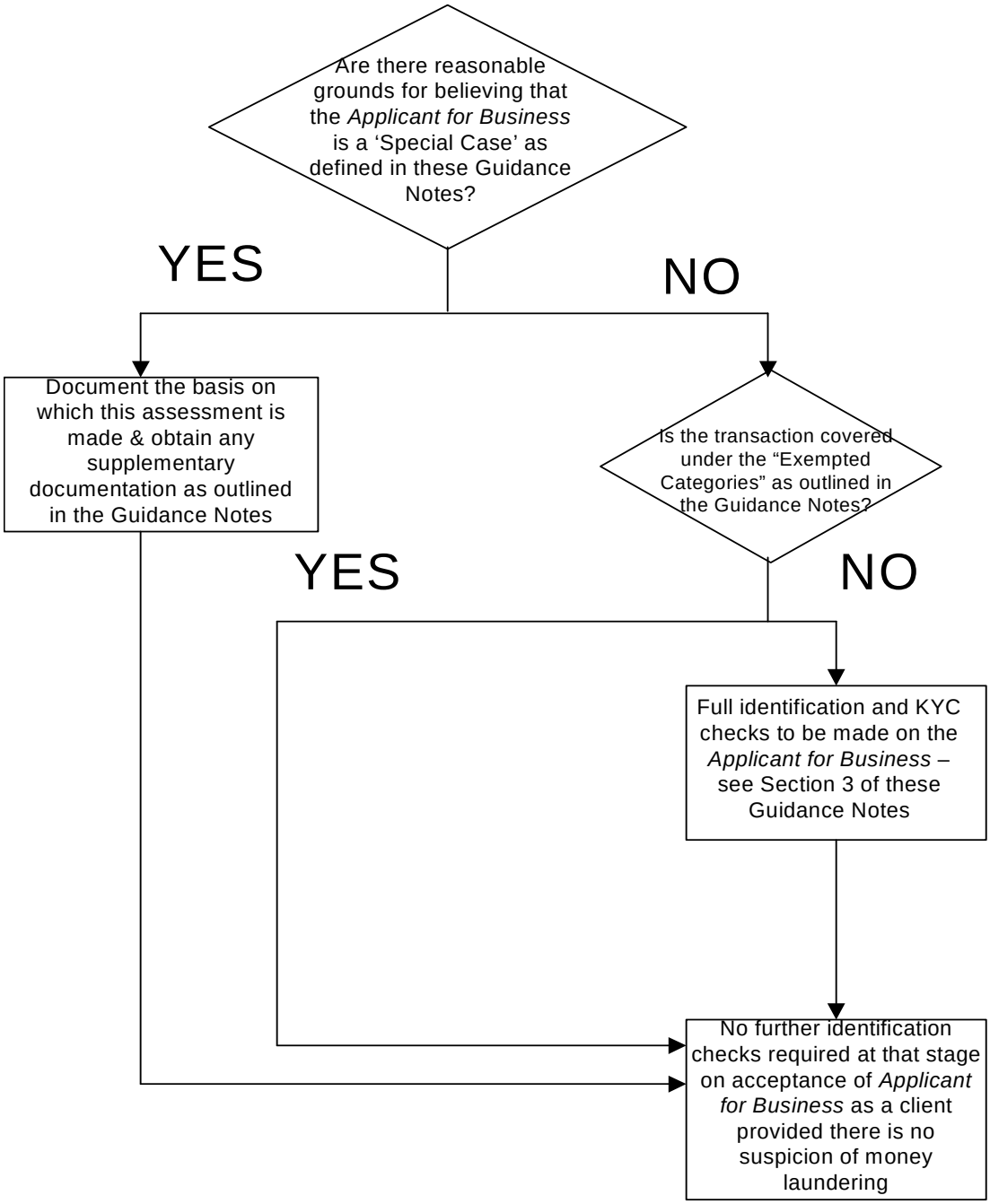
Argentina
Australia
Austria
Bahamas
Bahrain
Barbados
Belgium
Bermuda
Brazil
British Virgin Islands
Canada
Denmark
Finland
France
Germany
Gibraltar
Greece
Guernsey
Hong Kong
Iceland
Ireland
Isle of Man
Israel
Italy
Japan
Jersey
Liechtenstein
Luxembourg
Malta
Mexico
Netherlands
New Zealand
Norway
Panama
Portugal
Singapore
Spain
Sweden
Switzerland
Turkey
United Arab Emirates
United Kingdom
United States of America

Publication in consolidated and revised form authorised by the Governor in Cabinet this 13th day of May, 2008.

Appendix D - Anti-Money Laundering Flowchart Summary Of Identification Checks

Note: This flow chart is designed as a summary document and may not be exhaustive. Financial Institutions should refer to specific previsions within the legislation and the Guidance Notes to ascertain the full requirements

DIRECT APPLICANTS FOR BUSINESS



Appendix E- Request For Verification Of Customer Identity

Financial Institutions *using this form must obtain the prior consent of the customer to avoid breaching confidentiality).*

To: (Address of financial institution to which request is sent)

From: (Stamp of financial institution sending the letter)

Dear Sirs,

REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY

In accordance with the Cayman Islands Anti-Money Laundering Guidance Notes for Financial Services Providers, we write to request your verification of the identity of our prospective customer detailed below.

Full name of customer
_____

Title:(Mr/Mrs/Miss/Ms)
SPECIFY_____

Address including postcode (as given by customer)
_____

Date of birth:_____ Account No. (if known
_____

A specimen of the customer's signature is attached.

Please respond promptly by returning the tear-off portion below. Thank you.

To: The Manager (originating institution)

From: (Stamp of sending Financial Institution)

Request for verification of the identity of [title and full name of customer]

With reference to your enquiry dated
_____ we:

(*Delete as applicable)

1. Confirm that the above customer *is/is not known to us. If yes, for _____years.

2. *Confirm/Cannot confirm the address shown in your enquiry. If yes, the nature of evidence held is_____

3. *Confirm/Cannot confirm that the signature reproduced in your enquiry appears to be that of the above customer.

Name:_____
Signature:_____

Job Title: _____ Date: _____

The above information is given in strict confidence, for your private use only, and without any guarantee or responsibility on the part of this institution or its officials.

Appendix F - Eligible Introducer's Form

(To be completed by the Introducer)

Information about the Introducer

Name of Introducer:_____

Address of Introducer:_____

Telephone number: _____ Fax number _____

Email: _____

Name of Applicant for Business

_____

Address of Applicant for Business:

_____

_____

I/We confirm that I/We am/are:- *[Please tick as appropriate]*

1. A Financial Service Provider in a schedule 3 country as defined by the Money Laundering Regulations of the Cayman Islands ☐

2. An institution which belongs to the same corporate group as the Cayman Islands Financial Services Provider ☐

3. A Professional Intermediary in a schedule 3 country as defined by the Money Laundering Regulations of the Cayman Islands. (specify which country) ☐

4. A member of a local association or professional body to which the regulations apply which is subject to disciplinary procedures for failure to conduct relevant financial business in accordance with equivalent rules and guidelines to the Money Laundering Regulations of the Cayman Islands. ☐

5. A business which is subject to the Money Laundering Regulations of the Cayman Islands ☐

   Name and address of relevant regulator/professional body

   _____

   _____

   _____

I confirm that I have satisfactory evidence of the identity of the introduced client and will on request provide a copy of that evidence. Satisfactory evidence is such evidence

as will satisfy the anti-money laundering regime in the Schedule 3 country from which the introduction is made.

Name:_____

Signature:_____

Job Title:_____

Date:_____

OR

I confirm that under the law of the Schedule 3 jurisdiction from which the introduction is made, I am not required to have evidence of identity of the client since the relationship existed before the implementation of the anti-money laundering regime. I confirm that the applicant has been a client of mine since DD/MM/YY and I am not aware that the applicant has been found to be or has been suspected of activity that would presently constitute a money laundering offence. I also confirm that I have fully complied with the anti-money laundering regime to which I am subject.

Name:_____

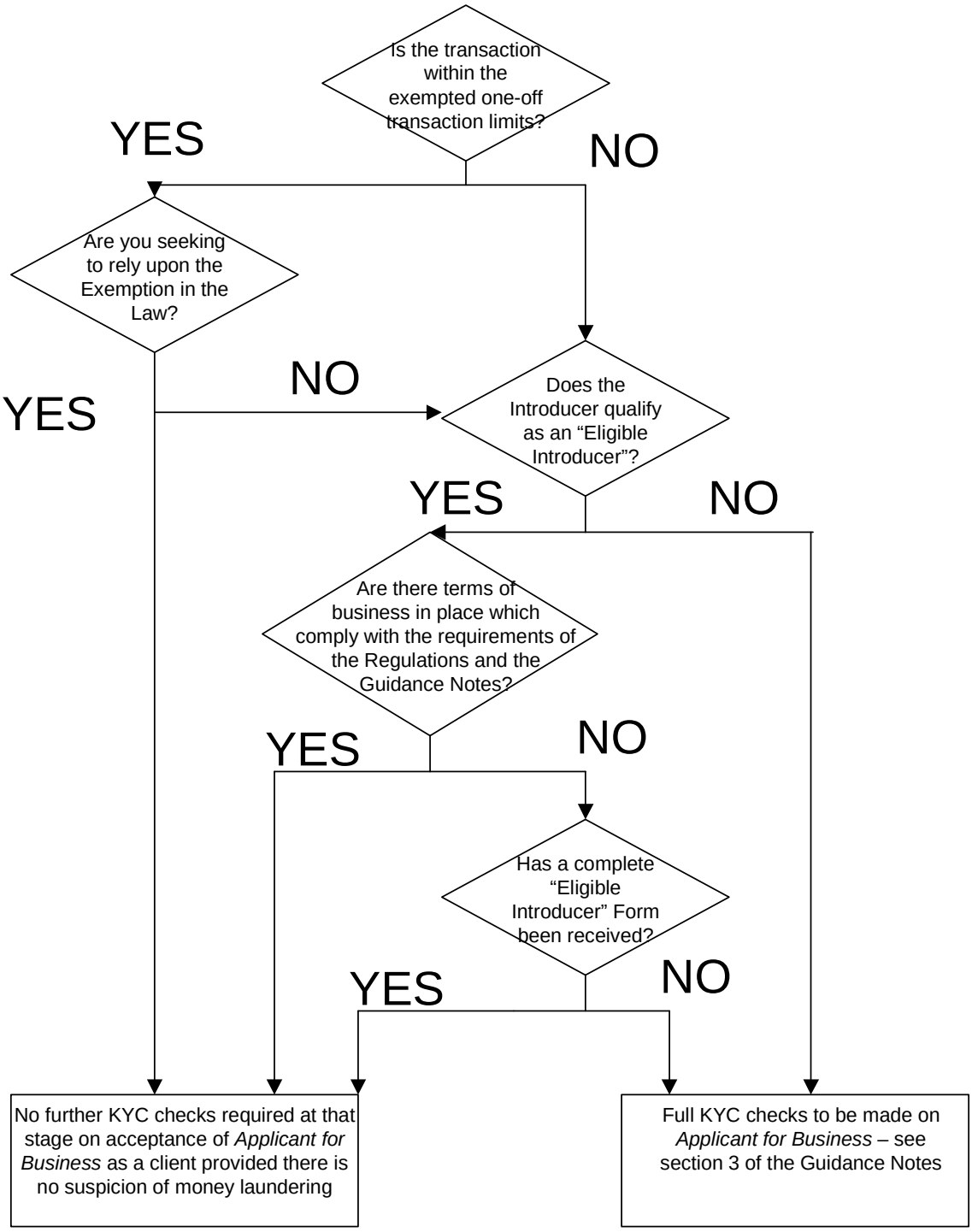
Signature:_____

Job Title:_____

Date:_____

Appendix G - Introduced Business Flow Chart

Note: This flowchart is designed as a summary document and may not be exhaustive. Financial Services Providers should refer to specific provisions within the legislation and the Guidance Notes to ascertain the full requirements.



Appendix H - Approved Markets And Exchanges

In addition to the Cayman Islands Stock Exchange, the following are markets and exchanges approved by the *Monetary Authority* as at [date], 2008. Amendments to this list may be made by the *Monetary Authority* from time to time. Such amendments will be gazetted.

American Stock Exchange (AMEX)
Athens Stock Exchange
Australian Securities Exchange
Barcelona Stock Exchange
Berlin Stock Exchange
Bermuda Stock Exchange
Bilbao Stock Exchange
Bolsa de Comercio de Buenos Aires
Bolsa de Comercio de Santiago
Bolsa de Valores de Caracas
Bolsa de Valores de Lima
Borsa Italiana SPA
Boston Stock Exchange
Chicago Stock Exchange
Dusseldorf Stock Exchange
Euronext Brussels
Euronext Lisbon
Euronext NV
Euronext Paris
Frankfurt Stock Exchange
Fukuoka Stock Exchange
Hamburg and Hannover Stock Exchange
Hong Kong Stock Exchange
International Securities Exchange
Irish Stock Exchange
Johannesburg Stock Exchange
Korea Stock Exchange
Kuala Lumpur Stock Exchange
London Stock Exchange
Luxembourg Stock Exchange
Madrid Stock Exchange
Mexican Stock Exchange
Montreal Exchange
Munich Stock Exchange
Nagoya Stock Exchange
NASDAQ
National Stock Exchange
New York Stock Exchange
New Zealand Stock Exchange
NYSE Arca
OMX Nordic Exchange
Osaka Securities Exchange
Oslo Stock Exchange
Philadelphia Stock Exchange
Rio de Janeiro Stock Exchange
São Paulo Stock Exchange (Bovespa)
Singapore Exchange
Stuttgart Stock Exchange
SWX Swiss Exchange
Taiwan Stock Exchange
Tel Aviv Stock Exchange
The Stock Exchange of Thailand
Tokyo Stock Exchange
Toronto Stock Exchange
Valencia Stock Exchange
Vienna Stock Exchange

Appendix I - Internal Report Form

Name of customer:

Full account name(s):

Account no(s):

Date(s) of opening:

Date of customer's birth:

Nationality:

Passport number:

Identification and references:

Customer's address:

Details of transactions arousing suspicion:

As relevant:

Amount (currency) Date of receipt Sources of funds

Other relevant information:

Money Laundering Reporting Officer:
(The Reporting Officer should briefly set out the reason for regarding the transactions to be reported as suspicious or, if he decides against reporting, his reasons for that decision.)

Appendix J - Suspicious Activity Reporting Form

CONFIDENTIAL

FINANCIAL REPORTING AUTHORITY

Delivery Address:
80E Shedden Road
3rd Floor, Elizabethan Square, Phase IV
George Town, Grand Cayman
Cayman Islands
Tel No. (345) 945-6267
Fax No. (345) 945-6268

Mailing Address:
P.O. Box 1054
Grand Cayman KY1 - 1102
Cayman Islands

SUSPICIOUS ACTIVITY REPORT

Note: This form should preferably be typed using arial 12 point font.

Date of this Report:	Date of Original Report (if applicable): FRA Case No. (if known):

1. REPORTING ENTITY DETAILS:

Name of Reporting Entity: Reference of Reporting Entity:

Address of Reporting Entity:

Name of Money Laundering Reporting Officer:
Note: The name of an individual who is authorized to discuss the contents of this report must be provided.

Phone number:

Fax number: Direct private fax: yes no

Do you wish to be contacted prior to faxes being sent to this number: yes no

Type of Reporting Entity:
(i.e. bank, trust company, mutual fund administrator, insurance manager, real estate agent etc.)

Nature of service(s) provided to the individual and / or entity that is the subject of this report:

2. SUBJECT(S) OF REPORT (Natural Persons):
Note: Please attach additional sheets as necessary.

Surname: First Name: Gender:

Date of Birth: Place of Birth: Nationality:

Occupation/Profession:

Address(es):
PO Box: Street No. and Name: City/Town

State/Province Country Zip/Postal Code:

Telephone No: Fax No.: E-Mail:

Identification Document Type:
(i.e. passport, driver's license etc.)

Identification Document Number:

Date of Issue:

Place of Issue:

Account number(s) if applicable:

Other signatories on the account. (Please include relevant KYC details):

Other Information:

3. SUBJECT(S) OF REPORT (Legal Entities)
Note: Please attach additional sheets as necessary.

Entity Type (company, trust, partnership, charity, other):

Name of Entity:

Jurisdiction of Incorporation/Registration:

Date of Incorporation/Registration:

Purpose of Entity:

Registered Office Address (or address of Trustee or General Partner etc.):

Business Address (if different from registered office address)**:**

NOTE: Please include relevant information for entity type (i.e. settlor and beneficiary information for a trust). For each of the following which is a natural person please provide the information noted in Section 2.

Shareholder(s):
Name(s):

Director(s):
Name(s)

Ultimate Beneficial Owner (s) if different from above:
Name(s):

Account number(s) if applicable:

Other signatories on the account: (Please include relevant KYC details):

4. OTHER FINANCIAL SERVICE PROVIDERS INVOLVED IN ACTIVITY:

Name(s): Address(es):

Account number(s) if applicable:

Other Information:

5. REASON FOR SUSPICION

Note: Please include relevant details including date business relationship established/declined, source of funds, value of assets currently held if any and nature of the suspicion. Attach additional sheets as necessary.

Appendix K - Examples Of Suspicious Activities

The examples within this Appendix are not exhaustive nor are they exclusive to any one type of investment business. They may apply equally to portfolio managers, investment advisers, stockbrokers, et al.

The fact that a particular kind of behaviour or type of transaction is mentioned does not of course mean that it is sinister. It may well have an entirely innocent explanation. The examples are intended to promote awareness and stimulate a culture of deterrence to money laundering.

Financial institutions should pay particular attention to:

Accounts

(1) Accounts that receive relevant periodical deposits and are dormant at other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out.

(2) A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

(3) When opening an account, the customer refuses to provide information required by the financial institution, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.

(4) An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

(5) An account opened by a legal entity or an organisation that has the same address as other legal entities or organisations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

(6) An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits are made in comparison with the income of the founders of the entity.

(7) The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

(8) An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation.

(9) An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organisation and that shows movements of funds above the expected level of income.

Deposits and withdrawals

(1) Deposits for a business entity in combinations of monetary instruments that are atypical of the activity normally associated with such a business (for example, deposits that include a mix of business, payroll and social security cheques).

(2) Large cash withdrawals made from a business account not normally associated with cash transactions.

(3) Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in cheques or other payment instruments.

(4) Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

(5) Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

(6) The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.

(7) The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

(8) The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.

(9) The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

Wire Transfers

(1) Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

(2) Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.

(3) Use of multiple personal and business accounts or the accounts of non-profit organisations or charities to collect and then funnel funds immediately or after a short time to a small umber of foreign beneficiaries.

(4) Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.

Characteristics of the customer or his/her business activity

(1) Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.

(2) Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.).

(3) Stated occupation of the transactor is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

(4) Regarding non-profit or charitable organisations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

(5) A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

(6) Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

Transactions linked to locations of concern

(1) Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example, countries designated by national authorities; and counties where major AML/CFT deficiencies have been identified by international organisations, such as the FATF).

(2) Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities; and counties where major AML/CFT deficiencies have been identified by international organisations, such as the FATF).

(3) A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern.

(4) The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern.

(5) A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.

(6) The opening of accounts of financial institutions from locations of specific concern.

(7) Sending or receiving funds by international transfers from and/or to locations of specific concern.

Financial Services Providers

The examples given for intermediaries/introducers may also be relevant to the direct business of *Financial Services Providers*. The product provider will often effectively be the counterparty of the intermediary and should be alert to unusual transactions or investment behaviour, particularly where under the Regulations the *Financial Services Provider* is relying on the intermediary/introducer for identification of the customer. The systems and procedures of the *Financial Services Providers* are geared to serving the needs of the "normal" or "average" investors, as this is the most cost-effective solution. Hence, unusual behaviour should be readily identifiable.

Particular care should be taken where:-

(a) settlement of purchases or sales involves (or appears to involve) third parties other than the investor;

(b) bearer shares (if available) are requested;

(c) bearer or unregistered securities/near-cash instruments are offered in settlement of purchases;

(d) there is excessive switching;

(e) there is early termination despite front-end loading or exit charges;

(f) they become aware that the customer's holding has been pledged to secure a borrowing in order to gear up his investment activities;

(g) they are managing or administering an unregulated collective investment scheme or pooled funds arrangement.

The routes and devices used to launder criminal money are limited only by the imagination and ingenuity of those concerned. These are examples of potentially suspicious transactions. The Authority is always pleased to learn from Financial Institutions of new examples and techniques they come across in their day-to-day business.

Appendix L: Sources of Information on the Financing of Terrorism

Several sources of information exist that may help financial institutions in determining whether a potentially suspicious or unusual transaction could indicate funds involved in the financing of terrorism and thus be subject to reporting obligations under national anti-money laundering or antiterrorism laws and regulations.

A. United Nations lists

Committee on S/RES/1267 (1999) website:
http://www.un.org/Docs/sc/committees/AfghanTemplate.htm

B. Other lists

(1) United States

Terrorism and financial intelligence

US Department of the Treasury website:
http://www.treas.gov/offices/enforcement/

(2) Council of the European Union

Council Regulation (EC) Nº 467/2001 of 6 March 2001 [on freezing Taliban funds]

Council Decision (EC) Nº 927/2001 of 27 December 2001 [list of terrorist and terrorist organisations whose assets should be frozen in accordance with Council Regulation (EC) Nº 2580/2001]

Council Common Position of 27 December 2001 on application of specific measures to combat terrorism [list of persons, groups and entities involved in terrorist acts]

EUR-lex website: http://eur-lex.europa.eu/en/index.htm

C. Standards

(1) Financial Action Task Force

FATF Special Recommendations on Terrorist Financing

a) FATF Forty Recommendations on Money Laundering

FATF website:

http://www.fatf-gafi.org/document/28/0,2340,en_32250379_32236930_33658140_1_1_1_1,00.html#40recs

(2) UN Conventions and Resolutions

International Convention on the Suppression of Terrorist Financing

Website: http://untreaty.un. org/English/Terrorism.asp

UN Security Council Resolutions on Terrorism
Website: http://www.un.org/terrorism

(3) Council of the European Union

Council Regulation (EC) Nº 2580/2001 of 27 December 2001 on specific restrictive

measures directed against certain persons and entities with a view to combating terrorism

EUR-lex website: http://eur-lex.europa.eu/en/index.htm

Appendix M - Glossary Of Terms

Applicant for Business
A person seeking to form a business relationship or carry out a one-off transaction, with a person who is carrying out relevant financial business in the Islands.

Appropriate Person
Money Laundering Reporting Officer

Associations not for Profit
An association that is formed and maintained for the purpose of promoting commerce, art, science, religion, charity or any other useful object where it is the intention of such association to apply the profits if any, or other income of the association in promoting its objects and to prohibit the payment of any dividend to the members of the association, other than payment for reasonable services rendered

Authorised Person
An individual who conducts relevant financial business, and is either licensed by the Monetary Authority, or licensed by a body in a Schedule 3 country with similar functions to the Monetary Authority.

Authority
The Cayman Islands Monetary Authority

Business Relationship
Regulation 3(2) defines a business relationship as an arrangement between two or more persons where the purpose of the arrangement is to facilitate the carrying out of transactions between the persons concerned on a frequent or habitual basis; and the total amount of any payment or payments to be made by any person to any other in the course of that arrangement is not known or capable of being ascertained at the time the arrangement is made.

Exempted one-off transaction
A single or series of linked transactions where the aggregate sum is less than $15,000.

Financial Services Provider
A person or business conducting relevant financial business as defined under the legislation.

Financial Institution
Reference is made in these Guidance Notes to Financial Institutions particularly in the context of due diligence procedures necessary when a prospective client is introduced by or is a Financial Institution in a country with equivalent legislation. In this context, Financial Institutions refer not only to banks but also to non bank financial institutions, namely insurance companies, savings or pension societies, building societies, security brokers and dealers, regulated investment managers, bureaux de change, credit unions, licensed or otherwise regulated corporate trustees and the following clearing agents, their operators and depositories:

i) Clearstream Banking Société Anonyme
ii) Euroclear;
iii) Canadian Depository For Securities; and
iv) Depository Trust Company,

and such other clearing agents (their operators and depositories) as the Cayman Islands Monetary Authority shall from time to time designate.

Introducer
An individual or institution, which is introducing business to a *Financial Services Provider* in the Cayman Islands

One-off transaction
Any transaction other than a transaction carried out in the course of an established business relationship formed by a person acting in the course of relevant financial business.

Relevant financial business
Defined in section 4(1) of the Money Laundering Regulations (2006 Revision)

Reporting Authority
The Reporting Authority as appointed by the Governor under section 21 (2) of the Proceeds of Crime Law.

Vigilance Policy
The policy, group-based or local, of an institution to guard against:
(i) its business (and the financial system at large) being used for laundering; and
(ii) the committing of any of the offences under the anti money laundering legislation of the Cayman Islands by the institution itself or its staff.