GUIDANCE NOTES

FOR THE PREVENTION & DETECTION OF MONEY LAUNDERING AND THE FINANCING OF TERRORISM

FOR THE LEGAL SECTOR

ISSUED BY

THE BARRISTERS AND ACCOUNTANTS AML/ATF BOARD

August 2012

TABLE OF CONTENTS

INTRODUCTION

1.1 Lawyers are key professionals in the business and financial sector who often facilitate vital transactions that underpin Bermuda's economy. As such, they have a significant role to play in ensuring that their services are not used to further a criminal purpose. Increasingly over the past decade, criminals have responded to the anti-money laundering and anti-terrorism financing measures taken by the traditional financial institutions and have sought other means to convert their proceeds of crime, or to mix them with legitimate income before they enter the banking system, thus making those proceeds of criminal conduct harder to detect. Frequently, professional advisors such as lawyers and accountants who interface with the financial sector have been used in some jurisdictions as a conduit for criminal property to enter the financial system and as such Bermuda's legal fraternity should be on guard to ensure that it is not used in this manner.

1.2 In particular, criminals and money launderers will often try to exploit the services offered by lawyers, through the business of undertaking property and financial transactions, setting up corporate and trust structures and when acting as directors or trustees. Furthermore, client accounts can provide a money launderer with a valuable, anonymous, route into the banking system.

1.3 The inter-governmental agencies and international standard-setting bodies such as the Financial Action Task Force ("FATF") have recognized the access that professional advisors provide for their clients to financial services and products, and have extended the scope of the international standards and recommendations to include lawyers and accountants – often referred to as 'gatekeepers'. As a well-regulated jurisdiction operating within the international financial arena, Bermuda has adopted these international standards to guard against money laundering and terrorist financing and has integrated the requirements into its legal and regulatory framework.

1.4 The continuing ability of Bermuda's finance industry to attract legitimate clients with funds and assets that are clean and untainted by criminality depends, in large part, upon the Island's reputation as a sound, well-regulated jurisdiction. Therefore, any professional legal advisor in Bermuda who is found to be involved in a money laundering or terrorism financing scheme with knowledge or suspicion of the connection to crime may face a range of penalties including the loss of reputation, disciplinary action by the Bermuda Bar Association ("the Bar") and prosecution for criminal offences. Every law firm in Bermuda must recognize the role that it must play in protecting itself and its employees from involvement in money laundering and terrorist financing, and also in protecting the Island's reputation. This principle relates not only to business operations within Bermuda, but also operations conducted by Bermuda law firms outside the Island.

1.5 These Guidance Notes have been issued by the Barristers and Accountants AML/ATF Board ("the Board") to provide law firms for whom the Board has supervisory authority with guidance as to how they should carry out their obligations as required under Bermuda's legislative framework for the prevention and detection of money laundering and terrorist financing. However, these Guidance Notes are not intended to be exhaustive or a replacement for a firm's internal policies and procedures manual. Section 30I (6) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 ("the SEA Act") provides that in deciding whether a regulated professional firm has failed to comply with a requirement of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 ("the AML/ATF Regulations"), the designated professional body must consider whether the firm followed any relevant guidance which was at the time issued by the designated professional body.

1.6 For the purposes of these Guidance Notes, "lawyers" refers to professional legal advisers as defined by Regulation 2(1) of the AML/ATF Regulations as read with Section 42A of the Proceeds of Crime Act 1997 ("POCA")- a barrister and attorney who is a member of the Bar, and "law firms" refers to firms as defined by section 2(1) of the SEA Act – a professional company, association or partnership of barristers in independent practice and the employees, servants and agents of such company, association or partnership of barristers,

including a barrister in independent practice, operating as a sole proprietor and his employees, servants and agents.

Separate Guidance Notes for the prevention and detection of money laundering and the financing of terrorism have been drafted for the Bermuda Accounting Sector.

LEGISLATIVE and REGULATORY FRAMEWORK

2.1 Bermuda's key legislative enactments pertaining to money laundering and terrorist financing (the "AML/ATF legislation") primarily consists of the following:

- Proceeds of Crime Act 1997 ("POCA");
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 ("AML/ATF Regulations");
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 ("SEA Act");
- Anti-Terrorism (Financial and Other Measures) Act 2004 ("ATFA");
- Financial Intelligence Agency Act 2007 ("FIA Act");
- Proceeds of Crime (Designated Countries and Territories) Order 1998;
- The Criminal Justice (International Cooperation)(Bermuda)Act 1994;
- Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011 ("TAFA 2011 Order");
- International Sanctions (Al-Qaida) (United Nations Measures) Regulations 2012 ("Al-Qaida Regulations") which implement The Al-Qaida (United Nations Measures) (Overseas Territories) Order 2012 No. 1757 ("Al-Qaida Order 2012");
- International Sanctions (Afghanistan) (United Nations Measures) Regulations 2012 ("Afghanistan Regulations which implement The Afghanistan (United

Nations Measures) (Overseas Territories) Order 2012 No. 1758 ("Afghanistan Order 2012");

- International Sanctions (Iran) (Nuclear Proliferation) (Restrictive Measures) Regulations 2012 ("Iran (Nuclear Proliferation) Regulations") which implements The Iran (Restrictive Measures) (Overseas Territories) Order 2012 No. 1756 ("Iran (Nuclear Proliferation) Order 2012"); and

- The North Korea (United Nations Measures) (Overseas Territories) Order 2006 No. 3327 ("North Korea Order 2006"), as amended.

In addition reference should also be made to www.bermudalaws.bm for a comprehensive list of Bermuda's legislation.

2.2 Supervisory Role

Regulation 2(1) of the AML/ATF Regulations defines a relevant person as a person to whom in accordance with Regulation 4 of the AML/ATF Regulations those Regulations apply, namely AML/ATF regulated financial institutions and independent professionals acting in the course of business carried on by them in or from Bermuda. Law firms that are "relevant persons" pursuant to Regulation 2(1) of the AML/ATF Regulations must put in place systems and controls to guard against money laundering and terrorist financing in accordance with Bermuda's requirements, which are based on the international standards set by the FATF. The FATF standards require that all relevant persons must be supervised by an appropriate anti-money laundering supervisory authority. The Board has been established pursuant to Section 25A of the Bermuda Bar Act 1974. The Minister of Justice by Order has designated the Board under section 4(1) of the SEA Act as the supervisory authority for the purposes of section 3(1) (b) of that Act as the professional body for the relevant persons regulated by it.

2.2.1 The AML/ATF Regulations apply to independent professionals pursuant to Regulation 4. An independent professional is defined in Regulation 2(1) of the AML/ATF Regulations as meaning a professional legal adviser or accountant being a firm or sole practitioner in independent practice who by way of business provides legal or accountancy services to other persons when participating in financial or real property transactions concerning -

- buying and selling of real property;
- managing of client monies, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies; or
- creation, operation or management of legal persons or arrangements, and buying and selling business entities

2.2.2 A person is defined as participating in a transaction by assisting in the planning or execution of the transaction, or otherwise acting for or on behalf of a client in the transaction.

2.3 Guidance Notes

2.3.1 The Board shall carry out its duties as set out in Section 5 of the SEA Act. Section 5(2) of that Act states that a supervisory authority must issue from time to time guidance as to compliance with –

- the AML/ATF Regulations;
- Part V of the POCA; and
- paragraph 1 of Schedule 1 to the ATFA.

2.3.2 These Guidance Notes are being issued in accordance with Section 5(2) of the SEA Act. Lawyers are required to comply with the AML/ATF Regulations and this Guidance when carrying out the services listed in Regulation 2 (1). The objectives of these Guidance Notes are as follows:-

- to outline the requirements of the AML/ATF legislation which applies to all professional legal advisers as defined by Regulation 2(1) of the AML/ATF Regulations;
- to outline good practice for implementing the legal requirements;
- to set out the Board's requirements for professional legal advisers undertaking business providing legal services to other persons when participating in financial or real property transactions as set out in Regulation 2(1) of the AML/ATF Regulations;
- to outline good practice in developing systems and controls to prevent lawyers from being used to facilitate money laundering and terrorist financing;
- to provide a base from which individual law firms can design and implement systems and controls and tailor their own policies and procedures for the prevention and detection of money laundering and terrorist financing;
- to ensure that Bermuda matches international standards to prevent and detect money laundering and the financing of terrorism;
- to provide direction on applying the risk-based approach effectively;
- to provide practical guidance on customer due diligence, including identification and verification of identity; and
- to provide an information resource to be used in training and raising awareness of money laundering and terrorist financing.

2.3.3 Where an affiliated company of a law firm is an AML/ATF regulated financial institution as defined by Section 2(1) of the AML/ATF Regulations reference should be made to the Guidance Notes for AML/ATF regulated financial institutions issued by the Bermuda

Monetary Authority ("BMA") when drawing up policies and procedures for the prevention of and detection of money laundering and the financing of terrorism.

2.3.4 This Guidance is intended for use by senior management and compliance staff of a firm to assist in the development of systems and controls, and detailed policies and procedures. These Guidance Notes are not intended as an internal procedures manual or to provide an exhaustive list of systems and controls to counter money laundering and terrorist financing. In applying the Guidance Notes, a firm should adopt an appropriate risk based approach and should always consider what additional measures might be necessary to prevent its exploitation, and that of its services, by persons seeking either to launder money or to finance terrorism.

2.4 Application of the AML/ATF Regulations

2.4.1 The AML/ATF Regulations came into effect for all law firms that are independent professionals pursuant to Regulation 2 (1) of the AML/ATF Regulations on August 15, 2012.

2.4.2 The AML/ATF Regulations only apply to certain activities of independent professionals and these are set out in Regulation 2(1) of the AML/ATF Regulations. In terms of activities covered it should be noted that:

- managing client monies is narrower than handling it; and

- operating or managing a bank account is wider than simply opening a client account. It would be likely to cover lawyers acting as a trustee, power of attorney, or receiver.

2.5 The Board has confirmed that the following would not generally be regarded as participating in business falling within the services described in the definition of "independent professional" in Regulation 2(1):

2.5.1 Payment on account of costs to a legal professional or payment of a lawyer's bill.

2.5.2 In respect of payments on account of costs, law firms should ensure that the payment is proportionate to the issue in respect of which the firm is asked to advise upon.

2.5.3 In respect of payment of a lawyer's bill, if the lawyer knowing that any property is or in whole or in part directly, or indirectly, represents the proceeds of criminal conduct or suspects that the payment is made out of the proceeds of criminal conduct, this would constitute an offence under Section 45 of the POCA

2.5.4 Provision of legal advice

2.5.4.1 In relation to the provision of legal advice, a lawyer needs to consider whether they are providing legal advice or whether they are a lawyer participating in a transaction by assisting in its planning or its execution. Ultimately, each case will have to be decided on its own facts and it is a matter for each firm to form a view.

2.5.4.2 However, generally, the giving of generic advice, or advice specific to a transaction in terms of whether such a transaction is possible under Bermuda law or what factors are taken into account in making such a transaction possible, will only constitute the giving of legal advice where the decision has not already been taken to proceed with the transaction.

2.5.4.3 Where a decision is made to proceed with a transaction set out in Regulation 2(1) of the AML/ATF Regulations, drafting documentation to enable that transaction to proceed, or seeking information to advise further on the planning or execution of the transaction will fall within the scope of the AML/ATF Regulations.

2.5.4.4 Participation in litigation or a form of alternative dispute resolution.

2.5.4.5 The following guidance should be taken into account:

2.5.4.6 In relation to litigation involving trusts where the proposed resolution includes a change in trusteeship or the application related to asking the Court to approve a future transaction, then the requirements of the AML/ATF Regulations may apply;

2.5.4.7 In respect of advising insolvency practitioners relating to individuals or entities, the requirements of the AML/ATF Regulations may apply.

2.5.4.8 Will Writing

In relation to Will writing, any steps taken during the lifetime of the deponent of the Will to enable their wishes to be given effect to as recorded in the Will, may well fall within the definition of Regulation 2(1) of the AML/ATF Regulations in which case the requirements of the AML/ATF Regulations will apply.

2.5.5.0 Publicly funded work

2.5.5.1 Publicly funded work extends to individuals under the legal aid scheme, even if an individual may be required to make a contribution to the fees of the law firm.

2.6 Penalties for Non-compliance

2.6.1 In determining whether to impose a penalty on a firm that has failed to comply with the requirements of the AML/ATF Regulations, the Board must consider whether the firm followed any relevant guidance which was issued at the time by the designated professional body. The sanctions for failing to comply with the AML/ATF Regulations may include civil penalties up to $250,000.00 and publication of the decision to impose the penalty pursuant to Sections 30I and 30K of the SEA Act.

2.6.2 Similarly, in determining whether a person has committed certain offences under POCA, for example section 46 (2) of the POCA (the offence of failing to disclose knowledge or suspicion of money laundering), the Supreme Court is required to take account of the

guidance provided herein.[1] The sanctions for failing to comply with section 46(2) may be an unlimited fine or up to ten years imprisonment, or both. The sanction for failing to comply with section 9(3) of ATFA (the offence of failing to disclose information) may be a fine of $100,000.00 or up to five years imprisonment, or both.

2.6.3 Nevertheless, these Guidance Notes are not a substitute for the law and compliance with them is not of itself a defence to offences under the AML/ATF legislation. However, courts will generally have regard to regulatory guidance when considering the standards of a professional person's conduct and whether they acted reasonably, honestly, and appropriately, and took all reasonable steps and exercised necessary due diligence to avoid committing the offence.

2.6.4 The consequences of non-compliance with the AML/ATF regulatory regime could include an investigation by the Board and the imposition of regulatory sanctions by the Board and the Bar.

[1] Section 49M of POCA

INTERNAL SYSTEMS AND CONTROLS

Regulation 16

3.1 Corporate governance is the system by which businesses are directed and controlled and the business risks managed. For lawyers, money laundering and terrorist financing are risks that must be managed in the same way as other business risks. These Guidance Notes describe the requirements for a law firm's general framework of systems and controls to manage the risk of money laundering and terrorist financing, and refers to the way in which those systems and controls are to be implemented into the day-to-day operation of the firm's business as policies and procedures.

3.2 Although the Board acknowledges that the legislation only brings within its scope the relevant business of law firms as specified in Regulation 2(1) of the AML/ATF Regulations, the AML/ATF legislation and the general offences and penalties cover all persons and all business activities within Bermuda. However, a law firm that does not undertake a significant amount of regulated activity (as defined in Regulation 2(1) of the AML/ATF Regulations) may wish to assess its money laundering and terrorist financing risks on an individual client and/or engagement basis and apply risk-based systems and controls when necessary. See Section 4 on Risk Based Approach for further guidance.

3.3 In accordance with Regulation 16 (1) of the AML/ATF Regulations a law firm must establish and maintain appropriate and risk sensitive policies and procedures relating to

- customer due diligence measures and ongoing monitoring;
- reporting;
- recordkeeping;
- internal control;
- risk assessment and management;

- the monitoring and management of compliance with and the internal communication of such policies and procedures in order to prevent activities related to money laundering and terrorist financing.

3.4 A law firm must establish and maintain systems and controls to prevent and detect money laundering and terrorist financing, that enable the business to:

- apply appropriate client due diligence ("**CDD**") policies and procedures that take into account vulnerabilities and risk which should include:
- the development of clear client acceptance policies and procedures; and
- indentifying and verifying the identity of the client;
- monitor and review instances where exemptions are granted to policies and procedures, or where controls are overridden;
- report to the Financial Intelligence Agency ("FIA") when it has knowledge or suspicion that another person is involved in money laundering or terrorist financing, including attempted transactions;
- ensure that relevant employees are adequately screened when they are initially employed, aware of the risks of becoming concerned in arrangements involving criminal money and terrorist financing, aware of their personal obligations and internal policies and procedures concerning measures to combat money laundering and terrorist financing, and provided with appropriate training;
- keep records in accordance with the AML/ATF Regulations; and
- monitor compliance by overseas branches and subsidiaries with policies and procedures.

3.5 A firm must have policies and procedures in place to address any specific risks associated with client relationships established where the client is not physically present for identification purposes (i.e. non-face to face).

3.6 A firm must ensure that the systems and controls are implemented and operating effectively. For systems and controls (including policies and procedures) to be effective, they will need to be both appropriate to the size and business of the firm and aligned with the risk profile of the firm. In addition, the firm would need to take appropriate measures to guard against the use of technological developments in money laundering or terrorist financing schemes. In particular, there should be policies and procedures in place to address specific risks associated with non-face to face business relationships or transactions, which should be applied when conducting due diligence procedures.

3.7 Issues which may be covered in an internal controls system include:

- the level of personnel permitted to exercise discretion on the risk-based application of regulations, and under what circumstances;
- CDD requirements to be met for simplified, standard and enhanced due diligence;
- when outsourcing of CDD obligations or reliance on third parties will be permitted, and on what conditions;
- how the firm will restrict work being conducted on a file where CDD has not been completed;
- the circumstances in which delayed CDD is permitted;
- when cash payments will be accepted;

- when payments will be accepted from or made to third parties;

- the manner in which disclosures are to be made to the Reporting Officer.

3.8 The firm may demonstrate that it has considered the effectiveness of the firm's risk management systems and controls where it, for example:

- receives regular and timely information relevant to the management of the firm's money laundering and terrorist financing risks;
- considers the adequacy of the management of the firm's money laundering and terrorist financing risks;
- monitors the on-going competence and effectiveness of the Compliance Person ("CP") and the Reporting Officer;
- considers the adequacy of resources to ensure effective compliance with the AML/ATF legislation, the Act and by extension this Guidance;
- periodically reviews the adequacy of policies and procedures for higher risk clients;
- considers the adequacy of policies and procedures in place where CDD information and documentation is held by third parties such as group entities, outsourcing service providers, introducers and intermediaries;
- considers whether the incidence of suspicious activity reports (or absence of such reports) has highlighted any deficiencies in the firm's CDD, monitoring or internal or external suspicious activity reporting policies and procedures, and whether changes are required to address any such deficiencies;
- takes into account changes made or proposed in respect of new legislation, regulatory requirements or guidance, or as a result of changes in business activities; and

- considers whether inquiries have been made by the FIA, or production orders received, without issues having previously being identified by CDD or reporting policies and procedures.

3.9 The implementation of systems and controls for the prevention and detection of money laundering and the financing of terrorism does not obviate the need for a firm to address cultural barriers that can prevent effective control. Human factors, such as the inter-relationships between different employees within a firm, and between employees and clients, can result in the creation of damaging barriers.

3.10 Unlike systems and controls, the prevailing culture of an organisation is intangible. As a result, its impact on the firm can sometimes be difficult to measure. The risk that cultural barriers might prevent the operation of effective systems and controls to prevent and detect money laundering and the financing of terrorism may be minimized by senior management considering the prevalence of the following factors:

- an assumption on the part of more junior employees that their concerns or suspicions are of no consequence;
- negative handling by partners or fee earners of queries raised by more junior employees regarding unusual, complex or higher risk activity and transactions;
- an unwillingness on the part of fee earners or other employees to subject high value (and therefore important) clients to effective CDD checks;
- pressure applied by senior management or fee earners outside Bermuda upon employees in Bermuda to conduct transactions without first obtaining all relevant CDD;
- excessive pressure applied on fee earners to meet aggressive revenue-based targets, or where employee or fee earner remuneration or bonus schemes are exclusively linked to revenue-based targets;

- the familiarity of fee earners or other employees with certain clients resulting in unusual, complex, or higher risk activity and transactions within such relationships not being identified as such;
- the inability of employees to understand the commercial rationale for client relationships, resulting in a failure to identify non-commercial enterprises and therefore potential money laundering and terrorist financing activity;
- a tendency for management to discourage employees from raising concerns due to lack of time and/or resources, preventing any such concerns from being addressed satisfactorily;
- an excessive desire on the part of employees to provide a confidential and efficient client service; and
- non-attendance of partners or other members of management at anti-money laundering and terrorist financing training sessions on the basis of mistaken belief that they cannot learn anything new or because they have too many other competing demands on their time.

3.11 Lawyers may outsource their systems and controls and processing to other jurisdictions or to other companies outside Bermuda within their group of companies. However, a law firm cannot contract out of their legal obligations and as such they remain responsible for the systems and controls which have been outsourced and as such must actively manage the risk to the firm that this activity represents.

In particular, where operational activities are undertaken by staff in other jurisdictions those staff should be subject to the same AML/ATF policies and procedures applicable to the Bermuda firm and internal reporting procedures implemented to ensure all suspicions related to Bermuda related accounts, transactions or activities are reported to the Reporting Officer in Bermuda.

Where the AML/ATF regulations and reporting requirements in another jurisdiction are not equivalent to those in Bermuda the Bermuda standard must be applied and adhered to.

3.12 All law firms must appoint a Reporting Officer who is responsible for receiving disclosures under section 46 of POCA and Schedule 1 Part 1 of ATFA and deciding on whether those disclosures should be reported to the FIA. Section 8 deals more comprehensively with Suspicious Activity Reporting.

RISK BASED APPROACH

Regulation 6(3)

4.1 The possibility of being used to assist with money laundering and terrorist financing poses many risks for law firms including:

- criminal prosecution under the AML/ATF legislation;
- disciplinary sanctions imposed by Bar Council and/or the Board;
- civil liability under the SEA Act; and
- damage to reputation leading to loss of business.

4.2 These risks must be identified, assessed and mitigated in the same way as for all business risks faced by a firm. Firms should develop a risk profile for their business which:

- recognises that the money laundering and terrorist financing threats to a firm vary across clients, jurisdictions, services and delivery channels;
- allows a firm to differentiate between clients in a way that matches risk in a particular business;
- while establishing minimum standards, allows a firm to apply its own approach to systems and controls, and other arrangements in particular circumstances; and
- helps to produce a more cost effective system.

4.3 It must be accepted that applying a risk based approach will vary between firms. Regulation 6 (3) of the AML/ATF Regulations requires that a relevant person must:

- determine the extent of customer due diligence measures on a risk sensitive basis depending on the type of client, business relationship, or transaction; and

- be able to demonstrate to its supervisory authority that the extent of customer due diligence measures is appropriate in view of the risks of money laundering and terrorist financing.

4.4 The AML/ATF Regulations require a firm to conduct (and keep up to date) a risk assessment, which considers the firm's activities and structure and concludes on the business' exposure to money laundering and terrorist financing risk. The AML/ATF Regulations also require a firm to use the outcome of this risk assessment in the development of appropriate risk management systems and controls, and the business' policies and procedures.

In particular, a firm is required to develop CDD procedures that take into account risk, and to apply enhanced CDD procedures (also referred to as Enhanced Due Diligence or "EDD") to higher risk client relationships, and simplified CDD (also referred to as Simplified Due Diligence or "SDD") procedures low risk client relationships.

Firms can decide for themselves how to carry out their risk assessment, which may be simple or sophisticated depending on the nature of the firm and its business. Where the business is simple, involving few practice areas, with most clients falling into similar categories, a simple approach may be appropriate for most clients, with the focus being on those clients that fall outside the norm.

4.5 Systems and controls will not detect and prevent all money laundering or terrorist financing. A risk-based approach will, however, serve to balance the cost burden placed on individual firms and on their clients with a realistic assessment of the threat of a firm being used in connection with money laundering or terrorist financing by focusing effort where it is needed and has most impact.

An effective and documented risk-based approach will enable a firm to justify its position on managing money laundering and terrorist risks to law enforcement, the courts, regulators and supervisory bodies.

4.6 The risk-based approach does not apply to reporting suspicious activity. The AML/ATF Regulations lay down specific legal requirements not to engage in certain activities and to make reports of suspicious activities once a suspicion is held. However, the risk-based approach does apply to ongoing monitoring of clients and retainers which enable firms to identify suspicions.

Taking into account the conclusions of the risk assessment, senior management must organise and control its affairs effectively and be able to demonstrate the existence of adequate risk management systems and controls. A firm may extend its existing risk management systems to address money laundering and terrorist financing risks.

The risk assessment will depend on the firm's size, type of clients and the practice area it engages in. In particular, a firm should consider the following risk factors:

4.7 **Client risk** - A firm's client geographical diversity can affect the risk of money laundering or terrorist financing. Factors which may vary the risk level include whether a firm:

- acts for politically exposed persons ("PEPs");
- acts for clients without meeting them;
- practices in locations with high levels of acquisitive crime, or for clients who have convictions for acquisitive crimes, which increases the likelihood the client may possess criminal property;
- acts for clients affiliated to countries with high levels of corruption or organized crime, or where terrorist organisations operate, or countries with inadequate frameworks to prevent and detect money laundering and the financing of terrorism;
- acts for clients that it is, or is not, easy to obtain details of beneficial owners for;
- acts for entities that have complex ownership structures

Additional factors to consider are:

- Nature and scope of business activities generating the funds/assets. For example, a client conducting "sensitive" activities (as defined by the Board), engaged in higher risk trading activities or engaged in a business which involves significant amounts of cash may indicate higher risk;
- Transparency of client. For example, persons that are subject to public disclosure rules, e.g. on exchanges or regulated markets (or majority-owned and consolidated subsidiaries of such persons), or subject to licensing by a statutory regulator, e.g. the Bermuda Stock Exchange, or BMA may indicate lower risk. Clients where the structure or nature of the entity or relationship makes it difficult to identify the true beneficial owners and controllers may indicate higher risk;
- Secretive clients. Whilst face to face contact with clients is not always necessary or possible, an excessively obstructive or secretive client may be a cause for concern;
- Reputation of client. For example, a well known, reputable company, with a long history in its industry, and with abundant independent information about it and its beneficial owners and controllers may indicate lower risk;
- Behaviour of client. For example, where there is no commercial rationale for the service that is being sought, or where undue levels of secrecy are requested, or where it appears that an "audit trail" has been deliberately broken or unnecessarily layered, may indicate higher risk;
- The regularity or duration of the relationship. For example, longstanding relationships involving frequent client contact that result in a high level of understanding of the client relationship may indicate lower risk;

4.8 Service risk - Firms should consider the different types of risk to which they are exposed within the different service areas that they provide. Some services and areas of law provide greater opportunities to facilitate money laundering or terrorist financing. For example:

- complicated financial or property transactions;

- providing assistance in setting up trusts or company structures which could be used to obscure ownership of property;
- payments that are made to, or received from, third parties;
- payments made by cash; and
- transactions with a cross-border element.

The risks should be considered within the context that a firm may be used to launder funds or assets through the firm. Factors may include:

- the firm directly handling cash, assets or through payments that are made to, or received from, third parties; or
- the firm directly handling the financial affairs, setting up companies, trusts or other structures for politically exposed persons that may be used to obscure beneficial ownership.

4.9 **Delivery channels risk** – Firms should consider how they interact with their clients and the channels through which it delivers its services to them. Factors may include:

- the firm acting for clients without meeting them in person; or
- accepting a client through another firm referral or engagement (such as through an appointed law firm).

4.10 **Geographical areas of operation risk** – Business activity in locations with high levels of acquisitive crime, or for clients who have convictions for acquisitive crimes, which increases the likelihood the client may possess criminal property. Factors may include:

- acting for clients affiliated to countries with high levels of corruption or organized crime, or where terrorist organisations operate, or countries with inadequate frameworks to prevent and detect money laundering and the financing of terrorism; and

- in assessing which jurisdictions may present a higher risk, objective data published by the International Monetary Fund ("IMF"), Financial Action Task Force ("FATF"), World Bank, the Egmont Group of Financial Intelligence Units, US Department of State ("International Narcotics Control Strategy Report"), Office of Foreign Assets Control ("OFAC") and Transparency International (Corruption Perception Index) will be relevant.

4.11 A firm may demonstrate that it has considered its exposure to money laundering and terrorist financing risk by:

- Involving all members of senior management in determining the risks posed by money laundering and terrorist financing within those areas for which they have responsibility;

- Considering organizational factors that may increase the level of exposure to the risk of money laundering and terrorist financing, e.g. business volumes and outsourced aspects of regulated activities or compliance functions;

- Considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation;

- Considering who its clients are and what they do;

- Considering whether any additional risks are posed by the jurisdictions with which the firm or its clients (including intermediaries and introducers) are connected;

- Considering how the firm establishes and delivers services to its clients. For example, risks are likely to be greater where relationships may be established remotely; and

- Considering the characteristics of its service areas and assessing the associated vulnerabilities posed by each service area, including delivery channels. For example:

- the use of third parties such as group entities, introducers and intermediaries to conduct elements of the CDD process; or
- assessing how legal entities and structures might be used to mask the identities of the underlying beneficial owners.

4.12 Firms should prepare a risk profile for clients based on the type of instructions it has received. A client profile should contain sufficient information to enable it to:

- identify a pattern of expected business activity and transactions within each client relationship; and

- identify unusual, complex or higher risk activity and transactions that may indicate money laundering or terrorist financing activity.

4.13 One of the factors to be taken into account in undertaking any risk assessment for a client is whether or not the client is acting for a third party – as an intermediary. One or more of the following factors will be relevant when conducting a risk assessment for an introducer or intermediary:

- the stature and regulatory track record of the intermediary or introducer;
- the adequacy of the framework to combat money laundering and terrorist financing in place in the jurisdiction in which the intermediary or introducer is based;
- the adequacy of the supervisory regime to combat money laundering and terrorist financing to which the intermediary or introducer is subject;
- the adequacy of the measures to combat money laundering and terrorist financing in place at the intermediary or introducer;
- previous experience gained from existing relationships connected with the intermediary or introducer;
- the nature of the business conducted by the intermediary or introducer. In this case relevant factors include:
- the geographic location of the client base;
- the general nature of the client base, e.g. whether institutional or private client;
- the risk appetite of the intermediary or introducer;

- the nature of the services which the intermediary or introducer provides to its clients;
- whether relationships are conducted by the intermediary or introducer on a face to face basis;
- whether specific relationships are fully managed by the intermediary or introducer; and
- the extent to which the intermediary or introducer itself relies on third parties to identify its clients and to hold evidence of identity or to conduct other due diligence procedures, and whether such third parties are financial services businesses that are overseen for AML/ATF compliance in Bermuda or carry out an equivalent business. Whether or not specific intermediary or introduced relationships involve PEP's or other higher risk relationships.

4.14 A firm should conduct (and keep up to date) a risk assessment, which considers the firm's exposure to money laundering and terrorist financing risk and then use the outcome of this risk assessment in the development of appropriate risk management systems and controls, and the firm's policies and procedures. In particular, a firm is required to develop CDD procedures that take into account risk, and to apply enhanced CDD procedures (also referred to as Enhanced Due Diligence or "EDD") to higher risk client relationships, and simplified CDD (also referred to as Simplified Due Diligence or "SDD") procedures low risk client relationships.

Firms can decide for themselves how to carry out their risk assessment, which may be simple or sophisticated depending on the nature of the firm and its business. Where the business is simple, involving few service lines, with most clients falling into similar categories, a simple approach may be appropriate for most clients, with the focus being on those clients that fall outside the norm.

4.15 A firm may demonstrate that it has considered the business' exposure to money laundering and terrorist financing risk by:

- involving all members of senior management in determining the risks posed by money laundering and terrorist financing within those areas for which they have responsibility;
- considering organisational factors that may increase the level of exposure to the risk of money laundering and terrorist financing, e.g. business volumes and outsourced aspects of regulated activities or compliance functions;
- considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation;
- considering who its clients are and what they do;
- considering whether any additional risks are posed by the jurisdictions with which the firm or its clients (including intermediaries and introducers) are connected; and
- considering the characteristics of the services and areas of law that it offers and assessing the associated vulnerabilities posed by each service or area, including delivery channels. For example:
- the use of third parties such as group entities, introducers and intermediaries to conduct elements of the CDD process;
- assessing how legal entities and structures might be used to mask the identities of the underlying beneficial owners; or
- considering how the firm establishes and delivers services to its clients. For example, risks are likely to be greater whether relationships may be established remotely (non face-to-face).

4.16 The following sub-sections set out some key legal service area vulnerabilities drawn from FATF and law enforcement guidance and case studies, and some key warning signs that have been drawn up by the Law Society for England and Wales, as an indication of service area vulnerabilities:

4.16.1 Use of client accounts

Lawyers should not provide a banking service for their clients. However, it can be difficult to draw a distinction between holding client money for a legitimate transaction and acting more like a bank. For example, when the proceeds of a sale are left with a firm to make payments, these payments may be to mainstream lending companies, but these may also be to more obscure recipients, including private individuals, whose identity is difficult or impossible to check.

The following situations could give rise to cause for concern:

- a client deposits funds into a firm's client account, but then ends the transaction for no apparent reason;
- a client advises that funds are coming from one source and at the last minute the source changes; or
- a client unexpectedly requests that money received into a firm's client account be sent back to its source, to the client or to a third party.

Firms should think carefully before disclosing client account details as this allows money to be deposited into a client account without the firm's knowledge. If it is necessary to provide account details, firms should ask the client where the funds will be coming from. Will it be an account in their name, from Bermuda or another jurisdiction? Firms should consider whether they are prepared to accept funds from any source they are concerned about.

Circulation of client account details should be kept to a minimum. Clients should be discouraged from passing the details on to third parties and should be asked to use the account details only for previously agreed purposes.

4.16.2 Establish a policy on handling cash

It is good practice to establish a policy of not accepting cash payments above a certain limit either at the firm's office or into the firm's bank account. Clients may attempt to circumvent such a policy by depositing cash directly into a client account at a bank. Firms may consider advising clients in such circumstances that they might encounter a delay in completion of the final transaction. Avoid disclosing client account details as far as possible and make it clear that electronic transfer of funds is expected.

4.16.3 Source of funds

Accounts staff should monitor whether funds are from credible sources. For example, it is reasonable for monies to be received from a company if your client is a director of that company and has the authority to use company money for the transaction.

However, if funding is from a source other than a client, firms may need to make further enquiries, especially if the client has not advised what they intend to do with the funds before depositing them into the firm's account. If it is decided to accept funds from a third party, perhaps because time is short, firms should ask how and why the third party is helping with the funding.

Enquiries do not need to be made into every source of funding from other parties. However firms must always be alert to warning signs and in some cases will need to seek more information. In some circumstances, cleared funds will be essential for transactions and clients may want to provide cash to meet a completion deadline. Firms should assess the risk in these cases and ask more questions if necessary.

4.16.4 Private client work – Administration of Estates

A deceased person's estate is very unlikely to be actively utilised by criminals as a means for laundering their funds; however, there is still a low risk of money laundering for those working in this area where estate assets have been earned or are located in a higher risk territory, firms may need to make further checks about the source of those funds.

When winding up an estate, there is no blanket requirement that firms should be satisfied about the history of all the funds which make up the estate under administration; however where estate assets have been earned in a foreign jurisdiction, firms should be aware of the wide definition of criminal conduct in the POCA.

Firms should be alert from the outset and monitor throughout so that any disclosure can be considered as soon as knowledge or suspicion if formed and problems of delayed consent can be avoided.

Firms should bear in mind that an estate may include criminal property. An extreme example would be where the firm knows or suspects that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime. If firms know, or suspect that the deceased person improperly claimed benefits/allowances or had evaded the due payment of taxes during their lifetime, criminal property will be included in the estate and so a money laundering disclosure may be required.

Relevant local laws will apply before assets can be released. For example, a grant of probate will normally be required before assets can be released. Firms should remain alert to warning signs, for example if the deceased or their business interests are based in a higher risk jurisdiction. If the deceased person is from another jurisdiction and a lawyer is dealing with the matter in the home country, firms may find it helpful to ask that person for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate. The issue of the tax payable on the estate may depend on the jurisdiction concerned.

4.16.5 Charities

While the majority of charities are used for legitimate reasons, they can be used as money laundering/terrorist financing vehicles. Firms acting for charities should consider its purpose and the organisations it is aligned with. If money is being received on the charity's behalf

from an individual or a company donor, or a bequest from an estate, firms should be alert to unusual circumstances including large sums of money.

4.16.6 Property transactions

Criminal conduct generates huge amounts of illicit capital and these criminal proceeds need to be integrated into personal lifestyles and business operations. The Police advise that property purchases are one of the most frequently identified methods of laundering money. Property can be used either as a vehicle for laundering money or as a means of investing laundered funds. Criminals will buy property both for their own use, e.g. as principal residencies or second homes, business or warehouse premises and as investment vehicles to provide additional income.

The purchase of real estate is commonly used as part of the last stage of money laundering. Such a purchase offers the criminal an investment which gives the appearance of financial stability. The purchase of a restaurant or hotel, for example, offers particular advantages, as it is often a cash-intensive business, which is the preferred currency of the criminals. Retail businesses provide a good front for criminal funds where legitimate earnings can be used as a front for the proceeds of crime.

4.16.7 Criminal use of conveyancing services

Law enforcement advises that of all the services offered by legal practitioners, conveyancing is the most utilised function by criminal groups. Conveyancing is a comparatively easy and efficient means to launder money with relatively large amounts of criminal monies 'cleaned' in one transaction. In a stable or rising property market, the launderer will incur no financial loss except fees. Conveyancing transactions can also be attractive to money launderers who are attempting to disguise the audit trail of the proceeds of their crimes, as the property itself can be 'criminal property' for the purposes of the POCA can still be involved in money laundering even if no money changes hands.

Corrupt lawyers may employ trainees to perform the conveyancing work from criminal groups, thereby distancing themselves from the criminal aspect of the business. Conveyancers should also be alert to instructions which are a deliberate attempt to avoid assets being dealt within the way intended by the court or through the usual legal process. For example, lawyers may sometimes suspect that instructions are being given to avoid the property forming part of a bankruptcy, or forming part of assets subject to confiscation.

4.16.8 Ownership issues

Properties owned by nominee companies or multiple owners may be used as money laundering vehicles to disguise the true owner and /or confuse the audit trail. Firms should be alert to sudden or unexplained changes in ownership.

Another potential cause for concern is where a third party is providing the funding for a purchase, but the property is being registered in someone else's name. There may be legitimate reasons for this, such as a family arrangement, but firms should be alert to the possibility of being misled about the true ownership of the property. Further CDD measures should be undertaken on the person providing the funding.

4.16.9 Methods of funding

Many properties are bought with a combination of deposit, mortgage and/or equity from a current property. Usually, the lawyer acting for the purchaser will have information about how the client intends to fund the transaction. Lawyers should expect to be updated if those details change, for example, if a mortgage falls through and new funding is obtained.

Firms should remember that payments made through the mainstream banking system are not guaranteed to be clean.

Transactions that do not involve a mortgage or are not being financed wholly from the sale of a previous property have a higher risk of being fraudulent. Firms should be alert for large

payments from private funds, especially if the client receives payments from a number of individuals or sources. If concerns arise;

- the client should be asked to explain the source of funds. Firms should assess whether the explanation appears to be valid - e.g. the money has been received from an inheritance;
- ensure that the client is the beneficial owner of the funds being used in the purchase.

Third parties often assist with purchases and firms may be asked to receive funds directly from third parties, for example relatives often assist first time buyers. Consideration will need to be given as to the extent of due diligence that needs to be undertaken on those third parties. Firms should consider whether there are any obvious warning signs and what needs to be known about:

- the client;
- the third party;
- their relationship; and
- the proportion of the funding being provided by the third party.

Firms should consider their obligations to the lender in these circumstances – firms are normally required to advise lenders if the buyers are not funding the balance of the price from their own resources.

4.16.10 Valuations

An unusual sale price can be an indicator of money laundering. Whilst lawyers acting in a property sale are not required to get independent valuations, if a firm becomes aware of a significant discrepancy between the sale price and what a property would reasonably be asked to sell for, consideration should be given to asking more questions.

Properties may also be sold below the market value to an associate, with a view to obscuring the title to the property which the original owner still maintains the beneficial ownership.

4.16.11 Mortgage fraud

A firm may discover or suspect that a client is attempting to mislead a lender client to improperly inflate a mortgage advance – for example, by misrepresenting the borrower's income or because the seller and buyer are conspiring to overstate the sale price. Transactions which are not at arm's length may warrant particular consideration. However, until the improperly obtained mortgage advance is received, there is not any criminal property for the purposes of disclosure to the FIA.

Sometimes fraud is achieved by selling the property between related private companies. The transactions will involve inflated values and will not be at arm's length. Increasingly, offshore companies are used with the property sold several times within the group before approaching a lender for a mortgage at an inflated value.

Firms that discover or suspect that a mortgage advance has already been improperly obtained should consider advising the mortgage lender.

Firms acting in a connection with a mortgage who discover or suspect that a previous mortgage has been improperly obtained may need to advise the lender, especially if the new mortgage is with the same lender. Consideration should also be given to making a disclosure to the FIA as the improperly obtained mortgage advance represents criminal property.

If a client has made a deliberate misrepresentation on their mortgage application, it is likely that the crime/fraud exemption to legal professional privilege will apply. This means that no waiver of confidentiality will be needed before a disclosure is made. However, such matters will need to be dealt with on a case-by-case basis.

4.16.12 Company and commercial work

The nature of company structures can make them attractive to money launderers because it is possible to obscure true ownership and protect assets for relatively little expense. For this reason, lawyers working with companies and in commercial transactions should remain alert throughout their retainers, with existing as well as new clients.

A common operating method amongst serious organized criminals is the use of front companies. These are often used to disguise criminal proceeds as representing the legitimate profits of fictitious business activities. They can also help to make the transportation of suspicious cargoes appear as genuine goods being traded. More often than not, they are used to mask the identity of the true beneficial owners and the source of criminally obtained assets. Corporate vehicles are also frequently used to help commit tax fraud, facilitate bribery/corruption, shield assets from creditors, facilitate fraud generally or circumvent disclosure requirements.

The lack of transparency concerning the ownership and control of corporate vehicles has proved to be a consistent problem for money laundering investigations. Corporations serving as directors and nominee directors can be used to conceal the identity of the natural persons who manage and control a corporate vehicle.

Several international reports have highlighted the extent to which private limited companies, nominees, front companies, and special purpose vehicles have been used in laundering operations. Case studies submitted to the FATF have indicated the following common elements in the misuse of corporate vehicles:

- multi-jurisdictional and/or complex structures of corporate entities and trusts;
- foreign payments without a clear connection to the actual activities of the corporate entity;
- use of offshore bank accounts without clear economic necessity;

- use of nominees; and
- tax, financial and legal advisers were generally involved in developing and establishing the structure. In some case studies a lawyer was involved and specialised in providing illicit services for clients.

The more of the above elements that exist, the greater the likelihood and the risk that the identity of the underlying beneficial owner may be able to remain unidentifiable.

4.16.13 Shell Corporation

The shell corporation is a tool that appears to be widely used by criminals. Often purchased "off-the-shelf" it remains a convenient vehicle for laundering money and form concealing the identity of the beneficial owner of the funds. The company records are often more difficult for law enforcement to access because they are held behind a veil of professional privilege or the professionals who run the company act on instructions remotely and anonymously.

Shell companies are often used to receive deposits of cash which are then transferred to another jurisdiction, to facilitate false invoicing or to purchase real estate and other assets. They have also been used as the vehicle for the actual predicate offence of fraud on many occasions.

4.16.14 Bearer Shares

Bearer shares confer rights of ownership to a company upon the physical holder of the share. They are commonly and legitimately used in a number of countries. However, the high level of anonymity that bearer shares offer provides opportunities for misuse where the identity of the shareholder is not recorded when the share is issued and transferred, ownership of the share is effectively anonymous.

Such shares are open to two money laundering risks:

- financial assets can be acquired without the purchaser being identified; and
- the company owners and controllers may not be capable of being identified.

To guard against misuse, a number of jurisdictions have dematerialized or immobilized bearer shares when they are registered in an effort to ensure that the identity of the beneficial owners can be verified. Dematerialisation is achieved by requiring registration upon transfer or requiring registration in order to vote or collect dividends. While physical transfer of bearer shares is possible, it is believed to be rare.

4.16.15 Holding of funds

Firms who choose to hold funds as stakeholder or escrow agent in commercial transactions should consider the checks to be made about the funds they intend to hold before the funds are received. Consideration should be given to conducting CDD measures on all those on whose behalf the funds are being held.

Particular consideration should be given to any proposal that funds are collected from a number of individuals whether for investment purposes or otherwise. This could lead to wide circulation of client account details and payments being received from unknown sources.

4.16.16 Private equity

Law firms could be involved in any of the following circumstances:

- the start-up phase of a private equity business where individuals or companies seek to establish a private equity firm (and in certain cases, become authorised to conduct investment business);
- the formation of a private equity fund;
- ongoing legal issues relating to a private equity fund; or

- execution of transactions on behalf of a member of a private equity firm's group of companies (a private equity sponsor that will normally involve a vehicle company acting on its behalf (newco)).

Generally private equity work will be considered to be low risk for money laundering or terrorist financing for the following reasons:

- private equity firms are also covered by the AML/ATF Regulations and similar legislation in equivalent jurisdictions;
- investors are generally large institutions, some of which will also be regulated for money laundering purposes;
- there are generally detailed due diligence processes followed prior to investors being accepted;
- the investment is generally illiquid and the return of capital is unpredictable; and
- the terms of the investment in the fund generally strictly control the transfer of interests and the return of funds to investors.

Factors which may alter this risk assessment include:

- where the private equity firm, fund manager or an investor is located in a jurisdiction which is not regulated for money laundering to a standard which is equivalent to the FATF recommendations;
- where the investor is either an individual or an investment vehicle itself (a private equity of funds); and
- where the private equity firm is seeking to raise funds for the first time or is approaching a large investor base.
-

4.17 Systems and controls will not detect and prevent all instances of money laundering or terrorist financing. A risk-based approach will, however, serve to balance the cost burden placed on a firm and on clients with the risk that the firm may be used in money laundering or to finance terrorism by focusing resources on higher risk areas.

In determining a risk assessment for a client, the presence of one factor to consider that might indicate higher risk will not automatically establish that a client is higher risk. Equally, the presence of one lower risk factor should not automatically lead to a determination that a client is lower risk. As set out above, the process of determining an appropriate risk assessment should take into account the absence or presence of relevant factors, whether any compensating factors apply and the CDD information held by the firm business.

Firms should keep records of decisions on the risk assessment process and CDD that was undertaken for a client, and how the category of risk was determined. Such an approach will assist firms to demonstrate that they have applied a risk based approach to CDD in a reasonable and proportionate manner.

CLIENT DUE DILIGENCE (CDD)

Regulation 5

Regulation 6

Regulation 10

Regulation 11

5.1 Regulation 5 of the AML/ATF Regulations sets out the meaning of customer due diligence. The minimum CDD measures required involve:

(a) identifying the client or prospective client and verifying the client's identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) identifying where there is a beneficial owner who is not the client, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that it knows who the beneficial owner is; and

(c) obtaining information on the purpose and intended nature of the business relationship.

5.2 Identification

A firm may demonstrate collection of relevant identification information. The identity of an individual has a number of aspects e.g. his/her given name (which of course may change), date of birth, place of birth. Other factors about an individual accumulate over time (the so-called electronic "footprint"): which will include family circumstances and addresses, employment and business career, contacts with the authorities or with other institutions and physical appearance.

The identity of a client who is not a private individual is a combination of its constitution, its business, and its legal and ownership structure.

Evidence of identity can take a number of forms. In respect of individuals, much weight is placed on so called "identity documents" such as passports and photocard driving licenses and these are often the easiest way of being reasonably satisfied as to someone's identity. It is however, possible to be reasonably satisfied as to a client's identity based on other forms of confirmation including in appropriate circumstances, written assurances from persons or organizations that have dealt with the client for some time.

A firm may demonstrate collection of relevant identification information where it requests and keeps up to date the following:

All clients (minimum)
• Legal name, any former names (such as maiden name) and any other names used; • Principal residential address; and • Date of birth • Where client is not an individual copies of constitutional documents evidencing its legal structure
Standard and higher risk: additional information
• Place of birth; • Nationality; • Sex; and • Government issued personal identification number or other government issued unique identifier.

5.3 Regulation 6(1) of the AML/ATF Regulations states that a relevant person must conduct CDD measures when it:

- establishes a business relationship (where the relationship is expected to have some duration);
- carries out occasional transactions (i.e.: one off transactions of $15,000.00 or more);
- suspects money laundering or terrorist financing; or
- doubts the veracity or adequacy of the documents or information previously obtained for the purpose of identification or verification.

5.4 Regulation 6(2) of the AML/ATF Regulations states that a relevant person must apply customer due diligence measures at appropriate times to existing clients on a risk-sensitive basis.

Regulation 6 (3) of the AML/ATF Regulations requires that a relevant person must:

(a) determine the extent of customer due diligence measures on a risk sensitive basis depending on the type of client, business relationship, or transaction; and

(b) be able to demonstrate to its supervisory authority that the extent of customer due diligence measures is appropriate in view of the risks of money laundering and terrorist financing.

5.5 Where the client is a Bermuda public authority, Regulation 10 of the AML/ATF Regulations does not require satisfactory evidence of identity to be obtained in respect of the public authority or its beneficial owners and controllers.

A public authority means any designated person or body of persons (whether corporate or unincorporated) required or authorized to discharge any public function under any Act of the Legislature of Bermuda, or under any act of the Parliament of the United Kingdom which is expressed to have effect, or whose provisions are otherwise applied, in respect of Bermuda, or under any statutory instrument.

5.6 Enhanced Due Diligence

Regulation 11(1) of the AML/ATF Regulations requires that an institution must apply enhanced customer due diligence ("EDD") measures on a risk sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. This may arise in particular situations where the client has not been physically present for identification purposes and when it is determined that a client is Politically Exposed Person ("PEP"). Where a relationship or transaction is assessed as presenting a higher risk, a firm may demonstrate that it has applied EDD to the higher risk client relationships where it undertakes one or more of the measures set out below. The nature of the measures to be applied will depend on the circumstances of the relationship or transaction and the factors leading to the client relationship being considered to be higher risk. Where a relationship or transaction involves a PEP then it must always be considered to present a higher risk.

5.6.1 Definition of PEP

A PEP is defined by Regulation 11(5), (6) and (7) of the AML/ATF Regulations as a person who is in any country or territory outside Bermuda :-

(a) an individual who is or has at anytime in the preceding year, been entrusted with prominent public functions;

(b) a person who falls in any of the categories listed in paragraph 2(1)(a) of the Schedule to the AML/ATF Regulations;

(c) an immediate family member of a person referred to in (a) above including a person who falls in any of the categories listed in 2(1)(d) of the Schedule to the AML/ATF Regulations; or

(d) a known close associate of a person referred to in subparagraph (a) including a person who falls in either of the categories listed n paragraph 2(1)(e) of the Schedule.

Individuals who have or have had a high political profile, or hold or have held public office, can pose a higher money laundering or terrorist financing risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate

individuals or entities. It does, however, put the client or the beneficial owner, into a higher-risk category.

Although under the definition of a PEP an individual ceases to be so regarded after he has left office for one year, firms are encouraged to apply a risk-based approach in determining whether they should cease carrying out appropriately enhanced monitoring of his transactions or activity at the end of this period. In many cases, a longer period might be appropriate, in order to ensure that the higher-risks associated with the individual's previous position have adequately abated.

Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, firms should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs. Prominent public functions include:

- Heads of state, heads of government, ministers and deputy or assistant ministers;
- Members of parliaments;
- Members of supreme courts, of constitutional courts or of other high level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;
- Members of the boards of central banks;
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces; and
- Members of the administration, management or supervisory bodies of State-owned enterprises.

These categories do not include middle-ranking or more junior officials.
Immediate family members include:

- A spouse;
- A partner (including a person who is considered by national law as equivalent to a spouse);
- Children and their spouses or partners; and
- Parents.

Persons known to be close associates include:

- Any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person who is a PEP; and
- Any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person who is a PEP.

For the purpose of deciding whether a person is a known close associate of a PEP, the firm needs only to have regard to any information which is in its possession, or which is publicly known. Having to obtain knowledge of such a relationship does not presuppose active research by the firm.

Firms are required, on a risk-sensitive basis, to:

- Have appropriate risk-based procedures to determine whether a client is a PEP;
- Obtain appropriate senior management approval for establishing a business relationship with such a client;
- Take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and
- Conduct on-going monitoring of the business relationship.

Risk-based procedures

The nature and scope of a particular firm's business will generally determine whether the existence of PEPs in their client base is an issue for the firm, and whether or not the firm needs to screen all clients for this purpose. In the context of this risk analysis, it would be appropriate if the firm's resources were focused in particular on transactions that are characterized by a high-risk of money laundering or terrorist financing.

Establishing whether individuals qualify as PEPs is not always straightforward and can present difficulties. Where institutions need to carry out specific checks, they may be able to rely on an internet search engine, or consult relevant reports and databases on corruption risk

published by specialized national, international, non-governmental and commercial organizations. Resources such as the Transparency International Corruption Perceptions Index, may be helpful in terms of assessing the risk. If there is a need to conduct more thorough checks, or if there is a high likelihood of a firm having PEPs for clients, subscription to a specialist PEP database may be the only adequate risk mitigation tool.

Senior management approval

Obtaining approval from senior management for establishing a business relationship does not mean obtaining approval from the Board of directors (or equivalent body), but from the immediately higher level of authority to the person seeking such approval.

On-going monitoring

Guidance on the on-going monitoring of the business relationship is given in Section 7 of these Guidance Notes.

Firms should remember that new and existing clients may not initially meet the definition of a PEP, but may subsequently become one during the course of a business relationship. The firm should, as far as practicable, be alert to public information relating to possible changes in the status of its clients with regard to political exposure. When an existing client is identified as a PEP, enhanced customer due diligence must be applied to that client.

Enhanced due diligence measures include:

- obtaining further CDD information (identification information and relationship information, including further information on the source of funds and source of wealth, from either the client or independent sources (such as the internet, public and commercially available databases));
- taking additional steps to verify the CDD information obtained;
- commissioning due diligence reports from independent experts to confirm the veracity of CDD information held;

- requiring higher levels of management approval for higher risk new client relationships;
- requiring more frequent review of client relationships;
- requiring the review of client relationships to be undertaken by the compliance function, or other employees not directly involved in managing the client relationship; and
- setting lower monitoring thresholds for transactions connected with the client relationship.

5.7 The risk of handling the proceeds of corruption, or becoming engaged in an arrangement that is designed to facilitate corruption, is greatly increased where the arrangement involves PEP. Appropriate risk based systems and controls must be put in place to determine whether a: (i) client; (ii) owner or controller of a client; or (iii) third party on whose behalf a client acts, is a PEP. Such systems and controls must recognise that clients may subsequently acquire PEP status.

5.8 A firm may demonstrate that it has appropriate systems and controls for determining whether applicants for business or clients are PEPs where it:

- establishes who are the current and former holders of prominent public functions within those higher risk countries and determines, as far as is reasonably practicable, whether or not applicants for business and clients have any connections with such individuals (including through immediate family or close associates). In determining who are the current and former holders of prominent public functions, it may have regard to information already held by the firm and to external information sources such as the United Nations ("UN"), the European Parliament, the UK Foreign and Commonwealth Office, the Group of States Against Corruption, and commercially available databases; and exercises vigilance where applicants and clients are involved in business sectors that are vulnerable to corruption such as, but not limited to, oil or

arms sales. One source of information is the Transparency International Corruption Perception Index.

5.9 A firm must have clear policies and procedures for dealing with PEPs, including:

- appropriate senior management approval to establish a relationship with a PEP and for continuing a relationship, should a subsequent connection with a PEP be identified; and
- enhanced CDD, including enhanced scrutiny and regular oversight of the relationship at appropriate senior management level.

5.10 Simplified Due Diligence

Simplified due diligence ("SDD") is defined in Regulation 10 of the AML/ATF Regulations and it means not having to apply CDD in certain circumstances where the risk of money laundering and the financing of terrorism may be lower. This means not having to identify the client or verify his identity or that of the beneficial owner where relevant nor having to obtain information on the purpose or intended nature of the business relationship. It is, however, still necessary to conduct on-going monitoring of the business relationship. Firms must have reasonable grounds for believing that the client or transaction falls within one of the categories set out in the AML/ATF Regulations and may have to demonstrate this to the Board. Clearly, for operating purposes, the firm will still need to maintain a base of information about the client.

The circumstances where SDD can be applied are where the client is:

- subject to the AML/ATF Regulations or to requirements to combat money laundering and the financing of terrorism equivalent to those in place in Bermuda and is supervised for compliance with those requirements;
- a company listed on an appointed stock exchange;

- an independent professional where the product is an account into which monies are pooled and information on the identity of the person on whose behalf monies are held is available on request to the institution acting as custodian for the account;
- a public authority in Bermuda.

5.11 Verification

All key documents (or parts thereof) used to verify identity must be understandable (i.e. in a language understood by the employees of the firm), and may be required to be translated into English.

Components of identity may be verified using the following sources:

All clients – identification verification methods
General identification information: • Current passport – providing photographic evidence of identity; • Current national identity card – providing photographic evidence of identity; or • Current driving license – providing photographic evidence of identity – where the licensing authority carries out a check on the holder's identity before issuing. Independent data sources (including electronic sources). Residential address: • Correspondence from a local government department or agency • A letter of introduction confirming residential address from: (i) a Relevant Person regulated by the BMA; (ii) a regulated Relevant Person which is operating in a well-regulated jurisdiction; or (iii) a branch or subsidiary of a group headquartered in a well-regulated jurisdiction which applies group standards to subsidiaries and branches worldwide,

and tests the application of and compliance with such standards; • Personal visit to residential address; • A bank statement or utility bill; or • One of the general identification information sources listed above.
Lower risk
Where the above general identification information sources are unavailable, identity may be verified using: • A Bermuda driving license; or • A birth certificate in conjunction with: o a bank statement or a utility bill; o documentation issued by a government source; or o a letter of introduction from a relevant person that is regulated by the BMA.

5.12 Verification methods provide evidence of identity from a number of sources. These sources may differ in their integrity, reliability and independence. For example, some identification documents are issued after due diligence on an individual's identity has been undertaken, for example passports and national identity cards; others are issued on request, without any such checks being carried out. A firm should recognize that some documents are more easily forged than others.

5.13 Additionally, verification methods incorporating photographic confirmation of client identity provide a higher level of assurance that an individual is the person who they claim to be. Where a firm is not familiar with the form of the evidence obtained to verify identity, appropriate measures may be necessary to satisfy itself that the evidence is genuine.

When applying reasonable measures to the re-verification of identity following a change in a particular aspect of identity, e.g. a change of address, a firm may apply a risk based approach which focuses on higher risk clients.

TIMING OF VERIFICATION

Regulation 8

6.1 To comply with the requirements of Regulation 8 of the AML/ATF Regulations, CDD procedures should normally be carried out before the start of a business relationship or prior to carrying out an occasional transaction. However, where there is little risk of money laundering or terrorist financing and it is necessary to enter into a relationship prior to obtaining identification evidence, then a concession is provided in respect of a business relationship (but not an occasional transaction).

A business relationship is defined in Regulation 2(1) of the AML/ATF Regulations as a business, professional or commercial relationship between a relevant person and a client which is expected by the relevant person when contact is first made between them to have an element of duration. For example a business relationship may be established once a firm undertakes to act on instructions as to the operation of that relationship, for example, by receiving and accepting signed terms of business from the client.

An occasional transaction is defined in Regulation 2(1) of the AML/ATF Regulations as a transaction (carried out other than as part of a business relationship) amounting to $15,000.00 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked.

6.2 Where urgent advice is required in the course of conducting specified business in Regulation 2 of the AML/ATF Regulations, this may be given prior to completing CDD requirements with the exception that such advice may not be given for the objective of furthering a criminal act.

A firm may complete verification of identity after the initial establishment of a business relationship if the following conditions are met:

appropriate time having regard to the degree of risk of money laundering, and taking into account the type of client, business relationship, product or transaction concerned.

- the need to perform verification of identity at a later stage is essential not to interrupt the normal conduct of business e.g. the provision of urgent advice; and

- there is little risk of money laundering or terrorist financing occurring and the verification is completed as soon as practicable after the contact is first established.

6.3 In any event, a firm must not permit final agreements to be signed or pay away funds to a third party (or to another account in the name of the client) other than to deposit the funds on behalf of the client until such time as identity has been verified.

At any time when a relevant person suspects money laundering or terrorist financing (unless agreed otherwise with the FIA) or they have doubts about the veracity or adequacy of documents, that relevant person must verify the identity of the client data or information previously obtained.

6.4 In the case of a higher risk client, an appropriate time to apply identification procedures will be:

- as soon as practicable after the risk has been assessed as high;
- when an existing standard or lower risk client instructs on a new higher risk retainer; or
- where an existing client has already been designated as higher risk.

6.5 In the case of standard and lower risk clients, an appropriate time to apply identification procedures will be:

- when a transaction of significance takes place;
- where there has been a gap in retainers of 3 years or more; or
- when the firm's client documentation standards change substantially

The verification requirements under the AML/ATF Regulations are, however, different as between a client and a beneficial owner. The identity of a client must be verified on the basis of documents, data or information obtained from a reliable and independent source. The obligation to verify the identity of a beneficial owner is for the institution to take risk-based and adequate measures so that it is satisfied that it knows who the beneficial owner is. It is up to each institution whether they make use of records of beneficial owners in the public domain (if any exist), ask their clients for relevant data or obtain the information otherwise. There is no specific requirement to have regard to particular types of evidence.

6.6 Irrespective of risk, verification procedures must always be applied to existing clients:

- where a firm suspects money laundering or terrorist financing; or

  where there are doubts about the veracity or adequacy of documents, data or information that a firm has previously obtained for the purposes of CDD.

6.7 When conducting or updating CDD measures on existing clients a firm may demonstrate that it has taken reasonable measures to apply identification procedures when other information already held on file for an existing client provides satisfactory evidence that the client is who they claim to be. Publicly available information may also confirm the information held by the firm.

6.8 A firm may delay obtaining satisfactory evidence of identity until such time as this has been collected by the introducer. However, confirmation should be received from the introducer that identification procedures are to be applied within a reasonable period of time and the firm should periodically check that this is the case.

6.9 On occasions, an individual resident abroad may be unable to provide evidence of their principal residential address using the verification methods set out above. Examples of such individuals include residents of countries without postal deliveries and few street addresses, who rely upon post office boxes or employers for delivery of mail, and residents of countries where, due to social restraints, private addresses may not be verified by personal visits.

6.10 It is essential for law enforcement purposes that a record of an individual's residential address (or details of how that individual's residential address may be reached) be recorded, so that an individual may be located by law enforcement if necessary during an investigation. As a result, it is not acceptable only to record a post office box number as an address, or to fail to take steps to verify that a residential address is valid where CDD is required.

A firm must ensure that there is a valid reason for a client being unable to satisfy its more usual verification of address requirements, and must document that reason. Where alternative methods to verify address are relied on, a relevant person must consider whether enhanced monitoring of the activity and transactions carried out by the client is appropriate.

6.11 There may also be circumstances where there is face to face contact with an individual, but where documentary evidence is to be provided at a time when the individual is not present. Regulation 11 (2) of the AML/ATF Regulations requires that where the client has not been physically present for identification purposes, the firm must take specific and adequate measures to compensate for the higher risk, for example by applying one or more of the following measures:

(a) ensuring that the client's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by an AML/ATF regulated financial institution (or equivalent institution) which is subject to equivalent Regulations;

(c) ensuring that the first payment is carried out through an account opened in the client's name with a banking institution.

6.12 Where a relationship is established or transaction conducted remotely, or where the identity of an individual is to be verified using documentary evidence when the individual is not physically present, a firm must perform an additional check to reduce the risk of identity fraud. A firm may demonstrate that the specific additional check undertaken is appropriate

where it takes into account the client risk assessment, matching the level of assurance given by the check to the risk presented by the client.

6.13 For higher risk clients where certification is relied upon, a firm may demonstrate that it has obtained appropriate verification of identity where it takes steps to check that the certifier is real, or alternatively, performs a further check to reduce the risk of identity fraud. This will guard against the risk that copy documentation provided is not a true copy of the original document and that the documentation does not correspond to the applicant whose identity is to be verified. For certification to be effective, the certifier will need to have seen the original documentation and, where documentation is to be used to provide satisfactory evidence of identity for an individual, have met the individual (where certifying evidence of identity containing a photograph). An acceptable certifier will also be subject to professional rules (or equivalent) providing for the integrity of their conduct.

6.14 Persons certifying documents must certify that:

- they have seen original documentation verifying identity and/or residential address;
- the copy of the document (which they certify) is a complete and accurate copy of that original.

6.15 The certifier must also sign and date the copy document, and provide adequate information so that he may be contacted in the event of a query. An adequate level of information to be provided by a suitable certifier would include their name, position or capacity, their address and a telephone number or email address at which they can be contacted.

Acceptable persons to certify evidence of identity may include:

- Any barrister and attorney entitled to practise as such under the Supreme Court Act 1905.
- Magistrates.
- The Registrar of the Court of Appeal or the Supreme Court.

- Officers of the Bermuda Police Service of or above the rank of Inspector.
- The manager of any bank, being an institution licensed as a bank under the Banks and Deposit Companies Act 1999.
- The Deputy Governor.
- The Secretary to the Cabinet.
- The Registrar-General.
- The Registrar of Companies.
- Customs officers as defined in the Revenue Act 1898 in the performance of their duty as such.
- Immigration officers in the performance of their duty as such.
- Justices of the Peace.

A higher level of assurance will be provided where the relationship between the certifier and the subject (individual, legal body or express trust) is of a professional rather than a personal nature.

6.16 Incomplete Identification

Where identification procedures cannot be completed, a firm must not proceed or continue with a business relationship or occasional transaction. Regulation 9 (1) of the AML/ATF Regulations provides that if a Relevant Person is unable to apply identification procedures in accordance with the AML/ATF Regulations, it shall:

(a) not carry out a transaction with or for the client through a bank account;

(b) not establish a business relationship or carry out an occasional transaction with the client;

(c) terminate an existing relationship;

(d) consider making a disclosure to the FIA

ONGOING MONITORING

Regulation 6

Regulation 7

Regulation 15

7.1 Ongoing monitoring procedures apply to all business relationships, including those with existing clients. Monitoring of existing clients will be based on the type of risk the client represents.

Regulation 7(1) of the AML/ATF Regulations requires a relevant person to conduct ongoing monitoring of a business relationship. Ongoing monitoring of a business relationship means:-

(a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the client, his business and risk profile; and

(b) so far as practicable keeping the documents, data or information obtained for the purpose of applying client due diligence measures up to date.

Regulation 6(3) of the AML/ATF Regulations applies to the duty to conduct ongoing monitoring to CDD measures.

7.2 The monitoring procedures must:

- involve a firm applying its understanding of its business (i.e. the outcome of its risk assessment) to determine the nature of usual activity and its expectations for unusual and higher risk activity and transactions;

- be designed to result in the identification of unusual and higher risk activity or transactions;

- require that, in particular, special attention is paid to specific higher risk activity, clients and transactions;
- require the examination of any unusual or higher risk activity or transaction by an appropriate person to determine the background and purpose of the activity or transaction;
- in connection with the above examination, involve the collection of additional information (where appropriate);
- establish whether there is a rational explanation (an apparent economic or visible lawful purpose) for the unusual or higher risk activity or transaction, and document these findings in writing; and
- result in appropriate action being taken as a result of the findings of the above procedures.

7.3 When conducting monitoring procedures, the following are to be considered to be higher risk activity and transactions:

- complex transactions;
- unusual large transactions;
- unusual patterns of transactions;
- activity and transactions: (i) connected with jurisdictions which do not, or insufficiently apply the FATF Recommendations; or (ii) which are the subject of UN or European Union ("EU") countermeasures;
- activity and transactions that may be conducted with persons who are the subject of UN or EU sanctions and countermeasures;
- activity or transactions with PEPs or where PEPs are connected with the client; and

- activity or transactions for clients who have not been physically present for identification purposes.

7.4 In line with enhanced due diligence requirements for higher risk clients, more intensive scrutiny of client activity and transactions may involve, for example:

- more frequent reviews and updating of CDD information;
- more regular reviews of client activity and transactions against the client's expected activity profile; and
- client reviews being conducted by persons not directly involved in managing client relationships.

7.5 The examination of unusual and higher risk activity or transactions may be conducted either by fee earners or by accounts or administration staff. In any case, a firm should ensure that the reviewer has access to relevant CDD information, and that the enquiries made and the conclusions reached by the reviewer are appropriate.

Appropriate follow up action may include:

- updating CDD information to record the results of the enquiries made;
- reviewing the appropriateness of the client risk assessment in light of the unusual activity and/or additional CDD information obtained;
- applying increased levels of monitoring to particular relationships; and
- where the activity or transaction does not have a rational explanation, considering whether the circumstances require a suspicious activity report to be submitted to the firm's Reporting Officer.

7.6 In determining the nature of the monitoring procedures that are appropriate, a firm may have regard to the following factors:

- its risk assessment;
- the size and complexity of its business;
- the nature of its legal business and services;
- whether it is possible to establish appropriate standardized parameters for unusual activity; and
- the monitoring procedures that already exist to satisfy other business needs.

7.7 Appropriate factors to consider in determining whether activity or transactions are unusual include:

- the expected frequency, size, and origin/destination of client funds or other activity for individual clients; and
- the presence of risk factors specific to the nature of the activity or matter undertaken for the client. A firm should determine risk factors based on its knowledge of its client and should have regard to typologies (whether external or developed from its own experiences) relevant to the nature of its business activities.

7.8 A firm may demonstrate that it is appropriately examining unusual and higher risk activity and transactions where it:

- reviews the identified activity/transaction in light of the client risk assessment and the CDD information that it holds;
- makes further enquiries to obtain any further information required to enable a determination as to whether the activity/transaction has a rational explanation; and

- considers the activity or transaction in the context of any other relationships connected with the client.

7.9 Risk assessment should be carried out on an ongoing basis for those clients that have been identified as high risk throughout the business relationship and for each instruction. In the case of a client relationship assessed as presenting a higher risk, a firm may demonstrate that its CDD information remains up to date where it is reviewed and updated on at least an annual basis.

7.10 In the case of other relationships, a firm may demonstrate that its CDD information remains up to date where it is reviewed and updated on a risk sensitive basis, including where additional "factors to consider" become apparent (i.e. trigger events - when taking new instructions from a client, or meeting with a client may also present a convenient opportunity to update CDD information).

A comprehensive understanding of the risk presented by a client relationship may only become evident at a later stage following the establishment of a relationship. A firm may demonstrate that its client risk assessments remain up to date where its monitoring procedures involve consideration as to the ongoing appropriateness of the client's risk assessment.

7.11 FATF Recommendation 22 states that Designated Non-Financial Businesses and Professions ("DNFBPs") should be required to apply, amongst other things, Recommendation 10 (which deals with CDD) to existing clients at appropriate times on the basis of materiality and risk. For the purposes of the AML/ATF Regulations an existing client of a firm conducting business as set out in Regulation 2(1) of the AML/ATF Regulations, means a relationship established before August 15th, 2012. CDD procedures must be applied by law firms to those existing relationships at appropriate times on or after August 15th, 2012.

7.12 Source of funds

Source of funds is the activity which generates the funds for a relationship e.g. a client's occupation or business activities. Information concerning the geographical sphere of the activities may also be relevant. Regulation 15 of the AML/ATF Regulations stipulates record keeping requirements for transaction records which require information concerning the remittance of funds also to be recorded (e.g. the name of the bank and the name and account number of the account from which the funds were remitted). This is the source of transfer and is not to be confused with source of funds. The ability to follow the audit trail for criminal funds and transactions flowing through the professional and financial sector is a vital law enforcement tool in money laundering and terrorist financing investigations.

7.13 Firms should monitor whether funds received from clients are from credible sources. If funding is from a source other than a client, a firm may need to make further enquiries. If it is decided to accept funds from a third party, perhaps because time is short, firms should ask how and why the third party is helping with the funding. In some circumstances, cleared funds will be essential for transactions and clients may want to provide cash to meet a completion deadline. Firms should assess the risk in these cases and ask more questions if necessary.

SUSPICIOUS ACTIVITY REPORTING

Regulation 17

8.1 Regulation 17 of the AML/ATF Regulations requires a relevant person to maintain internal reporting procedures to allow for reports to be made to a Reporting Officer when information comes to the attention of an employee which gives rise to knowledge or suspicion that another person is engaged in money laundering or terrorist financing. The Reporting Officer after considering the information shall disclose that information to the FIA where he knows or suspects that a person is engaged in money laundering or terrorist financing.

The provisions of Regulation 17 requiring a relevant person to maintain internal reporting procedures however do not apply to sole practitioners.

8.2 Firms are required to make a report in respect of information or any other matter that comes to them in the course of their profession or business where they know or suspect that a person is engaged in money laundering or terrorist financing.

Having knowledge means knowing the existence of certain facts. In a criminal court, it must be proved that the individual in fact knew that a person was engaged in money laundering. That said, knowledge can be inferred from the surrounding circumstances; so, for example, a failure to ask obvious questions may be relied upon by a jury to imply knowledge. The knowledge must, however, have come to the person in the course of their trade, profession, business or employment. Information that comes to the person in other circumstances do not come within the scope of S. 46 of POCA or Schedule 1 of the ATFA and therefore no obligation exists to make a report. This does not preclude a report being made should the person choose to do so.

Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, for example: "A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not"; and "Although the

creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation." Justice Nelson in the case of N2J Ltd v Cater Allen before the High Court in London cited with approval Lord Devlin's definition of suspicion in Hussein v Chong Fook Kam [1970] AC 942: "Suspicion in its ordinary meaning is a state of conjecture or surmise where proof is lacking." "I suspect but I cannot prove." Justice Nelson continued "Suspicion does not have to have a long history of misdoing before it arises. It may arise in an otherwise seamless period of good conduct from one important new piece of information." "Suspicion may be no more than a feeling based on material which may fall well short of prima facie evidence."

A transaction which appears unusual is not necessarily suspicious. Even clients with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many clients will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgment as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later,
an obligation to report then arises.

8.3 Reporting on activities outside Bermuda

The offence of money laundering, and the duty to report under POCA, apply in relation to the proceeds of any criminal conduct, wherever carried out, that would constitute an offence if it took place in Bermuda. This broad scope excludes offences which the institution, staff member or Reporting Officer knows, or believes on reasonable grounds, to have been committed in a country or territory other than Bermuda and not to be unlawful under the criminal law then applying in the country or territory concerned.
The duty to report under the ATFA applies in relation to any terrorist financing offence under Sections 5-8 of that Act, that would have been an offence under these sections of the Act had it occurred in Bermuda.

The requirement to report knowledge or suspicion of money laundering or terrorist financing also applies where a Bermuda company or Bermuda partnership conducts business outside Bermuda. Where business is conducted outside Bermuda, for example through an office in another jurisdiction, through business trips to another jurisdiction, or where functions are outsourced to another jurisdiction, or where functions are outsourced to another jurisdiction and knowledge or suspicion of money laundering or terrorist funding arises in respect of that non-Bermuda business, a report must be made to the FIA in the same way as for business conducted in Bermuda. Under the AML/ATF Regulations, where a firm conducts business pertaining to the specified activities in Section 49(5) of POCA in Bermuda, but outsources aspects of its activities to another jurisdiction, whether to a group entity or to a third party, its money laundering and terrorist financing reporting procedures must also cover those outsourced activities.

It is likely that there will also be a requirement to report the knowledge or suspicion of money laundering or terrorist financing to an overseas financial intelligence unit to avoid the commission of an offence in that jurisdiction. This is known as a dual reporting requirement.

8.4 Reporting Officer

A firm's Reporting Officer is responsible for ensuring that, when appropriate, the information or other matter leading to knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing is reported to the FIA. The decision to report or not to report must not be subject to the consent of anyone else.

A firm must ensure that the Reporting Officer:

- is employed by the firm;
- has sufficient experience and skills;
- has appropriate independence;
- has a sufficient level of seniority and authority within the business;

- has sufficient resources, including sufficient time, and (if appropriate) is supported by Deputy Reporting Officer(s);
- is able to raise issues directly with senior management;
- is fit and proper;
- maintains a record of all enquiries received from law enforcement authorities and records relating to all internal and external suspicious activity reports;
- is fully aware of both their own and the business' obligations under AML/ATF Regulations, POCA and by extension this Guidance;
- ensures that relationships are managed effectively post disclosure to avoid tipping-off any third parties; and
- acts as the liaison point with the Board/the Bar/FIA and in any other third party enquiries in relation to money laundering or terrorist financing.

8.5 Whilst the AML/ATF Regulations requires one individual to be appointed as Reporting Officer it recognizes that given the size and complexity of operations of many firms, it may be appropriate to designate an additional person ("Deputy Reporting Officer") to whom suspicious activity reports may also be made. Where a firm has appointed one or more Deputy Reporting Officers, it must ensure that the requirements set out above for the Reporting Officer are also applied to any Deputy Reporting Officer.

8.6 Where a firm has appointed one or more Deputy Reporting Officers, it must ensure that the Reporting Officer:

- keeps a record of the appointment of all Deputy Reporting Officers;
- provides support to and routinely monitors the performance of any Deputy Reporting Officer; and
- ensures that suspicious activity reports are considered and determined in an appropriate and consistent manner.

In the event that the position of Reporting Officer is expected to fall vacant, to comply with the statutory requirement to have an individual appointed to the office of Reporting Officer at all times, a firm must take action to appoint an appropriate member of senior management to the position on a temporary basis.

8.7 Reporting

Section 44 (assisting another to retain the benefit of criminal conduct) and Section 45 (acquisition, possession or use of proceeds of criminal conduct) of POCA states that where a person is concerned in an arrangement involving the proceeds of crime, or has possession of the proceeds of crime, they will not have committed an offence if the disclosure is made before he does the act concerned and the act is done with the consent of the FIA or the disclosure is made after he does the act but is made on his initiative as soon as it is reasonable for him to make it.

8.8 Section 12 of ATFA contains similar provisions in circumstances where offences would otherwise be committed under Section 5 (fund-raising), Section 6 (use and possession of property), Section 7 (funding arrangements) and Section 8 (money laundering).

8.9 Section 9 of ATFA contains an offence of failure to report knowledge or suspicion of another person's involvement in terrorist financing or money laundering (Sections 5 to 8 of ATFA), where the knowledge or suspicion arose during the course of a trade, profession, business or employment, other than in the course of a business in the regulated sector.

8.10 Schedule 1 Part 1 Section 1 of ATFA contains a further offence, where a person fails to report another person's involvement in terrorist financing or money laundering (Sections 5 to 8 of ATFA), where their knowledge or suspicion, arose during the course of business in the regulated sector.

8.11 The mental elements of knowledge and suspicion, which are relevant to statutory offences are not terms of art and are not defined within the statutes. Knowledge means actual knowledge. There is some suggestion that wilfully shutting one's eyes to the trust may amount to knowledge. However, the current general approach from the criminal courts is that nothing less than actual knowledge will suffice. Additional guidance may be found in Shah v HSBC (2012) EWHC 1283 (QB)

The term 'suspects' is one which the court has historically avoided defining; however because of its importance in English criminal law, some general guidance has been given. In the case of *Da Silva* [1996] EWCA Crim 1654, Longmore LJ stated:

'It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.'

8.12 There is no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond speculation.

The test for whether a person holds a suspicion is a subjective one. If someone thinks a transaction is suspicious, they are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. They may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. There does not have to be evidence that money laundering is taking place for there to be a suspicion.

8.13 The meaning of suspicion detailed above was also confirmed by the Court of Appeal in the case of *K v NatWest* [2006] EWCA Civ 1039.

If someone has not yet formed a suspicion, but they have cause for concern, a firm may choose to ask the client or others more questions. This choice depends on what is already known, and how easy it is to make enquiries.

If there is a belief that a client is innocent, but there are suspicions that another party to a transaction is engaged in money laundering, a firm may need to consider referring the client for specialist advice regarding the risk that they may be a party to one of the principal offences. However, whether someone has a suspicion is a matter for their own judgment.

8.14 A firm must ensure that:

- where a new or an existing client fails to supply adequate CDD information, or adequate documentation verifying identity (including the identity of any beneficial owners and controllers), consideration is given to making a SAR;

- internal reporting procedures encompass the internal recording of attempted transactions and business that has been turned away;

- employees make internal SARs containing all relevant information to the Reporting Officer (or a Deputy Reporting Officer) as soon as it is reasonable practicable after the information comes to their attention – in writing;

- SARs include as full a statement as possible of the information giving rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing activity and full details of the client;

- reports are not filtered out by supervisory staff or managers such that they do not reach the Reporting Officer (or Deputy Reporting Officer); and

- reports are acknowledged by the Reporting Officer (or a Deputy Reporting Officer).

8.15 A firm must establish and maintain arrangements for disciplining any member of staff who fails, without reasonable excuse, to make an internal SAR where they have knowledge, or suspicion of money laundering or terrorist financing.

Firms, but not sole practitioners, need to have a system clearly setting out the requirements for making an internal SAR. These may include:

- the circumstances in which a disclosure is likely to be required;
- how and when information is to be provided to the Reporting Officer or deputies;
- resources which can be used to resolve difficult issues around making a disclosure;
- how and when a disclosure is to be make to the FIA;
- how to manage a client when a disclosure is made whilst waiting for consent; and
- the need to be alert to tipping-off issues.

A firm may demonstrate that it has established and maintained appropriate arrangements for disciplining staff, where employment contracts and employment handbooks provide for the imposition of disciplinary sanctions for failing to report knowledge or suspicion.

8.16 A firm must ensure that:

- all relevant information is promptly made available to the Reporting Officer (or Deputy Reporting Officer) on request to ensure that internal SARs are properly assessed;

- each SAR is considered by the Reporting Officer (or Deputy Reporting Officer) in light of all relevant information; and

- the Reporting Officer (or Deputy Reporting Officer) documents the evaluation process following and reasons for the decision to report or not to report to the FIA.

8.17 In order to demonstrate that a report is considered in light of all relevant information when evaluating a suspicious activity report, the Reporting Officer (or Deputy Reporting Officer) may:

- review and consider transaction patters and volumes, previous patterns of instructions, the length of the business relationship and CDD information; and

- examine other connected accounts or relationships. Connectivity can arise through commercial connections, such as transactions to or from other customers or common introducers, or through connected individuals, such as third parties, common ownership of entities or common signatories. However, the need to search for information concerning connected accounts or relationships should not delay the making of a report the FIA.

8.18 Communication with the FIA

A firm must ensure that the Reporting Officer makes external SARs containing all relevant information including the provision of all the necessary documentation in support of the SAR directly to the FIA as soon as is reasonable practicable, in a format approved by the FIA. Relevant information includes:

- full details of the client and as full a statement as possible of the information giving rise to knowledge or suspicion. It will be particularly important to provide as comprehensive a narrative to the FIA as possible describing the who, what ,when, where and why of the suspicion;

- if a particular type of criminal conduct is suspected, a statement of this conduct;
- financial records;
- correspondence;
- file/account opening documentation;
- where a firm has additional relevant information that could be made available, the nature of this information; and
- statistical information to assist the FIA in its analysis of reports.

The FIA does not accept manual submissions of SARs (including those faxed or emailed). All SAR filing is done electronically, and in order to file a SAR you should:

1. Register with goAML by filling out a Registration form on the www.fia.bm website
2. Obtain your login information
3. File your SAR(s) online
4. Contact the FIA for any training issues at: analyst@fia.bm

Additional information may be obtained at www.fia.bm.

8.19 A SAR must be filed with the FIA as soon as it is reasonably practicable to do so once knowledge or suspicion has been formulated. As such it must be made either before a transaction occurs, or afterwards, if knowledge or suspicion is formulated with the benefit of hindsight after a transaction or activity occurs.

8.20 Firms should keep comprehensive records of suspicions and disclosures because disclosure of a suspicious activity or transaction is a defense to criminal proceedings. Such records may include notes of:

- ongoing monitoring undertaken and concerns raised by management and staff;

- discussions with the Reporting Officer (or Deputy Reporting Officer) regarding concerns;
- advice sought and received regarding concerns;
- why the concerns did not amount to a suspicion and a disclosure was not made;
- copies of any disclosures made;
- conversations with the FIA, insurers, supervisory authorities etc. regarding disclosures made; and decisions not to make a report to the FIA which may be important for the Reporting Officer to justify his position to law enforcement.

8.21 Tipping Off

POCA and ATFA contain sections creating offences of "tipping off"
POCA section 47 & ATFA section 10A

POCA section 47(1) & ATFA section 10A(1)
Where a person knows or suspects that the police are acting or proposing to act in connection with an investigation which is being or is about to be conducted into money laundering or terrorist financing, and discloses any information to any other person which is likely to prejudice that investigation or proposed investigation, they commit an offence. It is a defence if the person does not know or suspect that disclosure is likely to prejudice the investigation.

POCA section 47(2) & ATFA section 10A(2)
Once an internal or external suspicious activity report has been made, it is a criminal offence for any person knowing or suspecting that such a report has been made, to disclose to any other person information or any other matter which is likely to prejudice any investigation which might be conducted following such a disclosure.

In order to prevent the commission of a tipping-off offence, at the time of acknowledging receipt of an internal SAR, the Reporting Officer (or Deputy Reporting Officer) may provide a reminder to the member of staff submitting the report of the risk of communicating information that might prejudice law enforcement enquiries.

Regulation 6(1) (c) of the AML/ATF Regulations requires a relevant person to apply customer due diligence measures when the firm suspects money laundering or terrorist financing. Therefore, there is a risk that the contact between the firm and the client (or his advisors) could unintentionally lead to the client being tipped-off, where the process is managed without due care. Although it is not tipping-off to include a paragraph about a firm's obligations under the money laundering and terrorist financing legislation in a firm's standard client care letter. Reference should be made to the client due diligence procedures outlined in Section 5 of the Guidance Notes.

8.22 In circumstances where a SAR has been filed with the FIA, and the CDD procedures are incomplete, the risk of tipping-off a client (and its advisers) may be minimized by ensuring that employees undertaking due diligence enquiries are aware of tipping-off procedures and are provided with adequate support, such as specific training or assistance from the Reporting Officer.

8.23 Obtaining Consent from the FIA

Where a SAR is made before a suspected transaction or event takes place, FIA consent must be obtained before the transaction or event occurs. Consent will only be given in respect of that particular transaction or activity and future transactions or activity should continue to be monitored and reported accordingly (POCA sections 44(3)(b)(i) and 45(5)(b)(i); and ATFA section 12 sets out consent provisions).

Where a SAR report is made after the transaction or event, this will be acknowledged by the FIA. In the absence of any instruction to the contrary from the FIA, a firm will be free to maintain the client relationship under normal commercial circumstances. However, receipt of an acknowledgment from the FIA in these circumstances does not indicate that the knowledge or suspicion is with or without foundation, and future transactions or activity should continue to be monitored and reported as appropriate.

Refusal to act upon a client's instruction (for example, as a result of the FIA refusing to give consent for a transaction to proceed) may also lead to civil proceedings being instituted by the client. It may be necessary in circumstances where a client has instigated civil proceedings for a firm to seek the directions of the court.

8.24 Transactions following a disclosure

A firm is not obliged to continue relationships with clients if such action would place them at commercial risk. Termination is ultimately a commercial decision, however, in certain circumstances a firm should consider liaising with the FIA to determine whether it is likely that termination would alert the client, and in such a case the FIA may request that a relationship is not terminated to avoid prejudicing an investigation.

If a firm, having filed a SAR, wishes to terminate a relationship or transaction and is concerned that in doing so, it may prejudice an investigation resulting from the report, it should seek the consent of the FIA to do so where the activities referred to fall within Sections 44 and 45 of POCA and section 12 of ATFA. This is to avoid the danger of tipping-off.

8.25 Obtaining Information

Section 16(1) of the FIA Act provides that the FIA may, in the course of enquiring into a suspicious transaction relating to a money laundering offence or a terrorist finance offence, serve a notice in writing on any person requiring that person to provide the FIA with such information as it may reasonably require for the purpose of its enquiry.

Section 16(2) of the FIA Act provides that a person who is required to provide information pursuant to a notice served under subsection (1) must provide the information to the FIA in such manner as the FIA requires.

Pursuant to Section 16(3) of the FIA Act, any person who without reasonable excuse fails to comply with a requirement imposed on him under this section shall be guilty of an offence and liable on summary conviction to a fine of $10,000 or to imprisonment for six months or to both.

Nothing in section 16 requires the disclosure of information which is subject to legal professional privilege.

8.26 Service of Orders and Notices

During the course of an investigation, a firm may be served with an order designed to restrain particular funds or property pending the outcome of an investigation. It should be noted that the restraint order may not apply to all funds or assets involved within a particular business relationship and a firm should consider what, if any, property may be utilized.

Upon the conviction of a defendant, a court may order the confiscation of their criminal proceeds or the confiscation of assets to a value representing the benefit of their criminal conduct, which may require the realization of legitimately obtained assets. A firm may be served with a confiscation order in relation to any funds or property belonging to that defendant. For example, if a person is found to have benefited from drug dealing to a value of $100,000, then the court may order the confiscation of any assets belonging to that person to a value of $100,000. Confiscation of the proceeds of criminal conduct is becoming commonplace within many jurisdictions, and legislation in place in Bermuda provides a mechanism by which overseas criminal confiscation orders may be recognized. Overseas civil confiscation orders may also be recognized in Bermuda.

8.27 Freezing of funds

Section 15(1) of the FIA Act provides that the FIA may in the course of enquiring into a suspicious transaction relating to the suspected proceeds of criminal conduct or to a money laundering offence or terrorist finance offence serve a notice on any relevant institution in Bermuda requiring it to not make available any funds to any person specified in the notice. Pursuant to Section 15(2) of the FIA Act such a notice shall be in writing and may require the relevant institution, as defined by Section 2(2), to freeze funds for a period not exceeding 72 hours. A relevant institution commits an offence if without reasonable excuse it fails to comply with a notice served on it under subsection (1) and a relevant institution guilty of an offence under subsection (1) is liable on summary conviction to a fine of $50,000.

Under Section 52A(1) and (2) of POCA, a magistrate, upon the application of a police officer in the course of a confiscation investigation or an investigation into money laundering, may make an order requiring a relevant institution, as defined by Section 7(2), to not make available the suspected funds to any person. Pursuant to Section 52A(3) such an order shall not have effect for more than seven days,

8.28 Persons firms should not accept as clients

Recommendation 6[2] and 7[3] of the FATF Standards require that countries implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions ("UNSCRs") relating to the prevention and suppression of terrorism and terrorist financing,

[2] Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999) and any future UNSCRs which impose targeted financial sanctions in the terrorist financing context. At the time of issuance of the FATF Interpretive Note, (February 2012), the successor resolutions to resolution 1267 (1999) are resolutions: 1333 (2000), 1363 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

[3] Recommendation 7 is applicable to all current Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Recommendation, (February 2012), the Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: resolutions 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), and 1929 (2010).

and the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

Prevention and suppression of terrorism and terrorist financing

On 31 March 2011, the **Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011** ("TAFA 2011 Order") brought into effect in Bermuda the requirements of UNSCR 1373 (2001)[4]. The purpose of the TAFA 2011 Order is to ensure that the necessary international anti-terrorism and terrorist asset-freezing measures are in place in the Overseas Territories of the UK. To this end the TAFA 2011 Order extends, with modifications, the UK Terrorist Asset-Freezing etc. Act 2010 ("TAFA") to Overseas Territories. The key objective of TAFA is to prevent and suppress the financing and facilitation of any acts of terrorism. There are five core prohibitions in the TAFA 2011 Order, breach of any of which is a criminal offence:-

(i) Dealing with the funds and economic resources of a designated person;

(ii) Making funds or financial services available to a designated person;

(iii) Making funds or financial services available for the benefit of a designated person;

(iv) Making economic resources available to a designated person; and

(v) Making economic resources available for the benefit of a designated person.

In August 2012, the requirements of UNSCR 1267 (1999)[5] as amended, and other additional European Union ("EU") measures, were brought into force in Bermuda through the **International Sanctions (Al-Qaida) (United Nations Measures) Regulations 2012** ("Al-Qaida Regulations") and **International Sanctions (Afghanistan) (United Nations Measures) Regulations 2012** ("Afghanistan Regulations"). The Al-Qaida Regulations and the Afghanistan Regulations implement respectively **The Al-Qaida (United Nations Measures) (Overseas Territories) Order 2012 No. 1757** ("Al-Qaida Order 2012") and **The Afghanistan (United Nations Measures) (Overseas Territories) Order 2012 No. 1758**

[4] The requirements of UNSC Resolution 1373 (2001) were previously implemented in Bermuda through the Terrorism (United Nations Measures) (Overseas Territories) Order 2001 ("2001 Order") and the Terrorist Asset-Freezing (Temporary Provisions) Act 2010.

[5] The requirements of UNSC Resolution 1267 (1999) were previously implemented in Bermuda through **The Al-Qa'ida and Taliban (United Nations Measures) (Overseas Territories) Order 2002**, as amended.

("Afghanistan Order 2012"). As with previous measures implementing non-UN obligations of the UK, these EU measures cannot be directly extended to Bermuda as such non-UN Sanctions obligations must be implemented by Regulations, made under section 2(1) of the International Sanction Act 2003.

The Al-Qaida Order 2012 places restrictive measures on certain persons and entities associated with Al-Qaida. These restrictive measures include, inter alia, asset freezing measures and the prohibition of the supply of military goods and technical assistance related to military activities to designated persons. The Afghanistan Order 2012 places restrictive measures on certain persons and entities associated with the Taliban. These restrictive measures include, inter alia, asset freezing measures and the prohibition of the supply of military goods and technical assistance related to military activities to designated persons.

Prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing

On 16 December 2006, the requirements of UNSCR 1718 (2006) were implemented in Bermuda through The North Korea (United Nations Measures) (Overseas Territories) Order 2006 No. 3327 ("North Korea Order 2006"). The North Korea Order 2006 was amended by The North Korea (United Nations Measures) (Overseas Territories) (Amendment) Order 2007 No. 1347 and The North Korea (United Nations Measures) (Overseas Territories) Order 2009 No. 1746, which implemented UNSCR 1874 (2009). The North Korea Order 2006, as amended, implements restrictions on a range of goods from entering or leaving the North Korea and imposes a travel ban and an asset freeze against those persons designated by the competent UN Security Council Sanctions Committee or by the Security Council as persons who engage in or provide support for, including through other illicit means, North Korea's nuclear-related, other weapons of mass destruction-related and ballistic missile-related programmes.

On 18 July 2012, the requirements of UNSCR 1737 (2006) as amended, and other additional European Union ("EU") measures, were brought into force in Bermuda through the

International Sanctions (Iran) (Nuclear Proliferation) (Restrictive Measures) Regulations 2012 ("Iran (Nuclear Proliferation) Regulations"). The Iran (Nuclear Proliferation) Regulations implement **The Iran (Restrictive Measures) (Overseas Territories) Order 2012 No. 1756** ("Iran (Nuclear Proliferation) Order 2012") which provides for a prohibition on the supply of arms to, or purchase of arms from, Iran; a prohibition on the sale or supply of goods and technology which could contribute to Iran's proliferation activities; a prohibition on providing assistance or financing in relation to prohibited goods; a prohibition on the importation or transportation of oil from Iran; a prohibition on the importation or transportation of petrochemical products from Iran; a prohibition on financing any Iranian person or entity engaged in certain nuclear-related activities; a prohibition on supplying equipment to any Iranian person or for use in Iran for the exploration and production of oil or gas, or for use in the petrochemical industry in Iran; a prohibition on the sale or purchase of gold, precious metals or diamonds to or from Iran; a prohibition on the supply of newly printed banknotes and coins to Iran; restrictions on financial transactions to or from Iranian persons or entities; and a prohibition on the purchase of Iranian bonds.

It should be appreciated that any obligations that arise under these Orders are in addition to any obligations under the AML/ATF suite of legislation and are separate from those obligations. The full text of the Orders are available at: www.legislation.gov.uk/ and the International Sanctions Act Regulations are available at: www.bermudalaws.bm. Persons should ensure that they fully understand their obligations under this legislation. As appropriate, persons should take legal advice to assist in their understanding and compliance.

The links provided below may be of assistance in relation to financial sanctions regimes in the United Kingdom, the European Union and the United States –

United Kingdom – HM Treasury:

Financial sanctions - HM Treasury

European Union – External Relations:

Common Foreign & Security Policy (CFSP) - Sanctions or restrictive measures in force

United States of America – Office of Foreign Asset Control:

U.S. Treasury - Office of Foreign Assets Control

RELIANCE ON THIRD PARTIES

9.1 Regulation 14

The AML/ATF Regulations expressly permit a firm to rely on another regulated entity ("entity") to apply any or all of the customer due diligence measures, provided that the other entity is listed in Regulation 14(2), and that consent to being relied on has been given. The relying firm, however, retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

For example:

- Where an entity (entity A) enters into a business relationship with, or undertakes an occasional transaction for, the underlying client of another entity (entity B), for example by accepting instructions from the client (given through entity B); Regulation 14(2) (a) & (b)

In this context, Entity B must be:

(1) a person who carries on business in Bermuda who is an AML/ATF regulated financial institution under section 2(2) of the AML/ATF Regulations or a business in the regulated sector under section 3 of the Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008; or an independent professional as defined at section (2) (1) of the AML/ATF Regulations.

Regulation 14(2) (c);

(2) a person who carries on business in a country or territory other than Bermuda who is:

(a) an institution that carries on business corresponding to the business of an AML/ATF regulated financial institutions or independent professionals;

(b) subject to mandatory professional registration recognised by law;

(c) subject to requirements equivalent to those laid down in the regulations; and

(d) supervised for compliance with those requirements in a manner equivalent to supervision by the relevant supervisory authority.

9.2 Consent to be relied upon

The Regulations do not define how consent must be evidenced. Ordinarily, 'consent' means an acceptance of some form of proposal by one party from another – this may be written or oral, express or implied. Written acknowledgement that an entity is being relied on makes its relationship with the firm relying on it clear. On the other hand, it is not necessary for an entity to give an express indication that it is being relied on, and it may be inferred from their conduct.

In order to satisfy the purpose behind Regulation 14(1)(a), a firm may wish to consider providing the entity being relied on with notification of the reliance. The notification should specify that the firm intends to rely on the third party institution for the purposes of Regulation 14(1) (a). Such a notification can be delivered in a number of ways. For example, where one firm is introducing a client to another firm, the issue of reliance can be raised during the introduction process and may form part of the formal agreement with the intermediary. Similarly, where the relying and relied upon entities are party to tripartite agreement with a client, the notification may be communicated during exchange of documents. Where a relationship exists between the parties it is likely that such a notification plus some form of acceptance should be sufficient for the purposes of establishing consent.

Where there is no contractual or commercial relationship between the relying and relied upon entities it is less likely that consent can be assumed from the silence of the entity being relied on. In such circumstances firms may wish to seek an express agreement as to reliance. This does not need to take the form of a legal agreement and a simple indication of consent (e.g., by e-mail) should suffice.

9.3 Basis of reliance

For one firm to rely on verification carried out by another entity, the verification that the entity being relied upon has carried out must have been based at least on the standard level of customer verification. It is not permissible to rely on simplified due diligence carried out, or

any other exceptional form of verification, such as the use of source of funds as evidence of identity.

Firms may also only rely on verification actually carried out by the entity being relied upon. An entity that has been relied on to verify a customer's identity may not 'pass on' verification carried out for it by another entity.

Whether an entity wishes to place reliance on a third party will be part of the firm's risk-based assessment, which, in addition to confirming the third party's status (Regulation 14(2)), may include consideration of matters such as:

- Its public disciplinary record, to the extent that this is available;
- The nature of the client the service sought and the sums involved;
- Any adverse experience of the other entity's general efficiency in business dealings; and
- Any other knowledge, whether obtained at the outset of the relationship or subsequently, that the firm has regarding the standing of the entity to be relied upon.

The assessment as to whether or not a firm should accept confirmation from a third party that appropriate customer due diligence measures have been carried out on a client will be risk-based, and cannot be based simply on a single factor.

In practice, the firm relying on the confirmation of a third party needs to know:

- The identity of the client and/or beneficial owner whose identity is being verified;
- The level of customer due diligence that has been carried out; and
- Confirmation that the third party understands his obligation to make available, on request, copies of the verification data, documents or other information.

The third party has no obligation to provide such confirmation to the firm, and may choose not to do so. In such circumstances, or if the firm decides that it does not wish to rely upon the

third party, then the firm must carry out its own customer due diligence measures on the client.

For an entity to confirm that it has carried out customer due diligence measures in respect of a customer is a serious matter. An entity must not give a confirmation on the basis of a generalized assumption that the entity's systems have operated effectively. There has to be awareness that the appropriate steps have in fact been taken in respect of the client that is the subject of the confirmation.

Regulation 15(5)

An entity which carries on business in Bermuda and is relied on by another person must, within the period of five years beginning on the date on which it is relied on, if requested by the firm relying on it:

- As soon as reasonably practicable make available to the firm which is relying on it any information about the client (and any beneficial owner) which the third party obtained when applying customer due diligence measures; and
- As soon as reasonably practicable forward to the firm which is relying on it relevant copies of any identification and verification data and other relevant documents on the identity of the client (and any beneficial owner) which the third party obtained when applying those measures.

Regulation 15(6)

A firm which relies on an entity situated in a country or territory other than Bermuda to apply customer due diligence measures must take steps to ensure that the entity on which it relies will, within the period of five years beginning on the date on which the third party is relied on, if requested, comply with the obligations to retain and maintain information as set out above.

The personal information supplied by the client as part of a third party's customer identification procedures will generally be set out in the form that the relying firm will require to be completed, and this information will therefore be provided to that entity.

Regulation 15(5) & (6)

A request to forward copies of any identification and verification data and other relevant documents on the identity of the customer or beneficial owner obtained when applying customer due diligence measures, if made, would normally be as part of a firm's risk-based customer acceptance procedures. However, the entity giving the confirmation must be prepared to provide this data or other relevant documents throughout the five year period for which it has an obligation under the Regulations to retain them.

Where a firm makes such a request and it is not met, the firm will need to take account of that fact in its assessment of the third party in question, and of the ability to rely on the third party in the future. In addition, the firm should review its application of CDD in respect of the client or beneficial owner in question.

A firm must also document the steps taken to confirm that the entity relied upon satisfies the requirements in Regulation 14(2). This is particularly important where the entity relied upon is situated in a country or territory other than Bermuda.

Part of the firm's AML/ATF policy statement should address the circumstances where reliance may be placed on other entities and how the firm will assess whether the other entity satisfies the definition of third party in Regulation 14(2)

9.4 Group Introductions

Where clients are introduced between different firms of the same group, entities that are part of the group should be able to rely on identification procedures conducted by that part of the group which first dealt with the client. One member of a group should be able to confirm to another part of the group that the identity of the client has been appropriately verified.

Where a client is introduced by one part of a firm to another, it is not necessary for his identity to be re-verified, provided that:

- The identity of the client has been verified by the introducing firm in line with AML/ATF standards of Bermuda or an equivalent jurisdiction; and

- The group entity that carried out the customer due diligence measures can be relied upon as a third party under Regulation 14(2).

The acceptance by a Bermuda firm of confirmation from another group entity that the identity of a client has been satisfactorily verified is dependent on the relevant records being readily accessible, on request, from the other entity.

Where Bermuda firms have day-to-day access to all group client information and records, there is no need to obtain a group introduction confirmation, if the identity of that client has been verified previously to AML/ATF standards in Bermuda, or in an equivalent jurisdiction. However, if the identity of the client has not previously been verified, for example because the group client relationship pre-dates the introduction of AML/ATF regulations, or if the verification evidence is inadequate, any missing
verification evidence will need to be obtained.

9.5 Use of pro-forma confirmations

Regulation 14(2)
Whilst a firm may be able to place reliance on another party to apply all or part of the customer due diligence measures under Regulation 14(2), it may still wish to receive, as part of its risk-based procedures, a written confirmation from the third party, not least to evidence consent. This may also be the case, for example, when a firm is unlikely to have an on-going relationship with the third party. Confirmations can be particularly helpful when dealing with third parties located in a country or territory other than Bermuda, where it is necessary to confirm that the relevant records will be available

The provision of a confirmation certificate implies consent to be relied upon, in the terms agreed and in accordance with Regulation 14

9.6 Situations which are not reliance

One firm or entity acting solely as introducer

At one end of the spectrum, one entity may act solely as an introducer between the client and the firm providing the service, and may have no further relationship with the client. The introducer plays no part in the transaction between the client and the firm, and has no relationship with either of these parties that would constitute a business relationship.

In these circumstances, where the introducer neither gives advice nor plays any part in the negotiation or execution of the transaction, the identification and verification obligations under the Regulations lie with the firm. This does not, of course, preclude the introducing entity carrying out identification and verification of the client on behalf of the firm providing service, as agent for that firm.

Where the intermediary is the agent of the firm

If the intermediary is an agent or appointed representative of the firm, it is an extension of that firm. The intermediary may actually obtain the appropriate verification evidence in respect of the client, but the firm is responsible for specifying what should be obtained, and for ensuring that records of the appropriate verification evidence taken in respect of the client are retained.

9.7 Regulation 10(2)

Depending on jurisdiction, where the client is an intermediary carrying on appropriately regulated business, and is acting on behalf of another, there is no obligation on the firm to carry out customer due diligence measures on the client, or on the underlying party.

Where a firm cannot apply simplified due diligence to the intermediary,
the firm is obliged to carry out customer due diligence measures on the
intermediary and, as the intermediary acts for another, on the underlying client.

In particular, where the intermediary is located in a higher-risk jurisdiction, the risk-based approach should be aimed at ensuring that the business does not proceed unless the identity of the underlying client has been verified to the firm's satisfaction.

LEGAL PROFESSIONAL PRIVILEGE

10.1 Lawyers are professionally and legally obliged to keep the affairs of their clients confidential and the circumstances in which they are able to disclose client communications are strictly limited. This obligation extends to all matters revealed to a lawyer, from whatever source, by a client or someone acting on the client's behalf. Only in exceptional circumstances, may this general obligation of confidence be overridden. The most relevant instances are where a court orders disclosure or disclosure is required by statute.

POCA, the FIA Act and ATFA all contain provisions requiring the disclosure of confidential information in certain circumstances to the FIA (or the Reporting Officer) by persons working in firms that fall within Regulation 2(1) of the AML/ATF Regulations.

10.2 There will likely be potential tensions between a lawyer's duty of confidentiality to his client and the disclosure requirements imposed under POCA, the FIA Act and ATFA.

10.3 Under Section 44 of POCA, a person who enters into an arrangement with another person knowing or suspecting that the other person is or has been engaged in criminal conduct or has benefited from criminal conduct commits an offence, unless they disclose that knowledge or suspicion or any matter on which it is based to the FIA or to the Reporting Officer in accordance with their employer's procedures. Such a disclosure is to be made before he does the act concerned and the act is done with the consent of the FIA, or the disclosure is made after he does the act but is made on his initiative as soon as it is reasonable for him to make it.

10.4 Under Section 45 of POCA a person commits an offence if that person acquires, uses or has possession of property knowing that the property represents another person's proceeds of crime, unless they disclose that knowledge to the FIA or to the Reporting Officer in accordance with their employer's procedures. Again, such a disclosure is to be made before he does the act concerned and the act is done with the consent of the FIA, or the disclosure is made after he does the act but is made on his initiative as soon as it is reasonable for him to make it.

10.5 Section 5-10 of ATFA contains similar provisions in relation to terrorist financing and money laundering relating to terrorist property.

10.6 Section 46 of POCA and Section 9 of the ATFA contain comparable provisions. Those provisions provide that a person commits an offence if they come into information in the course of their employment which leads them to know or suspect that another person is engaged in money laundering or committing an offence under Section 5-8 of ATFA. and the person does not report their knowledge or suspicion to the FIA or to the Reporting Officer in accordance with their employer's procedures.

Sections 46(4) POCA and 9(4) ATFA set out defence of reasonable excuse for not making a disclosure.

10.7 The POCA, FIA Act and ATFA also include exemptions from the requirement to make such disclosures for professional legal advisers acting in privileged circumstances (see Section 46 (3) of POCA, 9(6) of ATFA, and 16(4) and 20(3) of FIA Act),). Legal professional privilege is defined in Section 46(6) of POCA and 9(7) of ATFA as any information or other matter which comes to a professional legal advisor in privileged circumstances where it is communicated to him by or by a representative of a client of his in connection with the giving by the adviser of legal advice to the client; or by a person seeking legal advice from the adviser or by any person in contemplation of or in connection with legal proceedings and for the purpose of those proceedings .

The exemptions do not apply to information or other matters communicated or given with a view to furthering a criminal purpose.

10.8 Section 47 of POCA and Section 10A of the ATFA covers the offence of "tipping-off" However, sections 47(3) and 10A(3) also provide that it is not an offence where a professional legal adviser discloses any information or other matter:

(a) to or to a representative of a client of the legal adviser in connection with the giving by the adviser of legal advice to the client; or

(b) to any person –

(i) in contemplation of or in connection with legal proceedings, and

(ii) for the purpose of those proceedings.

Again, this exemption does not apply in relation to any information or other matter that is disclosed with a view to furthering a criminal purpose

10.9 Certain confidential communications between a lawyer and his client will fall into a category known as Legal Professional Privilege ("LPP"). LPP is a privilege against disclosure, ensuring clients know that certain documents and information provided to lawyers cannot be disclosed without the client's consent. It recognises a client's fundamental right to be candid with their legal adviser, without fear of later disclosure to their prejudice. It is an absolute right and cannot be overridden by any other public interest. LPP can, however, be waived and it can be overridden by statute (R (Morgan Grenfell & Co Ltd.) v Special Comr of Income Tax [2003] 1 AC 563).

LPP does not extend to everything lawyers have a duty to keep confidential. LPP protects only those confidential communications falling under either of the two heads of privilege – advice privilege or litigation privilege.

10.10 For the purposes of LPP, lawyers include barristers, solicitors, in-house lawyers and their employees.

Communications between a lawyer, acting in their capacity as a lawyer, and a client, are privileged if they are both:

- confidential; and
- for the purpose of seeking advice from a lawyer or providing it to a client.

(Bene Ltd. v. VAR Hanson & Partners 1997 JLR N-10)

10.11 Communications are not privileged merely because a client is speaking or writing to their lawyer. The protection applies only to those communications which directly seek or provide advice or which are given in a legal context, that involve the lawyer using their legal skills and which are directly related to the performance of the lawyer's professional duties

(Three Rivers District Council and Others v Governor and Company of the Bank of Scotland (No 6) [2004] UKHL 48).

Case law has given some examples of what advice privilege covers:

10.12 Communications subject to advice privilege:

- a lawyer's bill of costs and statement of account (Chant v Brown (1852) 9 Hare 790); and

- information imparted by prospective clients in advice of a retainer will attract LLP if the communications were made for the purpose of indicating the advice required (Minister v Priest 1930 AC 558 per Lord Atkin at 584).

10.13 Communications not subject to advice privilege:

- notes of open court proceedings (Parry v News Group Newspapers (1990) 140 New Law Journal 1719 and Pacific Investments Ltd. v Christensen 1996 JLR N-7) are not privileged, as the content of the communication is not confidential;

- a client account ledge maintained in relation to the client's money (Nationwide Building Society v Various Solicitors [1999] P.N.L.R. 53);

- an appointments diary or time record on an attendance note, time sheet or fee record relating to a client (R v Manchester Crown Court, ex p. Rogers [1999] 1 W.L.R. 832 and Bene Ltd. v VAR Hanson & Partners 1997 JLR N-10)); and

- conveyancing documents are not communicated so not subject to advice privilege (R v Inner London Crown Court ex p. Baines and Baines [1988] QB 579).

10.14 All communications between a lawyer and their client relating to a transaction in which the lawyer has been instructed for the purpose of obtaining legal advice are covered by advice privilege, notwithstanding that they do not contain advice on matters of law and construction, provided that they are directly related to the performance by the lawyer of their

professional duty as legal adviser of their client. (*Three Rivers District Council v the Bank of England [2004] UKHL 48 at 111*).

10.15 This means that where a lawyer is providing legal advice in a transactional matter (such as conveyancing) the advice privilege will cover all:

- communications with;
- instructions from; and
- advice given to

the client, including any working papers and drafts prepared, as long as they are directly related to the lawyer's performance of their professional duties as a legal adviser.

10.16 This privilege, which is wider than advice privilege, protects confidential communications made in pursuance of, or contemplation of, litigation, between either:

- a lawyer and a client;
- a lawyer and an agent, whether or not that agent is a lawyer; or
- a lawyer and a third party.

(*Bene Ltd. v VAR Hanson & Partners* 1997 JLR N-10)

10.17 Such communications must be for the sole or dominant purpose of litigation, either:

- for seeking or giving advice in relation to it;
- for obtaining evidence to be used in it; or
- for obtaining information leading to obtaining such evidence.

10.18 An original document not brought into existence or privileged purposes and so not already privileged, does not become privileged merely by being given to a lawyer for advice or another privileged purpose.

10.19 Furthermore, where a lawyer has a corporate client, communication between the lawyer and the employees of the corporate client may not be protected by LPP if the employee cannot be considered to be "the client" for the purpose of the retainer. As such, some employees will be clients, while others will not. (*Three Rivers District Council v the Governor and Company of the Bank of England* (no 5) [2003] QB 1556).

10.20 It is not a breach of LPP to discuss a matter with your Reporting Officer for the purpose of receiving advice on whether to make a disclosure. Privilege will continue to apply whilst such a determination is being made.

10.21 LPP protects advice a lawyer gives to a client on avoiding committing a crime (*Bullivant v Att-Gen of Victoria* [1901] AC 196) or warning them that proposed actions could attract prosecution (*Butler v Board of Trade* [1971] Ch 680). LPP does not extend to documents which themselves form part of a criminal or fraudulent act (*Hume v Attorney General* 2006 LJR N-36), or communications which take place in order to obtain advice with the intention of carrying out an offence (*R v Cox and Railton* (1984) 14 QBD 153). It is irrelevant whether or not the lawyer is aware that they are being used for that purpose (*Banque Keyser Ullman v Skandia* [1986] 1 Lloyds Rep 336).

10.22 Section 44, 45, and 46 of the POCA, Section 10 of ATFA, and section 20 of the FIA Act provides that, if a person discloses information under those laws, the disclosure will not be treated as a breach of any restriction on the disclosure of information (however imposed).

10.23 It is not just a client's intention which is relevant for the purpose of ascertaining whether information was communicated for the furtherance of a criminal purpose. It is also sufficient that a third party intends the lawyer/client communication to be made with that

purpose (e.g. where the innocent client is being used by a third party) (*R v Central Criminal court ex p Francis & Francis* [1989] 1 AC 346).

10.24 The direct reporting obligations contained in Section 46 (2) of POCA and Section 9(3) of ATFA do not apply to a lawyer's knowledge or suspicion arising from information obtained in privileged circumstances (as defined in those laws). A lawyer may, however, wish to consider making a joint report with his client. The agreement of the lawyer's client to waive LPP is necessary in order for this to be possible.

10.25 If information leading to knowledge or suspicion is obtained in circumstances that are not covered by LPP, a disclosure should be made to avoid the commission of an offence of failing to disclose. Lawyers will not be in breach of their professional duty of confidentiality when they do so.

10.26 If a lawyer commits an offence under Section 44 or 45 of POCA or Section 8 of ATFA they should make a disclosure to a police officer, otherwise they will not be able to avail themselves to the defences which operate under those Sections.

10.27 As the application of LPP is complex, it is recommended that firms consider requiring that reports be made to the Reporting Officer on each occasion that there is knowledge or suspicion of money laundering or terrorist financing. The Reporting Officer can then discuss the situation with the fee earner concerned and, as necessary, take advice from an appropriate partner, director or senior lawyer.

10.28 It would be prudent, and would facilitate a firm's compliance with the requirements of POCA, ATFA and the FIA Act, for consideration to be given to the need to separate all material on client files so that it is clear what material is non-privileged and the material for which privilege is claimed.

10.29 CDD and risk assessment documents should be completed, where possible, in a way which distinguishes privileged and non-privileged information. It would be prudent where

possible, to include guidance to the effect in internal procedure manuals. This will assist in ensuring that the Board can undertake audits of firms with the minimum disruption to business and those firms comply with their obligations to the Board.

TRAINING

Regulation 18

11.1 Regulation 18 of the AML/ATF Regulations requires a relevant person to take appropriate measures so that all relevant employees are made aware of the laws relating to money laundering and terrorism financing and regularly given training in how to recognize and deal with transactions which may be related to money laundering or terrorist financing. The effective application of even the best designed control systems can be quickly compromised if staff lack competence or probity, are unaware of or fail to apply systems and controls, and are not adequately trained.

Regulation 18(2) of the AML/ATF Regulations defines a relevant employee as an employee who at any time in the course of his duties has or may have access to any information which may be relevant in determining whether any person is engaged in money laundering or terrorist financing.

One of the most important controls over the prevention and detection of money laundering and terrorist financing is to have appropriately vetted staff who are: (i) alert to money laundering and terrorist financing risks; and (ii) well trained in the identification of unusual or higher risk activities or transactions, which may indicate money laundering or terrorist financing activity.

Therefore all relevant employees will need to have a basic understanding of money laundering and terrorist financing and an awareness of internal reporting procedures (including the identity of the Reporting Officer and the statutory penalties for non compliance). It is important for senior management to make employees aware of their obligations and to provide regular training on how to discharge them.

11.2 A firm must have appropriate measures in place to make relevant employees aware of:

- the firm's business' systems and controls (including policies and procedures) designed to prevent and detect money laundering and terrorist financing;

- the statutory obligations under which the business operates and under which employees may be held personally liable; and

- the implications of failing to report information in accordance with procedures, and that as well as criminal, civil or regulatory sanctions, disciplinary proceedings can also rise.

11.3 A firm may demonstrate that it has appropriate measures in place where it:

- provides relevant employees with a copy of, or intranet access to, the firm's procedure manual for AML/ATF;

- informs staff of the identity of the Reporting Officer and the procedures to make internal SARs;

- provides relevant employees with a document outlining the firm's and their own obligations and potential criminal liability under the AML/ATF legislation and this Guidance;

- requires employees to acknowledge that they have received and understood the business' procedures manual and document outlining statutory obligations; and

- periodically tests employees' awareness of policies and procedures and statutory obligations.

11.4 It is not sufficient solely to provide employees with a copy of these Guidance Notes as these are designed to provide a base from which a firm can design and implement systems and tailor its own policies and procedures appropriate to its business.

A firm may demonstrate that it has appropriate measures to maintain awareness where it:

- keeps employees aware of anti-money laundering and terrorist financing developments (such as updates issued by the Board or the Office of the National Anti-Money Laundering Committee (" NAMLC"), or developments in international standards) as they occur;

- provides employees with case studies illustrating how products or services provided by the financial services business may be abused;

- advises employees of current news stories involving money laundering and terrorist financing activity; and

- sends e-mail reminders of employee obligations and the need to remain vigilant.

11.5 The guiding principle of all anti-money laundering and terrorist financing training should be to encourage employees, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the business against the threat of money laundering and terrorist financing. A firm may demonstrate the provision of adequate training where the training promotes an awareness of the threat of money laundering and terrorist financing and the reporting procedures that should be followed in the event that unexplained unusual, or higher risk activity or transactions are spotted.

Training must:

- be tailored to the business and relevant to the employees to whom it is delivered;

- highlight to employees the importance of the contribution that they can individually make to the prevention and detection of money laundering and terrorist financing; and

- cover key aspects of legislation to prevent and detect money laundering and the financing of terrorism.

A firm may demonstrate the provision of adequate training to relevant employees where it addresses:

- the money laundering and terrorist financing legislation;
- vulnerabilities of services and products offered by the firm, and subsequent money laundering and terrorist financing risk;
- policies and procedures, and employees' responsibilities;
- application of risk based CDD policies and procedures;
- recognition of and dealing with unusual or higher risk activity and transactions, such as activity outside of expected patterns, unusual settlements, abnormal payment or delivery instructions and changes in the patterns of business relationships;
- money laundering and terrorist financing developments, including techniques, methods, trends and typologies; and
- management of client relationships which have been the subject of a SAR, e.g. risk of committing the offence of tipping-off, and dealing with questions from such clients, and/or their advisers.

11.6 A firm may demonstrate the provision of adequate training where (in addition to training for relevant employees) it addressed the evaluation of the effectiveness of systems and controls (and policies and procedures) in place to prevent and detect money laundering and the financing of terrorism.

A firm may demonstrate the provision of adequate training where (in addition to training for relevant employees) it addresses:

- the design and implementation of systems and controls to counter money laundering and terrorist financing; and

- the design and implementation of compliance testing and monitoring programs.

A firm may demonstrate the provision of adequate training where (in addition to training for relevant employees) it addresses:

- the handling and validation of internal disclosures;

- liaising with the FIA and law enforcement;

- management of the risk of tipping-off; and

- the handling of, for example, production and restraint orders.

A firm may demonstrate the provision of training at appropriate frequencies by:

- providing all employees with induction training within 30 days of the commencement of employment and, when necessary, where there is a subsequent change in an employee's role;

- delivering training to all employees at least annually, and otherwise determining the frequency of training for relevant employees on the basis of risk, with more frequent training where appropriate.

A firm may demonstrate that it has assessed the effectiveness of training provided by:

- testing employee's understanding of the business' policies and procedures to combat money laundering and terrorist financing, and also their ability to recognise money laundering and terrorist financing activity;

- monitoring the compliance of employees with systems and controls (including policies and procedures) to prevent and detect money laundering and terrorist financing, and taking any action that may be necessary;

- monitoring internal reporting patterns, and taking any action that may be necessary; and

- the routine supervision of employees.

RECORD KEEPING

Regulation 15

12.1 The record keeping obligations of the AML/ATF Regulations and additional regulatory requirements are essential to facilitate effective investigation, prosecution and confiscation of criminal property. If law enforcement agencies, either in Bermuda or elsewhere, are unable to trace criminal property due to inadequate record keeping, then prosecution for money laundering or terrorist financing and confiscation of criminal property may not be possible. Likewise, if the funds used to finance terrorist activity cannot be traced back through the financial system, then the sources and the destination of terrorist funding will not be identified.

12.2 Regulation 15 of the AML/ATF Regulations provides for record keeping procedures to be followed by a relevant person. Records may be kept:

- by way of original documents;
- by way of photocopies of original documents (certified where appropriate);
- microfiche;
- in scanned form; or
- in computerized or electronic form.

12.3 Regulation 15(2) of the AML/ATF Regulations requires the following records to be kept:

- a copy of or the references to, the evidence of the client's identity obtained pursuant to AML/ATF Regulations 6,11,13(4) or 14; and

- the supporting evidence and records (consisting of the original documents or copies admissible in court proceedings) in respect of the business relationships and occasional transactions which are the subject of customer due diligence.

12.4 Regulation 15 (3) of the AML/ATF Regulations requires a relevant person to retain records in relation to evidence of identity for at least five years beginning on the date on which the business relationship ends, or in the case of an occasional transaction five years beginning on the date on which the transaction is completed.

AML/ATF Regulation 2 defines an independent professional as a Relevant Person for the purposes of the records retention requirements.

12.5 A firm must ensure that the way in which CDD information is recorded and stored facilitates periodic updating of the information. A firm may demonstrate adequate recording and storage of CDD information by ensuring that updated information relating to a client that is obtained through meetings, discussions, or other methods of communication with the client is recorded and retained.

Records must contain the following details of each transaction carried out with or for a client in the course of business activities specified by Regulation 2 of the AML/ATF Regulations:

- name and address of the client;
- if a monetary transaction, the kind of currency and the amount;
- if the transaction involves a client's account, the number, name or other identifier for the account;
- date of the transaction;
- details of the counterparty, including account details;

- nature of the transaction; and

- details of the transaction.

The records prepared and retained by a firm in relation to client transactions and activity must be orderly and such that the audit trail for incoming and outgoing funds or asset movement is clear and complete. Adequate recording of details of transactions may be demonstrated by recording all transactions undertaken on behalf of a client within that client's records, enabling a complete transaction history for each client to be easily constructed.

12.6 Adequate recording of details of transactions may be demonstrated by including (where appropriate):

- valuation(s) and price(s);

- the form (e.g. cash, cheque, electronic transfer) in which funds are transferred;

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

- memoranda of purchase and sale;

- custody of title documentation; and

- other records in support of transaction of records where these are necessary to enable a clear and complete audit trail of fund or asset movements to be established.

A firm must keep for at least five years adequate and orderly records to enable the Board, internal and external auditors and other competent authorities to assess the effectiveness of systems and controls that are maintained by a firm to prevent and detect money laundering and the financing of terrorism.

12.7 A firm must keep adequate and orderly records documenting its policies and procedures to prevent and detect money laundering and the financing of terrorism for at least five years from the date those policies and procedures are superseded.

A firm may demonstrate that it has retained adequate records where it keeps:

- its risk assessment;
- compliance reports to senior management; and
- the working papers of the CP to the extent that these provide details of the testing programs conducted.

This does not necessitate the retention of all compliance testing working papers.

12.8 A firm must keep, for a period of five years from the date a business relationship ends, or, if in relation to an occasional transaction, for five years from the date that a transaction was completed, orderly records containing:

- internal SARs and supporting documentation;
- the decision of the Reporting Officer concerning whether to make an external suspicious activity report and the basis of that decision; and
- any external SARs in relation to that business relationship or an occasional transaction.

12.9 A firm must keep adequate and orderly records containing the findings of reviews of:

- complex transactions;

- unusual large transactions; and

- unusual patterns of transactions which have no apparent economic or visible lawful purpose, for a period of five years from the date the business relationship ends, or, if in relation to an occasional transaction, for five years from the date that the transaction was completed.

12.10 A firm must keep adequate and orderly records containing the findings of review of clients and transactions:

- connected with jurisdictions which do not or insufficiently apply the FATF Recommendations, where the business relationship or transaction has no apparent economic or visible lawful purpose; or

- which are the subject of international countermeasures – for a period of five years from the date the business relationship ends, or, if in relation to a one-off transaction, for five years from the date that the transaction was completed.

A firm must keep adequate and orderly records for five years detailing the dates on which training on the prevention and detection of money laundering and the financing of terrorism was provided, the nature of the training and the names of employees who received the training.

A firm must ensure that the way in which CDD information (including transaction information) is recorded facilitates ongoing monitoring of each relationship.

For all other purposes, the records retained by a firm must be readily accessible by the firm. A firm must periodically review the accessibility of, and condition of, paper and electronically retrievable records and ensure adequate consideration of the safekeeping of records.

A firm must periodically test procedures relating to retrieval of records.

A firm that undergoes mergers, take-overs, or internal reorganisations, must ensure that records remain readily retrievable for the required period when rationalising computer systems and storage arrangements.

Records must be maintained in a format which would enable the firm to respond fully and rapidly to enquiries received from the FIA or law enforcement relating to:-

- Whether it maintains, or has maintained during the previous five years a business relationship with any person and; the nature of that relationship.

Where documentation is held overseas or by third parties, such as under outsourcing arrangements, or where reliance is placed on introducers or intermediaries, this will present additional factors for a financial services business to consider. Where record keeping is outsourced, a firm remains responsible for compliance with all requirements.

Where an introducer ceases to trade or have a relationship with a client that it has introduced a firm, particular care needs to be taken to retain, or hand over, the appropriate client records.

A firm must not enter into outsourcing arrangement or place reliance on third parties to retain records where access to records is likely to be impeded by confidentiality or data protection restrictions.

Record keeping arrangements must be agreed with the Board where a firm terminates activities, or disposes of business or a block of client relationships to another accounting firm or service provider. Where a firm terminates activities, or disposes of business or a block of client relationships to other accounting firms or service providers, record keeping requirements are unaffected by the termination or disposal.