



Guide to
Anti-Money Laundering
and Anti-Terrorist Financing in Bermuda

TABLE OF CONTENTS

| | |
|---|----|
| PREFACE | 3 |
| INTRODUCTION | 4 |
| PART A: LEGISLATIVE FRAMEWORK | 4 |
| 1. Proceeds of Crime Act 1997 | 4 |
| 2. Anti-Terrorism (Financial and Other Measures) Act 2004..... | 5 |
| 3. Financial Intelligence Agency Act 2007 | 5 |
| 4. Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 | 6 |
| 5. Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008 | 6 |
| 6. Guidance Notes and Statement of Principles | 7 |
| PART B: ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING | 8 |
| 1. What is Money Laundering | 8 |
| 2. What is Terrorist Financing | 9 |
| PART C: AML/ATF CONTROLS | 10 |
| 1. Policies and Procedures..... | 10 |
| 2. Reporting Officer and Compliance Person..... | 11 |
| 3. Risk-based Approach..... | 11 |
| 4. Application of Group Policies to Branches and Subsidiaries Outside of Bermuda..... | 12 |
| PART D: CUSTOMER DUE DILIGENCE | 12 |
| 1. What is Customer Due Diligence | 12 |
| 2. Verification Procedures | 13 |
| 3. Timing of Verification | 15 |
| 4. Ongoing Monitoring..... | 15 |
| 5. Reliance on Third Parties | 15 |
| 6. Requirement to Cease Transactions | 16 |

| | |
|--|-----------|
| 7. Simplified Due Diligence | 16 |
| 8. Equivalent Jurisdictions..... | 17 |
| 9. Enhanced Due Diligence..... | 17 |
| 10. Politically Exposed Persons | 18 |
| PART E: SUSPICIOUS ACTIVITY REPORTING | 18 |
| 1. Suspicious Transactions..... | 18 |
| 2. Reporting Suspicious Transactions | 19 |
| 3. Tipping Off | 19 |
| PART F: FURTHER INTERNAL POLICIES AND PROCEDURES..... | 20 |
| 1. Staff Training and Awareness | 20 |
| 2. Record Keeping | 20 |
| PART G: NON-LICENSED AML/ATF REGULATED FINANCIAL INSTITUTIONS | 21 |
| PART H: PENALTIES FOR NON-COMPLIANCE WITH THE AML/ATF FRAMEWORK | 21 |
| CONCLUSION | 22 |

PREFACE

This Guide summarises the significant changes to Bermuda's anti-money laundering and anti-terrorist financing framework brought about in the past two years culminating in the entry into force of the following legislation:

- Proceeds of Crime Amendment Acts 2007, 2008 and 2009;
- Proceeds of Crime (Anti-Money Laundering and Anti-terrorist Financing) Regulations 2008;
- Anti-Terrorism (Financial and Other Measures) Amendment Act 2008;
- Anti-Terrorism (Financial And Other Measures) (Businesses in Regulated Sector) Order 2008;
- Financial Intelligence Agency Act 2007 and the Financial Intelligence Agency Amendment Act 2008; and
- Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008.

In addition, in 2009 the Bermuda Monetary Authority published the Guidance Notes on Anti-Money Laundering and Anti-Terrorist Financing, the Guidance Notes on Registration of Non-Licensed Persons and the Statement of Principles for the Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008, which provide further clarity to Bermuda's anti-money laundering and anti-terrorist financing framework.

It is recognised that this Guide will not completely answer the detailed questions that clients and their advisers may have. It is intended to provide a sketch of Bermuda's legal and regulatory environment in relation to anti-money laundering and anti-terrorist financing. The Guide is, therefore, designed as a starting-point for a more detailed and comprehensive discussion of the issues.

Whilst we have made every effort to ensure the accuracy of the statements made herein, we accept no liability for any errors. In all cases expert legal advice from a qualified practitioner of Bermuda law should be obtained.

Appleby
Hamilton, Bermuda
June 2009

INTRODUCTION

Over the past two years, Bermuda has continuously strived to enhance its anti-money laundering and anti-terrorist financing (“AML/ATF”) framework in order to get itself into line with the recommendations of the International Monetary Fund (“IMF”), the Financial Action Task Force (“FATF”) and other international anti-money laundering standards. The AML/ATF framework was undertaken with the corroboration of the Ministry of Finance, Ministry of Justice, the Bermuda Monetary Authority (“BMA”), industry bodies and other relevant stakeholders. The result is that Bermuda now has a strong, robust and effective regime for combating money laundering and terrorist financing.

PART A LEGISLATIVE FRAMEWORK

1. Proceeds of Crime Act 1997

The Proceeds of Crime Act 1997 (“POCA”) is the primary piece of legislation in Bermuda’s AML/ATF framework. The POCA establishes the powers of the police and the courts with respect to the tracing and confiscation of proceeds from drug trafficking and other relevant offences. Relevant offence is defined as “any indictable offence other than drug trafficking or any act or omission which, had it occurred in Bermuda, would have constituted an indictable offence other than drug trafficking”. The POCA also creates offences relating to money laundering and extends the powers of the police regarding seizure and forfeiture on import or export of suspected proceeds of crime.

On 15 November 2008, the Proceeds of Crime Amendment Act 2007 and the Proceeds of Crime Amendment Act 2008 (together the “POC Amendments”) both became operative. The POC Amendments broadens the definition of money laundering to include an attempt, conspiracy or incitement to commit money laundering and the aiding and abetting and/or the counselling or procuring of the commission of money laundering.

Where there are reasonable grounds for suspecting an incident of money laundering, the government’s investigative powers have now been extended to allow them to obtain production orders and search warrants. The POC Amendments also make provision for the granting of customer information orders which are issued against relevant institutions.

In addition to broadening the scope of money laundering offences, the POC Amendments provide for greater defences. They provide a defence through adherence by the entity to relevant guidance issued by a supervisory authority, approved by the Minister of Justice and published in a manner to bring it to the attention of persons likely to be affected by it. It is also a defence to money laundering if the relevant criminal conduct occurred outside of Bermuda and was not unlawful in the country or territory where it had occurred.

The POC Amendments clarify that disclosures made to the Financial Intelligence Agency (“FIA”) pursuant to the POCA are protected and would not breach any duty on confidentiality the institution may otherwise have.

The POC Amendments also provide for definitions for professional accountant and professional legal adviser and provide for them to be brought into scope of the regulations. Accountants and legal advisors are now required to, “establish and maintain procedures relating to the identification of clients, the keeping of records, the making of reports, the vetting of employees, the verification of the effective design and operation of anti-money laundering systems and the training of employees.”

The POC Amendments clarify the responsibility for offences by bodies corporate, ie officers, partners and the partnership are guilty of the offence as well as the body corporate and are liable to prosecution and punishment.

Further amendments include provisions pertaining to the voiding of agreements entered into for the purposes of money laundering; the grant of the power to the court to forfeit the instrumentalities of a money laundering offence; the grant of the power to the police to freeze funds for a period of seven days; the widening of the functions of the National Anti-Money Laundering Committee (“NAMLC”) that now operates under an independent Chairman; and the grant of the power to the Ministry of Justice to make regulations relating to controls to prevent and detect money laundering and to create offences of failing to comply with the regulations.

On 1 April 2009, the Proceeds of Crime Amendment Act 2009 became operative. This Act amends the POCA to allow the money seized within the AML/ATF framework to be released and used for the purposes of educating the public on drug trafficking and money laundering and helping to rehabilitate drug addicts.

2. Anti-Terrorism (Financial and Other Measures) Act 2004

The Anti-Terrorism (Financial and Other Measures) Act 2004 (“ATF Act”) establishes a series of offences relating to involvement in arrangements for facilitating, raising or using funds for the purpose of terrorism. Terrorism was originally defined in the ATF Act as the use or threat of action, involving serious violence against persons, serious risk to health and safety, damage to property, endangerment of life (other than the person committing the act) or disruption of electronic systems, designed to influence the government or intimidate the public and is made for the purpose of advancing a political, religious or ideological cause.

On 15 November 2008, the Anti-Terrorism (Financial and Other Measures) Amendment Act 2008 (the “ATF Amendment”) became operative. Its main purpose was to provide a broader definition for terrorism which is more consistent with international conventions on terrorism and to expand the offences related to terrorist financing. For instance, the actions which fall within the scope of the definition of terrorism were expanded to include unlawful seizure of aircraft in flight and unlawful violence against the safety of maritime navigation.

The ATF Amendment adds a tipping off offence and the offence of organising or directing others to raise funds for the purpose of terrorism. It also gives the Ministry of Justice the power to make regulations relating to controls to prevent financing of terrorism and to create offences of failing to comply with the regulations. The ATF Amendment clarify the responsibility for offences by bodies corporate, ie officers, partners and the partnership are guilty of the offence as well as the body corporate and are liable to prosecution and punishment.

On 6 November 2008, the Anti-Terrorism (Financial and Other Measures) (Businesses in Regulated Sector) Order 2008 was passed which designates the classes of business which fall within the “regulated sector” and are therefore required to disclose to the FIA any suspicions of terrorist financing. The regulated sector consists of deposit taking businesses; investment businesses; long term insurers (but not reinsurers); insurance managers or brokers in connection with long term business (other than reinsurance business); fund administrators; money service businesses; trust businesses and operators of investment funds.

3. Financial Intelligence Agency Act 2007

On 15 November 2008, the Financial Intelligence Agency Act 2007 and the Financial Intelligence Agency Amendment Act 2008 (together the “FIA Act”) became operative. The FIA is an independent agency established to receive, process and disseminate suspicious activity reports relating to suspected proceeds of crime and potential terrorist financing.

The FIA's powers include the ability to enter into arrangements to exchange information with regulatory bodies and law enforcement agencies globally; to serve a notice to freeze funds for up to 72 hours; and to serve notice for the production of relevant information for suspicious transactions. In carrying out its powers, the FIA has immunity from suit.

4. Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008

On 1 January 2009, the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 ("Regulations") became operative to replace the Proceeds of Crime (Money Laundering) Regulations 1998. The Regulations were made by an exercise of the powers granted to the Minister of Justice by the POCA and ATF Act and apply to AML/ATF regulated financial institutions as well as independent professionals¹ ("Applicable Institutions").

The Regulations require that the Applicable Institutions establish policies and procedures in order to prevent money laundering or terrorist financing. Such policies and procedures must cover, among other things,

- compliance management;
- risk assessment and management;
- customer due diligence requirements;
- external and internal reporting procedures;
- ongoing monitoring;
- training; and
- record keeping.

5. Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008

On 1 January 2009, the Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008 ("Supervision Act") became operative. The Supervision Act designates the BMA as the supervisory authority responsible for AML/ATF regulated financial institutions.

AML/ATF regulated financial institutions are persons who:

- carry on deposit-taking business within the meaning of section 4 of the Banks and Deposit Companies Act 1999;
- carry on investment business within the meaning of section 3 of the Investment Business Act 2003;
- are insurers (and not a reinsurers) registered under section 4 of the Insurance Act 1978 who carry on long term business falling within paragraph (a) or (c) of the definition of "long-term business" in section 1(1) of the Insurance Act 1978;
- are insurance managers or brokers registered under section 10 of the Insurance Act 1978 in so far as they act as managers or brokers in connection with long term business (other than reinsurance business) falling within paragraph (a) or (c) of the definition of "long-term business" in section 1(1) of the Insurance Act 1978;
- carry on the business of a fund administrator within the meaning of section 2(2) of the Investment Funds Act 2006;

¹ As at the date of this Guide, regulation 4(b) is not yet come into force and accordingly the Regulations do not currently apply to independent professionals.

- carry on money service business within the meaning of section 20AA of the Bermuda Monetary Authority Act 1969;
- carry on trust business within the meaning of section 9(3) of the Trusts (Regulation of Trust Business) Act 2001 and is not otherwise exempted by or under paragraph 3 of the Trusts (Regulation of Trust Business) Exemption Order 2002; or
- are operators of an investment fund within the meaning of section 2 of the Investment Funds Act 2006.

Pursuant to the Supervision Act, the BMA has a duty to maintain and publish a register of all AML/ATF regulated financial institutions (both licensed and non-licensed entities); to effectively monitor such institutions; and to take necessary measures to ensure compliance with the Regulations.

The Supervision Act requires that all non-licensed AML/ATF regulated financial institutions register with the BMA. For further detail on the registration requirements of non-licensed AML/ATF regulated financial institutions see Part G below.

The POCA, ATF Act, FIA Act, Regulations and Supervision Act will be collectively referred in this Guide to as the “AML/ATF legislation”.

6. Guidance Notes and Statement of Principles

a. Guidance Notes on Anti-Money Laundering and Anti-Terrorist financing

In March 2009, the BMA issued the Guidance Notes on Anti-Money Laundering and Anti-Terrorist Financing (“Guidance Notes”) which replaces the previous versions issued by NAMLC in 1998.

The purpose of the Guidance Notes is to assist AML/ATF regulated financial institutions and their staff in complying with the POCA, the ATF Act and the Regulations. The Guidance Notes allow the AML/ATF regulated financial institutions some discretion as to how they apply the requirements of Bermuda’s AML/ATF framework in the particular circumstances of the institution and its products, services, transactions and customers. The Guidance Notes provide a sound basis for institutions to meet their legislative and regulatory obligations by tailoring the information to meet their particular business risk profile.

Whilst the Guidance Notes are not legally binding, the Courts and the BMA are required to consider whether an AML/ATF regulated financial institution has followed any relevant guidance in determining whether it has committed an offence. Departures from the Guidance Notes (and the rationale for so doing) should be documented and institutions should be prepared to justify any departures.

The Guidance Notes include recommendations on the information to be gathered in relation to customer identification procedures. They also provide direction for policies on staff training, internal reporting and record keeping.

b. Statement of Principles

In March 2009, the BMA issued its Statement of Principles pursuant to the Supervision Act. The Statement of Principles sets out the principles in accordance with which the BMA will act in exercising its powers under the Supervision Act. The Statement of Principles covers the cancellation of the registration of non-licensed AML/ATF regulated financial institutions; the obtaining of information from

AML/ATF regulated financial institutions; the imposition of penalties and publishing of decisions; and the amounts to be paid with respect to penalties.

PART B ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING

1. What is Money Laundering

Money laundering is the process undertaken to conceal the origin of the proceeds from criminal activities so that they appear to have originated from legitimate sources. Criminals launder money in an attempt to avoid detection by law enforcement authorities and to make illicit proceeds available for use in further criminal activity and/or investment in legitimate businesses. Money launderers can and do use many different methods to make the origin of funds difficult or impossible to trace. These can vary from the most simple, such as the purchase and resale of an expensive piece of jewellery, to more complex schemes that involve money passing through networks of companies. The more sophisticated offenders make use of the financial system, which has become simpler and faster to use over recent years. There are three fundamental stages of money laundering:

- Placement – the physical disposal of criminal proceeds;
- Layering – separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide the appearance of legitimacy; and
- Integration – distributing the “cleaned” money into the mainstream, creating the appearance of legitimate wealth.

The offence of money laundering encompasses all processes and procedures used to conceal the origin of criminal proceeds so that they appear to have originated from a legitimate source. The common features of money laundering are (i) concealing the true ownership and origin of criminal proceeds; (ii) maintaining control over such proceeds; and (iii) changing the form of these proceeds.

Specific offences in relation to money laundering include:

a. Concealing or Transferring Proceeds of Criminal Conduct

Section 43 of the POCA makes it an offence to conceal, disguise, convert, transfer or remove property from Bermuda knowing or having reasonable grounds to suspect that it is the proceeds of criminal conduct with the intent to avoid prosecution or a confiscation order. The scope of this offence was widened by the POC Amendments to include in same the laundering of one's own proceeds of crime.

b. Assisting Another to Retain Proceeds of Criminal Conduct

Section 44 of the POCA makes it an offence for a person to be concerned in an arrangement whereby the retention or control by or on behalf of another person (“A”) of A’s proceeds of criminal conduct is facilitated and he knows or suspects A is or has been engaged in or has benefited from criminal conduct. This facilitation may be through the concealment of the proceeds of criminal conduct, its removal from the jurisdiction or its transfer to nominees or otherwise.

c. Acquisition, Possession or Use of Proceeds of Criminal Conduct

Section 45 of the POCA makes it an offence for a person to acquire, possess or use property, knowing that the property, in whole or in part directly or indirectly, represents the proceeds of criminal conduct.

d. Failing to Report

Section 46 of the POCA makes it an offence for a person to fail to report to the FIA where they have knowledge or suspicion that another person is engaged in money laundering which relates to any proceeds of criminal conduct as soon as is reasonably practicable after the information came to their attention in the course of their trade, profession, business or employment.

An exception to this offence is for a professional legal adviser who does not disclose information which has come to him in privileged circumstances, provided however the information is not communicated with a view to furthering any criminal purpose.

e. Tipping Off

Sections 42 and 47 of the POCA makes it an offence to disclose information likely to prejudice an investigation where the person knows or suspects a report has been made to the relevant authorities and there is or may be an investigation being conducted into money laundering.

An exception to this offence is for a professional legal adviser who discloses information in the context of providing legal advice, provided however such advice is not given with a view to furthering any criminal purpose.

2. What is Terrorist Financing

Terrorist financing is a fundamentally simple concept. It is the financial support, in any form, of terrorism or of those who encourage, plan or engage in terrorism. Money laundering and terrorist financing often display similar transactional features, mostly having to do with concealment and disguise. Whilst money launderers send illicit funds through legal channels in order to conceal their criminal origin, those who finance terrorism transfer funds that may be legal or illicit in origin in such a way as to conceal their source and ultimate use, which is to support acts of terrorism.

Specific offences in relation to terrorist financing under the ATF Act include:

a. Fundraising

It is an offence to invite another to provide money or other property where the person intends that money or property should be used, or suspects that it may be used, for the purposes of terrorism; or to organise or direct another person to commit such offences.

It is also an offence to receive, provide, use or possess money or other property knowing or suspecting that it may be used for the purposes of terrorism.

b. Funding arrangements

It is an offence for a person to be concerned in an arrangement as a result of which money or other property is made available or is to be made available to another knowing or suspecting that it will or may be used for the purposes of terrorism; or which facilitates the retention or control by or on behalf of

another person of terrorist property. This facilitation may be through the concealment of the terrorist property, its removal from the jurisdiction or its transfer to nominees or otherwise.

c. Failing to Report

It is an offence for a person to fail to report to the FIA where they have knowledge or suspicion that another person has committed an offence involving arrangements for facilitating, raising or using funds for terrorism purposes as soon as is reasonably practicable after the information came to their attention in the course of their trade, profession, business or employment.

An exception to this offence is for a professional legal adviser who does not disclose information which has come to him in privileged circumstances, provided however the information is not communicated with a view to furthering any criminal purpose.

d. Tipping Off

It is an offence to disclose information likely to prejudice an investigation where the person knows or suspects a report has been made to the relevant authorities and there is or may be an investigation being conducted into terrorist financing.

An exception to this offence is for a professional legal adviser who discloses information in the context of providing legal advice, provided however such advice is not given with a view to furthering any criminal purpose.

PART C AML/ATF CONTROLS

1. Policies and Procedures

The Regulations require that Applicable Institutions establish policies and procedures to forestall and prevent money laundering and terrorist financing. Such policies and procedures must cover: customer due diligence measures and ongoing monitoring; reporting; record keeping; internal control; risk assessment and management; and 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. The policies and procedures should be developed using the risk-based approach (see Part C.3. below). The nature and extent of such policies and procedures will depend on a variety of factors, including:

- the nature, scale and complexity of the Applicable Institution's business;
- the diversity of its operations, including geographical diversity;
- its customer, product and activity profile;
- its distribution channels;
- the volume and size of its transactions; and
- the degree of risk associated with each area of its operation.

The objective of the institution's AML/ATF policies and procedures must be to ensure that the institution is able to identify, assess, monitor and manage money laundering and terrorist financing risk. Furthermore, the policies and procedures must be comprehensive and proportionate to the nature, scale and complexity of the institution's business.

It falls under the responsibility of senior management of Applicable Institutions to adopt AML/ATF policies and procedures and ensure that such policies and procedures are appropriately carried out. To this end, the Guidance Notes suggest that senior management of these institutions should:

- allocate to a director or senior manager overall responsibility for the establishment and maintenance of AML/ATF systems and controls;
- appoint an appropriately qualified senior member of staff as the reporting officer; and
- provide direction to and oversight of the AML/ATF strategy.

AML/ATF policy statements should be customised to the circumstances of the institution, but should include, among other things, the following:

- an unequivocal statement of the culture and values to be adopted and promulgated throughout the institution towards the prevention of financial crime;
- a summary of its approach to assessing and managing money laundering and terrorist financing risk;
- a summary of the procedures for carrying out appropriate identification and monitoring checks on the basis of its risk-based approach; and
- a commitment to customer due diligence, both at the start and throughout the business relationship; and
- a summary of the appropriate monitoring arrangements in place to ensure that the institution's policies and procedures are being carried out.

While it is possible for an Applicable Institution to delegate some of its AML/ATF systems and controls to another entity, it is in the interest of the Applicable Institution to ensure that outsourcing does not result in reduced standards or requirements being applied, as institutions cannot contract out of their legal responsibilities and always remain responsible for systems and controls in relation to the outsourced activities. In all instances it is the Applicable Institution that bears the ultimate responsibility for the duties undertaken in its name (including ensuring that the provider of the outsourced services has in place satisfactory AML/ATF systems, controls and procedures, and that those policies and procedures are kept up to date to reflect changes in Bermuda requirements).

2. Reporting Officer and Compliance Person

All Applicable Institutions, other than sole proprietors, must appoint a reporting officer (“MLRO”) who is responsible for receiving disclosures from other employees within the institution that have a knowledge or suspicion that a person is engaged in money laundering or terrorist financing, and submitting, where appropriate, a suspicious activity report to the FIA. The institution must also appoint a compliance person who is responsible for monitoring the institution's compliance with Bermuda's AML/ATF framework. The MLRO and the compliance person may be the same person. Institutions should provide the BMA with the contact information of the MLRO and compliance person and notify them of any subsequent changes to these positions.

3. Risk-based Approach

As discussed, Applicable Institutions must put in place systems and controls which reflect the degree of risk associated with their business and customers. The starting point to the risk-based approach is to assume that most customers are not money launderers or terrorist financiers. The institution's policies and procedures should then set out criteria and situations which by their nature can present a higher risk of money laundering or terrorist financing. Such situations may include where the customer has not been physically present for identification

purposes; correspondent banking relationships; and business relationships and occasional transactions with politically exposed persons.

The Guidance Notes divide the risk-based approach into a number of discrete steps wherein the institution assesses the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks it faces. These steps are to:

- identify the money laundering and terrorist financing risks that are relevant to the institution;
- assess the risks presented by the institution's particular customers, products, delivery channels and geographical areas of operation;
- design and implement controls to manage and mitigate these assessed risks;
- monitor and improve the effective operation of these controls; and
- record appropriately what has been done, and why.

As the risk an institution faces may change from time to time, it is important that risk management be carried out on a dynamic basis. AML/ATF risk management processes must be kept under regular review and updated based on changes in the market environment.

4. Application of Group Policies to Branches and Subsidiaries Outside of Bermuda

The Bermuda AML/ATF framework is first and foremost concerned with the preventing of money laundering and terrorist financing which is connected to Bermuda, however, the Regulations do extend to the foreign branches and subsidiaries of AML/ATF regulated financial institutions. Pursuant to the Regulations, an AML/ATF regulated financial institution must require its foreign branches and subsidiaries to apply, to the extent permitted by the law of that jurisdiction, AML/ATF measures which are at least equivalent to those set out in the Regulations. Such measures are to include customer due diligence, record keeping and ongoing monitoring. If the foreign jurisdiction has a more rigorous AML/ATF framework than Bermuda, the foreign branches and subsidiaries are to adhere to those higher standards.

In the event that the law of the jurisdiction does not permit the branch or subsidiary to apply Bermuda equivalent measures, the AML/ATF regulated financial institution must inform the BMA and take additional measures to handle the risk of money laundering and terrorist financing.

PART D CUSTOMER DUE DILIGENCE

1. What is Customer Due Diligence

One of the key components of the AML/ATF framework is customer due diligence. Customer due diligence consists of identifying the customer and verifying their identity; identifying the beneficial owners of the customer and assessing on a risk-sensitive basis whether or not to verify those beneficial owners; and obtaining information on the purpose and intended nature of the business relationship.

Customer due diligence is necessary for two reasons:

- to assist the institution at the time due diligence is carried out, to be reasonably satisfied that customers are who they say they are, to know whether they are acting on behalf of another and that there is no legal barrier to providing them with the product or service requested; and

- to enable the institution to assist law enforcement agencies by providing available information on customers or activities being investigated.

2. Verification Procedures

The first step of customer due diligence is to identify and verify the identity of the customer on the basis of documents, data or information obtained from reliable and independent sources.

The Regulations do not define the term “customer” and accordingly its meaning is to be inferred from the definitions of “business relationship” and “occasional transaction”, the context in which the term is used in the Regulations and its common meaning. A “business relationship” is defined as a business, professional or commercial relationship between an institution and a customer, which is expected by the institution when contact is first made between them to have an element of duration. An “occasional transaction” means a transaction (carried out other than as part of a business relationship) amounting to \$15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked.

In situations where the Applicable Institution deems it necessary to verify the identity of the beneficial owners, the verification procedure may differ from the procedure used to verify the identity of a customer. As discussed, the identity of the customer must be verified by directly on the basis of documents, data or information obtained from reliable and independent sources. When verifying beneficial owners, the institution may, in accordance with its risk-based approach, make use of records in relation to the beneficial owners in the public domain, ask its customer for the relevant data or obtain the information otherwise. In some situations, it may be appropriate to rely on the information provided by the customer together with a confirmation that the beneficial owner is known to the customer.

Different identification and verification procedures will need to be applied depending on the customer, ie if the customer is an individual, company, trust or partnership.

a. Private Individuals

If the customer is a private individual, the Guidance Notes require the AML/ATF regulated financial institution to obtain at least the full name, residential address and date of birth of the individual. This information is to be verified using reliable and independent sources such as the individual’s passport, national identity document or other official document showing his or her photograph which has been issued by a government department.

b. Corporations

Verifying the identity of corporate customers is a two part process. Firstly, the Applicable Institution will need to verify the identity of the company itself. Secondly, it will need to identify, and possibly verify the identity of, the beneficial owner(s). Depending on the complexity of the customer’s corporate structure, it may be difficult for the Applicable Institution to determine the ultimate beneficial owner. However, in those situations, it may be even more important for the Applicable Institution to apply strict customer due diligence measures.

The information required to identify the company may include the full name, jurisdiction of incorporation, registered number, registered address in the jurisdiction of incorporation, business address, names of all directors and names of all beneficial owners. This information may be verified by obtaining

copies of the Certificate of Incorporation (or equivalent), the register of directors and officers and the register of members/shareholders.

The Regulations define the “beneficial owner” of a body corporate (other than a company whose securities are listed on an appointed stock exchange) to be any individual who ultimately owns or controls more than 25% of the shares or voting rights in the company; or otherwise exercises control over the management of the company.

Although directors do not fall within the definition of beneficial owner, the Applicable Institution, using a risk-based approach, may determine that it is necessary to verify the identity of some or all the directors of the company, in which case the verification procedure for individuals should be followed.

c. Trusts

With respect to trusts, which have no separate legal personality, the institution’s customer would be the trustees acting in their capacity as trustees of the trust and customer due diligence would be carried out based on whether the trustees are individuals, companies, partnerships, etc. In some situations, the institution may determine that, following a risk-based approach, the customers should be limited to those trustees who give instructions to the institution while the remaining trustees are to be verified as beneficial owners.

The information required to identify the trust may include the full name, country of establishment, nature and purpose of the trust, names of all trustees, names of all beneficial owners and name and address of any protector or controller, if applicable. This information may be verified by obtaining a copy of the trust deed or extracts therefrom.

The Regulations define the “beneficial owner” of a trust to mean any individual who is entitled to a specified interest in at least 25% of the capital of the trust property; as respects any trust other than one which is set up or operates entirely for the benefit of individuals with specified interests, the class of persons in whose main interest the trust is set up or operates; and any individual who has control over the trust.

The Guidance Notes recommend that AML/ATF regulated financial institutions verify the identity of all beneficial owners of the trust.

d. Partnerships

The information required to identify the partnership may include the full name, business address, names of all partners and names of all beneficial owners. This information may be verified by obtaining a copy of the partnership deed.

Similarly to trusts, in some situations, the institution may determine that, following a risk-based approach, the customers are those partners who give instructions to the institution while the remaining partners are to be verified as beneficial owners.

The Regulations define the “beneficial owner” of a partnership to mean any individual who is ultimately entitled to or controls more than a 25% share of the capital or profits, or of the voting rights in the partnership; or otherwise exercises control over the management of the partnership.

3. Timing of Verification

The Regulations require an Applicable Institution to apply customer due diligence measures when it:

- establishes a business relationship;
- carries out an occasional transaction;
- suspects money laundering or terrorist financing; or
- doubts the veracity or adequacy of documents, data or information already obtained for customer identification and verification.

Verification of the identity of the customer and where applicable, the beneficial owner, must subject to certain exceptions, take place prior to establishing a business relationship or the carrying out of an occasional transaction. Verification may be completed during the establishment of a business relationship in the following situations:

- Life assurance – verification must be completed at the very latest at or before the time of payout or at or before the time the beneficiary exercises a right vested under the policy;
- Opening of a bank account – verification must be completed at the very latest prior to any transactions being carried out by or on behalf of the account holder and there must be safeguards in place to ensure that the account is not closed;
- If necessary not to interrupt the normal conduct of business and there is little risk of money laundering or terrorist financing – verification must be completed as soon as practicable after the initial contact.

4. Ongoing Monitoring

In addition to the initial customer due diligence, Applicable Institutions are required to conduct ongoing monitoring of the business relationship. Ongoing monitoring shall consist of scrutiny of transactions undertaken throughout the course of the business relationship to ensure that the transactions are consistent with the Applicable Institution’s knowledge of the customer, his business and risk profile. Ongoing monitoring is also necessary to keep, so far as practicable, the documents, data or information obtained for the purpose of applying customer due diligence measures up to date.

5. Reliance on Third Parties

The Regulations permit an Applicable Institution to rely on certain third parties to apply any or all of the customer due diligence measures, provided however that consent to being relied on has been given by the third party. Applicable Institutions can only rely on third parties who fall within one of the following categories:

- AML/ATF regulated financial institutions or their foreign equivalents; or
- independent professionals who are supervised for the purpose of the Regulations by the Bermuda Bar Association or the Institute of Chartered Accountants of Bermuda², or their respective foreign equivalents.

² As at the date of this Guide, the Bermuda Bar Association and Institute of Chartered Accountants in Bermuda have not been designated as supervisory authorities by the Minister of Justice (in accordance with the Supervision Act) for the purposes of overseeing compliance by independent professionals with the Regulations.

With respect to the foreign third parties, the entities must be subject to requirements equivalent to those laid down in the Regulations and must be supervised for compliance in an equivalent manner. Foreign independent professionals also must be subject to mandatory professional registration recognised by law.

The Regulations do not provide how consent must be evidenced. Ordinarily consent means an acceptance of some form of proposal by one party to another – this may be written, oral, express or implied. A written acknowledgement confirms consent, however consent may also be inferred from conduct.

The basis of reliance is that the verification is of an equivalent standard to Bermuda, not based on simplified due diligence and must be directly performed by the institution being relied upon.

As a clarification, reliance on third parties for customer due diligence differs from the outsourcing of customer due diligence. In the case of the former, the Applicable Institution would be relying on the due diligence conducted by the third party with respect to the third party's customer (who would be a common customer) for the third party's own purposes. In the case of the latter, the third party acts as agent to the Applicable Institution and carries out the due diligence with respect to the customers of and for the purposes of the Applicable Institution. In either case, however, the Applicable Institution retains responsibility for any failure to comply with the requirement of the Regulations, as this responsibility cannot be delegated.

6. Requirement to Cease Transactions

Where an Applicable Institution is unable to apply customer due diligence in accordance with the Regulations, it must not establish a business relationship or carry out an occasional transaction with the customer. In particular, the institution must not carry out a transaction with or for the customer through a bank account. If there is an existing business relationship, the institution must take immediate steps to terminate the relationship. The Applicable Institution must consider the circumstances and reasons for the failure of the customer to provide the requested due diligence materials and determine whether it raises a suspicion of money laundering or terrorist financing. If there is a suspicion of money laundering or terrorist financing, the Applicable Institution must make a disclosure to the FIA.

The requirement to cease transactions does not apply where a professional legal adviser is in the course of ascertaining the legal position for his client or performing his task of defending or representing that client in or concerning legal proceedings including advice on instituting or avoiding proceedings.

7. Simplified Due Diligence

The Regulations recognise that not all situations warrant full customer due diligence. Section 10 of the Regulations sets out the circumstances where an Applicable Institution is not required to identify the customer or to verify the customer's identity or, where relevant, that of a beneficial owner, nor to obtain information on the purpose or intended nature of the business relationship.

Simplified due diligence ("SDD") may be applied when the customer is:

- an AML/ATF regulated financial institution;
- a financial institution (or equivalent) which is situated in a country other than Bermuda which has AML/ATF requirements equivalent to the Regulations 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 the monies are held is available on request to the institution acting as custodian for the account; or
- a public authority in Bermuda.

SDD may also be applied where the product falls within certain categories of insurance contracts or pension products, or where the product fulfills the all of the following conditions:

- the product has a written contractual base;
- any related transactions are carried out through an account of the customer with a bank which is subject to the Regulations (or to equivalent requirements in another jurisdiction);
- the product is not anonymous and its nature is such that it allows for the timely application of customer due diligence measures if and when the need arises;
- the product falls below the maximum threshold set out in the Regulations;
- the benefits of the product cannot be realised for the benefit of third parties, except in the case of death, disablement, survival to a predetermined advanced age, or similar events; and
- in the case of products allowing for the investment of funds in financial assets or claims, including insurance or other kinds of contingent claims the benefits of the product or related transaction are only realisable in the long term; the product or related transaction cannot be used as collateral; and during the contractual relationship, no accelerated payments are made, surrender clauses used or early termination takes place.

SDD is not permitted where the Applicable Institution suspects that a proposed business relationship or occasional transaction may involve money laundering or terrorist financing or it doubts the veracity or adequacy of documents, data or information already obtained for customer identification and verification.

The risks attached to the use of SDD remains solely with the Applicable Institution who may be required to demonstrate to the BMA the reasoning for the use of SDD.

The use of SDD provides an exemption from the basic verification obligation however this exemption does not extend to the Applicable Institution's obligation to conduct ongoing monitoring of the business relationship or to report suspicious activities.

8. Equivalent Jurisdictions

The Regulations and Guidance Notes make several references to countries and territories which have AML/ATF requirements which are equivalent to those set out in the Regulations ("Equivalent Jurisdictions"). The previous guidance notes issued by NAMLC contained a list of jurisdictions which it considered to be Equivalent Jurisdictions. This list was not adopted for the purpose of the new Guidance Notes. Applicable Institutions may obtain and make appropriate use of any government, IMF, World Bank, FATF, CFATF or other like regional body's findings concerning the approach to the prevention of money laundering or terrorist financing in particular countries or jurisdictions to make their own determination as to Equivalent Jurisdictions.

If the customer is connected with a non-Equivalent Jurisdiction, it does not prevent the Applicable Institution from establishing a business relationship or carrying out an occasional transaction with the customer. It may mean, however, that the Applicable Institution will need to apply enhanced due diligence.

9. Enhanced Due Diligence

An Applicable Institution must apply enhanced 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. Situations where EDD will be required include where a customer that has not been physically present for identification purposes; in respect of correspondent banking relationships; and in respect of business relationships or occasional transactions with a politically exposed persons (see Part D.10. below).

An Applicable Institution will need to hold sufficient information about the circumstances and business of its customers to inform its risk assessment, manage its money laundering and terrorist financing risks effectively and provide a basis for monitoring customer activity and transactions to help detect money laundering and terrorist financing. The institution should take into account the nature of the product or service and the customer’s business activities in deciding whether or not to seek additional information or documentation in assessing whether or not to accept a new customer.

10. Politically Exposed Persons

Politically exposed persons (“PEPs”) are individuals who have, or have had, a high political profile, or hold, or have held public office. PEPs can pose higher money laundering risks to an Applicable Institution as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known associates. A PEP status in itself does not incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category.

A PEP is defined as an individual who is or has, in a country or territory outside Bermuda, at any time in the preceding year, been entrusted with prominent public functions such as Heads of State, senior political figure, senior government, judicial or military officials, senior executives and their immediate family, their close associates and any corporate entity, partnership or trust arrangement that has been established by them or for their benefit.

Although an individual is no longer a PEP after he has left office for one year, institutions are encouraged to apply a risk-based approach in determining whether they should cease carrying out appropriate monitoring of his transactions or activities at the end of this period. In many cases a longer period is appropriate in order to ensure that the higher risks associated with the individual’s previous position have adequately abated.

PART E SUSPICIOUS ACTIVITY REPORTING

1. Suspicious Transactions

The POCA and ATF Act require that Applicable Institutions file a suspicious activity report (“SAR”) with the FIA if they have knowledge or suspicion a person is engaged in money laundering or terrorist financing as soon as is reasonably practicable after the information came to their attention in the course of their trade, profession, business or employment.

Having “knowledge” means knowing the existence of certain facts whilst “suspicion” is more subjective and falls short of proof based on firm evidence. Suspicion has defined through the courts as “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”.

Suspicious transactions may involve, among other things:

- transactions which are not typical for the customer based on the nature of his business;
- unusual patterns of transactions which have no apparent economic or visible lawful purpose;
- unusually linked transactions;
- unusual employment of an intermediary;
- unusual methods of payment; or
- unusual or disadvantageous early redemption of an investment.

Transactions which may be normal for one customer may be considered unusual for another. For this reason, it is very important that the Applicable Institution and its employees are familiar with their customers and their legitimate businesses and activities.

Suspicious may also be raised based on how the customer interacts with the Applicable Institution. For instance, if the customer gives the institution unusual directions for contacting him or is accompanied by someone with no apparent interest in the transaction. In some circumstances, an unusual interest in systems, controls and policies or knowledge of anti-money laundering or combating the financing of terrorism procedures may be cause for suspicion.

2. Reporting Suspicious Transactions

a. Internal Suspicious Activity Report

The obligation to report knowledge or suspicion of possible money laundering or terrorist financing affects all employees of an Applicable Institution. AML/ATF policies must require employees to make internal SARs to the MLRO where they have knowledge or suspicion that another person is engaged in money laundering or terrorist financing. The SAR should be concise and provide all relevant information to allow the MLRO to be able to determine if an external SAR should be filed with the FIA.

b. External Suspicious Activity Report

It is the responsibility of the MLRO to review all internal SARs and determine, in the light of all relevant information, whether or not the information or other matter contained in the report does give rise to such a knowledge or suspicion which should be reported to the FIA.

In making his determination, the MLRO must have access to and review all relevant information including the original customer due diligence. In some cases, it may be appropriate to obtain further information from the customer, however, care must be taken in such situations so as to avoid any possible tipping off of the customer.

Care should be taken when a filing is made prior to a transaction being completed that the filing does not lead to the unnecessary freezing of a customer's account, thus affecting other, non-suspicious transactions.

3. Tipping Off

It is a criminal offence under both the POCA and the ATF Act for a person who knows or suspects that the police are acting or proposing to act in connection with an AML/ATF investigation to disclose any information to any other person which is likely to prejudice that investigation or proposed investigation.

It is also a criminal offence for a person who knows or suspects that an internal or external SAR has been made to disclose any other information or any other matter which is likely to prejudice any investigation which might be conducted following such a disclosure.

Consequently, an Applicable Institution must not inform the customer that a transaction is being delayed because an SAR has been made or because the institution has been served a freezing funds notice from the FIA; nor can it inform the customer that law enforcement is conducting an investigation.

PART F FURTHER INTERNAL POLICIES AND PROCEDURES

1. Staff Training and Awareness

It is the responsibility of senior management to establish appropriate AML/ATF systems and procedures to prevent operations leading to money laundering and terrorist financing, including providing AML/ATF training to the other employees. Applicable Institutions are liable to civil penalties under the Regulations for not having adequate training and awareness arrangements in place.

AML/ATF training is required to make employees aware of the issue of money laundering and terrorist financing, relevant AML/ATF legislation and updates, and to assist them to understand their responsibilities and obligations within the AML/ATF framework.

Training must be provided to any employee who, during the course of his or her duties has, or may have, access to information which may be relevant in determining whether any person is engaged in money laundering or the terrorist financing.

Applicable Institutions should ensure that AML/ATF training occurs at regular intervals and the details of the training be recorded.

2. Record Keeping

Bermuda's AML/ATF framework requires institutions to obtain a significant amount of information from their customers to meet their AML/ATF obligations. It is important that such information is recorded and retained in a meaningful manner. The Regulations and the Guidance Notes provide institutions with direction as to the type of information to be recorded and the retention period for such records.

Applicable Institutions are required to retain copies of or references to the evidence obtained on customer identity for five years after the end of the customer relationship and details of customer transactions for five years from the date of the transaction.

It is recommended that Applicable Institutions maintain a register of SARs containing the details of all internal and external SARs. Such details may include the enquiries made by the MLRO in respect of the SAR; the MLRO's reasons for filing an external SAR; the information considered by the MLRO where no external report is filed; and communications made with or received from the authorities including the BMA and FIA.

Applicable Institutions should also maintain a register containing all relevant details of any enquiries made of them by the AML/ATF authorities (local or foreign), including any orders served on them. Such details may include the agency of the inquiring officer, the powers being exercised, and the details of the customer involved.

The Regulations do not require that the AML/ATF records be kept in Bermuda, however, if the records are not kept in Bermuda, the Applicable Institution must ensure that it is able to access and obtain copies of such records without undue delay.

PART G NON-LICENSED AML/ATF REGULATED FINANCIAL INSTITUTIONS

The Supervision Act requires all “non-licensed persons” to register with the BMA if they wish to carry on business activities in Bermuda. A non-licensed person is an AML/ATF regulated financial institution which is not already licensed under the Insurance Act 1978; the Credit Unions Act 1982; the Banks and Deposit Companies Act 1999; the Trusts (Regulation of Trust Business) Act 2001; the Investment Business Act 2003; the Investment Funds Act 2006; or the Money Service Business Regulations 2007.

In March 2009, the BMA issued a guidance note to clarify that for the purposes of the Supervision Act the term “licensed” is synonymous to “registered” or “authorised”. In other words, a non-licensed person is an AML/ATF regulated financial institution which is not already licensed, registered or authorised under the noted regulatory Acts. Examples of non-licensed persons are operators of an investment fund which is exempt from authorisation under the Investment Funds Act 2006 or operators of a private fund which is excluded from the Investment Funds Act 2006.

The deadline for registration is 30 June 2009, after which it is an offence for a non-licensed AML/ATF regulated financial institution to continue to carry on business if it is not appropriately registered. Non-licensed persons who commenced carrying on business after 1 January 2009 are required to register with the BMA prior to carrying on business.

PART H PENALTIES FOR NON-COMPLIANCE WITH THE AML/ATF FRAMEWORK

Failure to comply with the provisions of Bermuda’s AML/ATF legislation may lead to civil and criminal penalties including fines and/or imprisonment against the Applicable Institution and its employees.

Where a body corporate is guilty of an offence under the AML/ATF legislation and that offence is proved to have been committed with the consent or connivance of any director, manager, secretary or other similar officer of the body corporate or any person who was purporting to act in any capacity, he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

The main penalties under the AML/ATF legislation are as follows:

a. Proceeds of Crime Act 1997

For offences relating to the handling of proceeds of criminal conduct – eg concealing proceeds of crime, assisting another to retain proceeds of crime, or acquiring proceeds of crime – the penalty on summary conviction is imprisonment for five years and/or a fine of \$50,000. On indictment, the penalty is imprisonment for 20 years and/or an unlimited fine.

Offences relating to a failure to report or tipping off carry a penalty on summary conviction of imprisonment for three years and/or a fine of \$15,000. On indictment, the penalty is imprisonment for ten years and/or unlimited fine.

Offences relating to monitoring orders, production orders, search warrants, customer information orders and prejudicing investigations carry penalties ranging from imprisonment from two years and/or fines up to \$100,000.

b. Anti-Terrorism (Financial and Other Measures) Act 2004

Offences relating to fundraising or funding arrangements carry a penalty on summary conviction or imprisonment for 12 months and/or a fine of \$20,000. On indictment, the penalty is imprisonment for 14 years and/or a fine of \$200,000.

Offences relating to a failure to report or tipping off carry a penalty on summary conviction of imprisonment for six months and/or a fine of \$10,000. On indictment, the penalty is imprisonment for 14 years and/or a fine of \$200,000.

c. Proceeds of Crime Regulations 2008

Summary convictions under the Regulations carry a penalty of a fine of \$50,000 and on indictment the penalty is imprisonment for up to two years and/or a fine of \$750,000.

d. Proceeds of Crime Regulations (Supervision and Enforcement) Act 2008

Pursuant to the Supervision Act, the BMA may issue civil sanctions which carry a penalty not exceeding \$500,000 as it considers appropriate. The Statement of Principles sets out the criteria which the BMA will consider when determining the extent of the penalty.

In addition to the civil sanctions, the Supervision Act establishes certain criminal offences relating to registration under the Supervision Act, the appeal tribunal and disclosing restricted information. Such offences carry penalties ranging from 6 months to 5 years imprisonment and/or a fine of \$25,000 to \$100,000.

CONCLUSION

Bermuda has now had a number of year's experience working and doing business with anti-money laundering legislation in place. The recent bolstering of Bermuda's AML/ATF legislation allows regulatory authorities to cast a wider net to require more businesses to take responsibility toward the prevention money laundering and terrorist financing. The changes to the AML/ATF legislation put Bermuda well in line with international standards. Bermuda businesses as a whole have embraced anti-money laundering and anti-terrorist financing regulatory requirements and the international business sector continues to experience growth with Bermuda's reputation as a jurisdiction of integrity.

For more specific advice on anti-money laundering and anti-terrorist financing in Bermuda, we invite you to contact one of the following:

Cameron Adderley
Local Team Leader: Corporate Finance
+1 441 298 3229
cadderley@applebyglobal.com

Timothy Counsell
Local Team Leader: Banking & Asset Finance
+1 441 298 3212
tcounsell@applebyglobal.com

Alex Erskine
Global Team Leader: Funds & Investment Services
+1 441 298 3545
aerskine@applebyglobal.com

Timothy Faries
Global Team Leader: Insurance; Global Team Leader: Trusts
+1 441 298 3216
tfaries@applebyglobal.com

Appleby is the leading provider of offshore legal, fiduciary and administration services. With an unparalleled presence in the key offshore jurisdictions of Bermuda, the British Virgin Islands, the Cayman Islands, Isle of Man, Jersey, Mauritius and the Seychelles, the group offers advice on offshore law. We also have offices in the international financial centres of London, Hong Kong, Zurich and Bahrain.

Over 800 lawyers and professional specialists deliver sophisticated, specialised services, primarily in the areas of Corporate and Commercial; Litigation and Insolvency; Private Client and Trusts; and Property. We advise global public and private companies, financial institutions, and high net worth individuals, working with them and their advisers to achieve practical solutions, whether in a single location or across multiple jurisdictions.

This publication is intended only to provide a summary of the subject matter covered. It does not purport to be comprehensive or to provide legal advice. No person should act in reliance on any statement contained in this publication without first obtaining specific professional advice.

If this guide has been sent to you, and you would like to update your details or be removed from our marketing database, please contact the marketing department at Appleby or e-mail info@applebyglobal.com.

Bahrain

Bermuda

British Virgin Islands

Cayman Islands

Hong Kong

Isle of Man

Jersey

London

Mauritius

Seychelles

Zurich