ANTI-MONEY LAUNDERING/ ANTI-TERRORIST FINANCING GUIDANCE NOTES FOR REAL ESTATE BROKERS AND AGENTS IN BERMUDA

December 2017

Table of Contents

TABLE OF ABBREVIATIONS AND ACRONYMS

Act	Real Estate Brokers' Licensing Act 2017
AML/ATF	Anti-Money Laundering and Anti-Terrorism Financing
ATFA	Anti-Terrorism (Financial and Other Measures) Act 2004
BMA	Bermuda Monetary Authority
CDD	Customer due diligence
CTR	Cash transaction report
DNFBP	Designated non-financial businesses and professions
EU	European Union
FATF	Financial Action Task Force
FIA	Financial Intelligence Agency
FIA Act	Financial Intelligence Agency Act 2007
ML/TF	Money laundering and terrorist financing
NAMLC	National Anti-Money Laundering Committee
PEP	Politically exposed person
POCA	Proceeds of Crime Act 1997
REB	Real Estate Broker
Regulations	Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008
RE Regulations	– Real Estate Brokers' Licensing Regulations 2017
SAR	Suspicious activity report
SEA Act	Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008
UK	United Kingdom
UN	United Nations

INTRODUCTION

Over the years, Bermuda has enjoyed a high standard of living, due in part to its position as a premier international financial center. In keeping with this, there have been long-standing obligations to have effective procedures in place to detect and prevent money laundering and terrorist financing. The offence of money laundering has been contained in the Proceeds of Crime Act (POCA) since 1997 and obligations to combat terrorist financing set out in The Anti-Terrorism (Financial and Other Measures) Act (ATFA) since 2004. The original obligations on the financial sector in Bermuda have been in place since 1998.

Bermuda has committed itself to having a strong and robust framework to combat money laundering and terrorist financing. The international body responsible for outlining the minimum international expectations on such frameworks is the Financial Action Task Force (FATF). The FATF requires all jurisdictions to impose appropriate customer due diligence and other such regulatory requirements on entities in the financial sector (who are supervised by the BMA) and certain designated non-financial businesses and professions (DNFBP).

FATF Recommendations 22 and 23 outline obligations for DNFBPs which includes real estate brokers and agents when they are involved in transactions for their customers concerning the buying or selling of real estate.

Bermuda has taken steps to extend, as appropriate, the relevant legislative provisions to DNFBP sectors which are either required by the FATF, or are seen to pose a potential heightened level of risk for money laundering and terrorist financing in Bermuda.

DNFBP sectors are regulated in Bermuda from an anti-money laundering/anti-terrorist financing (AML/ATF) perspective by a number of different regulatory bodies:

- Real estate agents are supervised by the Superintendent of Real Estate;
- Lawyers and Accountants are supervised by the Barristers and Accountants AML/ATF Board;
- Corporate service providers and Trust providers are supervised by the BMA; and
- Casinos are supervised by the Bermuda Casino Gaming Commission.

The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (the SEA Act) designated the Superintendent of Real Estate (Superintendent) as being the supervisory authority responsible for ensuring that real estate brokers and real estate agents comply with the relevant AML/ATF Acts and Regulations. **Consequently, the Regulations will apply to real estate brokers and real estate agents who are licensed by the Superintendent to trade in real estate pursuant to the Act.**

These guidance notes have been prepared by the Superintendent to assist the licensed real estate brokers and real estate agents in Bermuda understand what is expected from them. The guidance includes:

- An outline of the legislation on anti-money laundering (AML), anti-terrorist financing (ATF) and international sanction measures;

- Explanation of the requirements of AML/ATF Acts and Regulations[1] and how these should be applied in practice;
- Specific good practice guidance on AML/ATF and international sanctions procedures;
- Information to assist licensed real estate brokers in designing and putting in place the systems and controls necessary to lower the risk of their business being used by criminals to launder money or finance terrorism.

HOW SHOULD THE GUIDANCE NOTES BE USED?

These guidance notes outline the laws and regulations of Bermuda to assist licensed real estate brokers in understanding and meeting their AML/ATF compliance obligations and provide comprehensive guidance to assist them to design and implement the systems and controls necessary to mitigate the risks of them being used in connection with ML/TF.

The guidance notes set out the minimum AML/ATF requirements for licensed real estate brokers.

Regulations 15-19 place a general obligation on licensed real estate brokers within its scope to establish adequate and appropriate policies and procedures to prevent ML and TF. Licensed real estate brokers may use the guidance notes as an aid in fulfilling their AML/ATF compliance obligations; however they must develop their own written business risk assessment document and AML/ATF policies and procedures that adequately mitigate the risks identified with their business.

Although these guidance notes generally provide a sound basis for licensed real estate brokers to meet their legal and regulatory obligations, effective risk mitigation may require additional measures beyond those set forth herein.

When a provision of the AML/ATF Acts or Regulations is directly described in the text of the guidance, the guidance notes use the term “must” to indicate that the provision is mandatory.

In other cases, the guidance notes use the term “should” to indicate ways in which the requirements of the AML/ATF Acts or Regulations may be satisfied, while allowing for alternative means, provided that those alternatives effectively accomplish the same objectives.

[1] Please refer to the Appendix 1 for the list of the key AML/ATF Acts and Regulations.

CHAPTER 1

DO THESE AML/ATF REQUIREMENTS APPLY TO YOU?

The AML/ATF requirements prescribed by Regulations apply to licensed real estate brokers and real estate agents who are involved in transactions for their customers concerning the buying and selling of real estate.

THE ROLE AND FUNCTIONS OF THE SUPERINTENDENT IN THE AML/ATF REGIME

The Superintendent is the supervisory authority for real estate brokers, for the purpose of detecting or preventing money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

As supervisory authority, the Superintendent has the duty to effectively perform all duties imposed by section 5 of the SEA Act, namely –

(1) Effectively monitor the licensed real estate brokers and take necessary measures for the purpose of securing compliance by licensed real estate brokers with AML/ATF Regulations;
(2) Issue guidance as to compliance with the AML/ATF Regulations, Part V of POCA and paragraph 1 of Schedule 1 to ATFA.

The Superintendent who, in the course of carrying out any of his functions, knows, suspects or has reasonable grounds to suspect that a real estate broker or real estate agent is engaging or has engaged, in money laundering or terrorist financing must inform the FIA.

The Superintendent has the powers conferred on him by the Act and the duty generally to supervise the real estate industry in his exercise of those powers. It is the Superintendent's duty to keep under review the operation of the Act and developments in the field of real estate which appear to him to be relevant to the exercise of his powers and the discharge of his duties. Also, the Superintendent must a make a report of his activities under the Act to the Minister[2] no later than six months after the end of each calendar year. The Superintendent, must publish a statement of principles, in such manner as he sees fit, in accordance with which he is acting or proposes to act-

(a) In interpreting the minimum criteria specified in Schedule 1 of the Act and the grounds for revocation specified in section 17 of the Act;
(b) In exercising his power to grant, revoke or refuse a licence;
(c) In exercising his power to obtain information and reports and to require production of documents; and
(d) In exercising his powers-
    (i) Under section 35 of the Act to impose a civil penalty;
    (ii) Under section 37 of the Act to censure publicity;

[2] Minister responsible for the Registrar of Companies

(iii) Under section 39 of the Act to make a prohibition order;

(iv) Under section 47 of the Act to publish information about any matter to which a decision notice relates.

If the Superintendent makes a material change to the principles, he must publish a statement of the change or the revised statement of principles in the same manner as he published the statement.

CHAPTER 2

WHAT IS MONEY LAUNDERING?

Money laundering is the process by which illegitimate or criminally derived money is made to appear legitimate. This result is achieved through a series of financial transactions designed to conceal the identity, source and/or destination of the criminally derived money. The process uses legal channels to conceal the criminal origins of illegal funds.

Money laundering generally involves three independent but sometimes simultaneous stages:

1. Placement: The physical placement or insertion of illegal money into the legitimate financial system. This stage deals primarily with cash proceeds of crime.
2. Layering: Separating the proceeds of criminal activity from their true origins by putting them through several layers of financial transactions.
3. Integration: This is the final stage of money laundering in which the criminal proceeds re-enter the legitimate economy, appearing to be derived from a legitimate source.

Under Bermuda law, money laundering involves the proceeds from any criminal conduct or any terrorist property. Criminal conduct includes all offences triable on indictment before the Supreme Court. Criminal conduct also includes all offences outside Bermuda that, had they occurred in Bermuda, would be triable on indictment before the Supreme Court. For more information, see section 3 of POCA and section 8 of ATFA.

The activities carried out at all stages of the money laundering process are criminalised under Bermuda laws by virtue of Sections 43 through 45 of POCA and Section 8 of ATFA. Money laundering is defined in POCA to include an attempt to commit an offence under Sections 43, 44 or 45.

Specific money laundering offences under Bermuda law include:

- Concealing or transferring proceeds of criminal conduct;
- Assisting another to retain proceeds of criminal conduct; and
- Acquisition, possession or use of proceeds of criminal conduct.

Examples of money laundering include:

- Attempting to turn money raised through criminal activity into legitimate or clean money;
- Involvement with any criminal or terrorist property, or entering into arrangements to facilitate the retention or control of criminal or terrorist property; and
- The investment of proceeds of crime in further criminal activity or in financial products and services.

There are three broad groups of offences related to money laundering that REBs need to avoid committing. These are:

- Knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of the proceeds of criminal conduct;
- Failing to report a knowledge or suspicion that another person is engaged in money laundering; and
- 'Tipping off.' i.e. intending to prejudice an investigation knowing or suspecting that a disclosure has been made to the Intelligence Unit of the FIA or that the police are acting or proposing to act in connection with an investigation into money laundering.

Regardless of whether or not money laundering actually takes place, it is also a separate offence under the Regulations for REB to fail to establish adequate and proportionate policies and procedures to prevent and detect money laundering.

The techniques used by money launderers constantly evolve, responding to the source, type and amount of funds to be laundered, and to the legislative, regulatory and law enforcement environment of the market in which the money launderer wishes to operate. Techniques employed may be local to a municipality, or they may be practiced commonly around the globe. One source of guidance on global money laundering methods is available at www.fatf-gafi.org.[3]

INHERENT RISKS OF MONEY LAUNDERING ASSOCIATED WITH CASH TRANSACTIONS

Cash is the mainstay of much organized criminal activity. For the criminal, it has the obvious advantage of leaving no discernable audit trail. Cash is also a weakness for criminals. Whilst they hold cash they are more at risk of being traced to the predicate offence. They will therefore often seek to dispose of cash into high value goods.

Money launderers normally want to move funds quickly in order to avoid detection. This is more easily done in one-off transactions. The purchase of high value goods, paid for in cash, with good portability represents an attractive area for money launderers. Goods purchased with cash that can easily be sold on (even for a loss) for 'clean money' are especially attractive. High value goods are also a useful store of value and may form part of a criminal lifestyle. Goods purchased would generally be luxury items that could be potentially sold on through the black market, for example, jewelry, antiques and high performance cars.

INTERNATIONAL CASE STUDY OF MONEY LAUNDERING

Use of Illegal Funds in Mortgage Loans and Interest Payments

This case originates in the Netherlands. Mr. X was the owner of Company A and the individual controlling its activities. Mr. X hired Mr. Y as front man of Company A. Company A had some low-profile activities in managing and exploiting properties. During the life of Company A, Mr. Y set up a relationship with Bank EUR

[3] The most recent FATF reports covering AML/ATF specific for high value goods can be found here: http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-risks-vulnerabilities-associated-with-gold.pdf, http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf

that provided for accounts and payment services. The property managed by Company A was used by other companies owned by Mr. X for activities such as storage, for example. Mr. X planned to buy office buildings for EUR 8,000,000 through Company A. The office buildings had to be renovated to be marketable. Mr. X knew a licensed assessor (real estate agent), Mr. Z.

Mr. X and Mr. Z found a way to set up false but plausible assessments of the market value of the office buildings after renovation in the amount of EUR 13,000,000, or EUR 5,000,000 greater than the true market value of the office buildings. Mr. X ordered Mr. Y to negotiate a mortgage with Bank EUR to finance the purchase and renovation of the property. Based on the assessment, Bank EUR was willing to grant a mortgage of EUR 13,000,000. Mr. Y entered into the loan agreement on behalf of Company A as the buying party. The real estate was paid for after the disbursement of the loan. Mr. X then paid Mr. Y EUR 500,000 and had the remaining EUR 4.5 million, together with the proceeds of other criminal activities, transferred into several bank accounts in countries with strict bank secrecy. The mortgage of Bank EUR was presented to the foreign banks as the legitimate source of the funds that were being transferred to the accounts. In this way, the money was layered and integrated.

The renovation of the office buildings never took place. Meanwhile the activities of Company A rapidly decreased. Company A finally went into default. Bank EUR called the loan, but Mr. Y was not in a position to reimburse it along with the interest payment. Mr. Y stated that he was not aware of the persons behind Company A, their whereabouts and the background of the accounts to which the money was transferred. The predicate offences identified in this case were forgery, deception, and fraud.

Indicators and methods identified in the scheme included:

- Applying for a loan under false pretenses;
- Using forged and falsified documents;
- The customer persisted in a picture of the financial situation that was unrealistic or that could not be supported by documents;
- The loan amount did not relate to the value of the real estate;
- Successive buying and selling of the real property involved; and
- The customer had several mortgage loans relating to several residences.

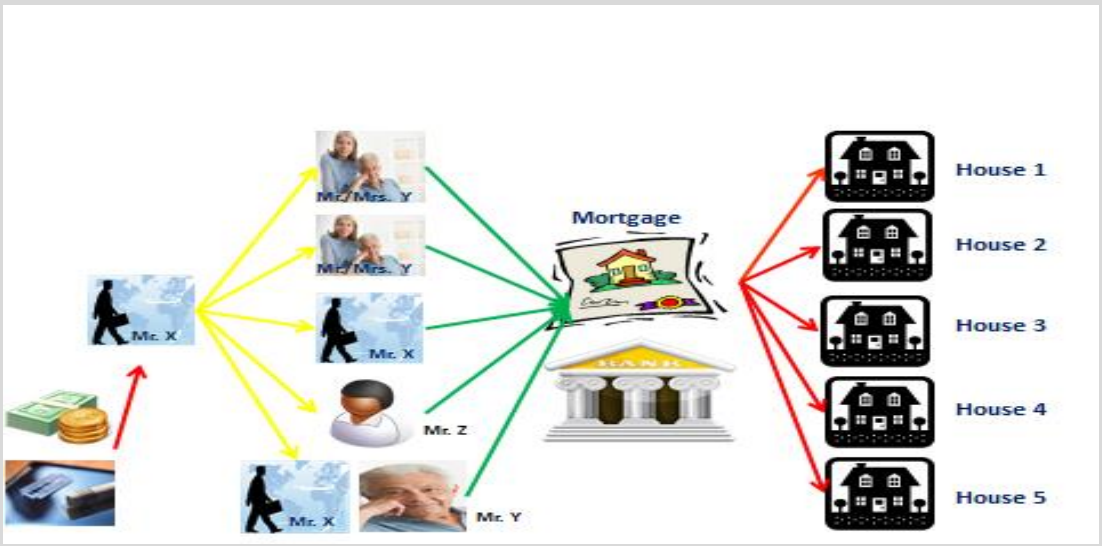
Overvaluation of real estate and use of third parties launder funds

This case originates from Canada. The parents of Mr. X (Mr. and Mrs. Y) purchased a residential property and secured a mortgage with a Canadian bank. In his mortgage application, Mr. Y provided false information related to his annual income and his ownership of another property. The property he had listed as an asset belonged to another family member. Mr. and Mrs. Y purchased a second residence and acquired another mortgage at the same Canadian bank. A large portion of the down payment came from an unknown source (believed to be Mr. X). The monthly mortgage payments were made by Mr. X through his father's bank

account. This was the primary residence of Mr. X. Investigative evidence shows that Mr. X made all mortgage payments through a joint bank account held by Mr. and Mrs. Y and Mr. X.

Mr. X then purchased a residential property and acquired a mortgage from the same Canadian bank. Mr. X listed his income (far higher than the amounts he had reported to Revenue Canada) from Company A and Company B. Mr. X made the down payment and monthly payments. Over two years, Mr. X paid approximately CAD 130 000 towards the mortgage. During this time his annual legitimate income was calculated to be less than CAD 20 000. Mr. X also used his brother Mr. Z as a front man (nominee) on title to purchase an additional property. Investigators discovered that Mr. Z had stated an annual income of CAD 72 000 on his mortgage application listing his employer as Mr. X although Mr. Z had never worked for his brother, and his total income for two years was less than CAD 13 000. Mr. X made the down payment on this property, and his tenants, who were members of Mr. X's drug trafficking enterprise, paid all the monthly mortgage payments. A total of CAD 110 000 was paid towards this property until Mr. X and his associates were arrested. Mr. X and his father purchased a fifth property. The origin of the down payment, made by Mr. Y, was unknown but is believed to be the proceeds of Mr. X's drug enterprise. Monthly payments were made by Mr. X. The use of real estate was one of many methods Mr. X employed to launder the proceeds from his drug enterprise. Recorded conversations between Mr. X and his associates revealed that he felt it was a fool-proof method to launder drug proceeds. Mr. X was convicted in 2006 of drug trafficking, possession of the proceeds of crime and laundering the proceeds of crime in relation to this case.

The use of real estate was one of many methods Mr. X employed to launder the proceeds from his drug enterprise. The only problem he faced was securing a mortgage alone, so he had to use a nominee to secure the mortgage or to co-sign on the mortgage.



Laundering the proceeds of drug trafficking through the real estate sector

In November 2003, law enforcement agencies of Country 1 took Mr. TM in for questioning, as well as Mr. AN who is suspected of being an intermediary between TM and a Columbian cartel. Questioned by the judge, Mr. TM denied any participation in the cocaine trafficking network between Columbia, Country 1 and Europe. His associate, Mr. NA, on the other hand, had revealed the existence of drug business relations between Mr. TM and Columbians Y and Z, and had narrated how and by what means the drugs were transported to Europe via Country 1. In January 2004, a team from the French drug enforcement agency and the French judiciary police arrived in Country 1 in order to take in Mr. TM for interrogation. This French intervention was justified by the fact that the two traffickers taken in for questioning in Paris for being in possession of 6 kg of cocaine had already declared being in the service of Mr. TM. But well informed by the accomplices, Mr. TM was taken into custody for interrogation and handed over by the law enforcement agencies of country 1.

An international regulatory commission visited Country 1, within the framework of the investigation of the case that was opened by a French investigation firm for hearing.

Mr. TM, who claimed to be a trader in his country, made large investments in the real estate sector with a significant number of constructions as well as a vehicles park with diverse brands, ranging from low- to high-quality luxury vehicles.

Use of the real estate sector to launder proceeds of crime by a Politically Exposed Persons (PEP)

The FIU was requested by one of the domestic Law Enforcement Agencies to assist in locating properties and associated companies linked to a high-profile PEP. The case related to a money laundering investigation on a former high ranking PEP in the continent who embezzled huge sums of monies from the state coffers of his jurisdiction. Three countries were involved in the case that is, the Republic of South Africa (RSA), the home country of the PEP.

The information received revealed that the PEP owned a high value property, worth approximately ZAR 2 million in one of the most sought after, prime residential areas in RSA. Further revelations were that the PEP, whilst in the third party country, contacted his local associates (lawyers) to assist in procuring real estate. To transfer funds the PEP utilised a shell company registered in another country as a conduit to ensure that his identity is not revealed. The attorney's trust account in the RSA received the funds and duly purchased the property and registered it under another company's name, which analysis revealed to be controlled by the PEP. A financial intelligence product was compiled and disseminated, leading to a joint application by the three investigating agencies for restraining and forfeiture of the real estate to the home country of the PEP, where funds were misappropriated.

Laundering through real estate using an offshore shell company

A PEP was involved in a syndicate in which state funds were siphoned from government coffers. The syndicate incorporated a shell company in a foreign country. When the PEP's term of office came to an end, investigations were instituted relating to a corruption matter that took place during the PEP's time in office. Investigations revealed that the syndicate siphoned millions of dollars using another government account from which wire transfers were made to offshore accounts including to the shell company. It was further revealed that the shell company was used to acquire a number of real estate properties in the PEP's country

and abroad. Money was used by the PEP to pay his school children's fees and upkeep abroad. He also bought large quantities of expensive clothing and his children started living a lavish life style. Upon conclusion of the investigation, the trio was arrested for corruption, theft and money laundering. The properties were seized and a number of them were forfeited to the state.

International Drug Trafficking Case

The FIU received a request for information from a local law enforcement agency on a person of interest that was known to be a king-pin in an international drug trafficking syndicate. The information required included bank accounts and properties under the subject's name, including those of his immediate family members and possible close associates. The FIU commenced with the analysis cycle and requested financial information from reporting institutions. Statutory and private databases were also accessed to source more information such as his movement in and out of the country and assets under his name or the name of his family. The information received and analysis conducted revealed that the subject had transferred huge sums of funds into the country, and further bought assets such as real estate and a game farm. It was also revealed that outward funds transfers were made to his home country and the funds were deposited into different bank accounts. Some of the funds were transferred into the spouse's account. This information was duly consolidated into a report and forwarded to the relevant authorities. Ultimately properties and funds to the amount of ZAR 3 million were seized by the State.

WHAT IS TERRORISM FINANCING?

Terrorism financing is the direct or indirect solicitation, collection or provision of financial or other material assistance for terrorism or for terrorist organizations or persons who encourage, plan or engage in terrorism or for their travel to perpetrate, plan or participate in terrorist acts or for providing or receiving training for that purpose.

Terrorism financing could involve funds raised from legitimate sources, such as personal or institutional donations and profits from businesses, as well as it may involve funds from criminal sources, such as the drug trade, arms smuggling, fraud, abduction and corruption. The primary objective of persons seeking to finance terrorism is not to conceal the source of funds, but to conceal the financing and the terrorist nature of the financed activity.

Terrorists and terrorist groups may have established links with organized crime groups and may use those links to move funds through the same channels as money launderers. Larger, property-owning terrorist groups may operate similarly to organized crime groups or governments, raising funds through various processes, including forms of "taxation". Other groups and individuals, however, may operate on a smaller scale, but nonetheless with devastating effect. Terrorism financing has two notable features:

- Terrorists are often funded from legitimately obtained income, including charitable donations and business profits; and
- Individual terrorist acts have been carried out using relatively small sums of money.

In seeking to evade detection by the authorities and to protect the identity of the ultimate beneficiaries, persons involved in terrorism financing use techniques similar to those employed by money launderers. REBs have substantively the same duty to combat terrorism financing as they do to prevent money laundering.

Specific terrorism financing offences under Bermuda law include:

- Fund raising for the purposes of terrorism;
- Soliciting, collecting or providing money or other property for the purposes of financing terrorist organisations or financing persons participating in terrorism;
- Using or possessing money or other property that is intended to be used for the purposes of terrorism;
- Participating in arrangements to make money or property available for the purpose of terrorism; and
- Financing a person's travel to perpetrate, plan or participate in terrorist acts or for providing or receiving training for that purpose.

Examples of terrorism financing include:

- Soliciting donations to a terrorist organization;
- Purchasing antiquities or natural resources from a terrorist organization; and
- Providing support to terrorist organizations.

Examples of activity which may indicate possible terrorism financing:

- Buying gold, jewelry, antiques or cars for the purpose of exporting them to countries bordering the conflict zones.
- Multiple identification documents containing inconsistent information provided by the same individual or multiple individuals using the same identification documents.

Regardless of whether or not terrorist financing actually takes place, it is also a separate offence under the Regulations for institutions to fail to establish adequate and proportionate policies and procedures to prevent and detect terrorist financing.

Bermuda law criminalises the financing of terrorist actions that occur both in and outside Bermuda. Bermuda law also criminalises the financing of terrorist actions by both individuals and legal entities.

WHAT ARE INTERNATIONAL SANCTIONS?

An important component of Bermuda's anti-terrorism financing system is the implementation of international sanctions against groups, entities and individuals designated as terrorists by the UN Security Council, the EU and UK (when such designations are extended to Bermuda by the UK).

International Sanctions are enforcement measures, usually of an economic nature, that are implemented for political reasons by countries and international organisations to maintain or restore international peace and

security. The principal purpose of international sanctions is usually to change the behavior of the individual, group, company, organisation, industry or political regime that is targeted by the sanction. Numerous different sanctions may be in effect at any given time. Most sanctions include information as to why they have been imposed and what their aim is.

The Government of Bermuda is committed to playing its role in the maintenance of international peace and security, and therefore as a British Overseas Territory, implements the international sanctions obligations of the United Kingdom. All REBs must be cognizant of any sanctions regimes in place in Bermuda and be in compliance with the applicable sanctions requirements. Refer to the NAMLC website for further details: https://www.gov.bm/international-sanctions-measures .

Any failure by an entity or person to comply with the requirements of the Bermuda Sanctions Regime will lead to criminal and/or civil liability.

CHAPTER 3

WHAT ARE THE CORE AML/ATF LEGAL OBLIGATIONS OF REBs?

1. Supervision by the Superintendent

All REBs will be subject to a periodic visit from the Superintendent or a body to whom the Superintendent has delegated its powers to test compliance with AML/ATF Acts and Regulations.

It is intended that some REBs will receive a visit in the FIRST YEAR of the operation of this regime.

The Superintendent will provide feedback on any weak areas or any areas where a business may not be in compliance with the legislation.

2. Obligations of REBs

- Appoint a reporting officer and a compliance officer[4];
- Develop, submit to the Superintendent and maintain AML/ATF written policies and procedures and business risk assessment;
- Perform assessment of the risks to money laundering and terrorism financing, and measures to mitigate high risks;
- Perform customer due diligence and ongoing monitoring;
- Submit suspicious activity reports to the FIA;
- Retain all relevant records at least 5 years
- Conduct regular AML/ATF training for staff
- Co-operate with the FIA and the Bermuda Police Service as required in any money Laundering or financing of terrorism investigation;
- Maintain an independent audit function to be conducted by a qualified independent third party or internally by persons independent of any other function
- Submit annual statistical returns to the Superintendent

3. Management responsibility

For the purposes of these guidance notes, the term "management" refers to one or more of the following:

- The board of directors as a single decision-making body;
- One or more appropriate directors;

[4] They can be one and the same person.

- A “chief executive” who, either alone or jointly with one or more persons, is responsible under the immediate authority of the directors for the conduct of the business of the REB;
- A “senior executive” other than a chief executive who, under the immediate authority of a director or chief executive of the REB, exercises managerial functions or is responsible for maintaining accounts or other records of the REB.

Management must apply a risk-based approach for the purposes of preventing and detecting ML/TF. In doing so, REBs may draw upon experience applying proportionate, risk-based policies across different aspects of its business[5].

Under a risk-based approach, REBs should identify and assign risk ratings to their customers, products, services, transactions, delivery channels, outsourcing arrangements and geographic connections.

Management must be fully engaged in decision-making processes, and must take ownership of the risk-based approach. Management is accountable where the approach is determined to be inadequate.

Management for all REB must adopt a formal policy[6] in relation to the prevention and detection of ML which addresses the following:

- Ensure compliance with the relevant Acts and Regulations;
- Identify, assess and effectively mitigate the ML/TF risks to its customers, transactions, delivery channels, outsourcing arrangements and geographic connections;
- Ensure that AML/ATF risk assessment framework remains relevant and appropriate given the REB’s risk profile;
- Management must oversee the establishment, maintenance and effectiveness of the REB’s AML/ATF policies, procedures and controls;
- Appoint a Reporting Officer and Compliance to process disclosures;
- Screen employees against high standards;
- Ensure that adequate resources are devoted to the REB’s AML/ATF policies, procedures and controls;
- Recognise potential personal liability if legal obligations not met.

REBs should apply adequate resources to counter the risk that they may be used for the purposes of financial crime. This includes systems and controls to prevent money laundering and terrorist financing. The level of resource should reflect the size, complexity and geographical spread of the REB customer and product base.

[5] Regulation 16.
[6] See Appendix 2 for a Policy Statement & Risk Assessment Template

4. Offences, fines and penalties

REBs should be aware that Regulation 19 provides that failure to comply with the requirements of specified Regulations is a criminal offence and carries with it significant penalties. On summary conviction, a fine of up to $50,000 and conviction on indictment, a fine of up to $750,000 or imprisonment for a term of two years.

Further, Section 20(1A) of the SEA Act empowers the Superintendent to impose a civil penalty on a REB up to $250,000 for each failure to comply with regulations referred to in subsection (3).

For full details concerning the civil penalties process, see Chapter 4 of the SEA Act. The SEA Act also provides for criminal offences. For example, Section 33 creates offences, which carry significant penalties if convicted, whether summarily or on indictment.

In deciding whether a person has committed an offence against the Regulations the court must consider whether any relevant guidance, issued at the time, was followed. The Superintendent must also consider whether any relevant guidance was followed when deciding if an institution has failed to comply with the Regulations.

Where a person has been convicted of an offence under the Regulations he shall not be liable to a civil penalty imposed by any other statutory provision in relation to the same matter.

5. Compliance policies and procedures

Compliance policies and procedures outline how you are planning to comply with your AML/ATF obligations and help demonstrate your commitment to prevent, detect and address non-compliance.

The formality of these policies and procedures depends on your needs. Generally, the degree of detail, specificity and formality of the program varies according to the complexity of the issues and transactions you are involved in. It will also depend on your risk of exposure to money laundering or terrorist financing. For example, the compliance policies and procedures of a small business may be less formal and simpler than those of a bank.

What is important for your compliance policies and procedures is that they are communicated, understood and adhered to by all within your business who deal with customers or any property owned or controlled on behalf of customers. This includes those who work in the areas relating to customer identification, record keeping, and any of the types of transactions that have to be reported. They need enough information to process and complete a transaction properly as well as identify customers and keep records as required.

They also need to know when an enhanced level of caution is required in dealing with transactions, such as those involving countries or territories that have not yet established adequate anti-money laundering programs consistent with international standards.

Your compliance policies and procedures should incorporate, at a minimum, the reporting, record-keeping, and customer identification requirements applicable to you.

Although directors and senior officers may not be involved in day-to-day compliance, they need to understand the statutory duties placed upon them, their staff and the entity itself.

Appendix 2 provides a proposed outline for AML/ATF policies and procedures as well as key questions that should be answered when developing your policies and procedures.

6. AML/ATF risk management

Risk based approach

A risk-based approach should balance the costs to the business and its customers with a realistic assessment of the risk of the business being used for money laundering and terrorist financing. It focuses effort where it is needed and will have most impact.

A risk-based approach requires a number of steps to be taken to determine the most cost effective and proportionate way to manage and mitigate ML/TF risks faced by the business. The steps are to:

- Identify the money laundering and terrorist financing risks that are relevant to the business;
- Assess the risks presented by the particular
  - customers – types and behavior
  - products and services
  - delivery channels, for example, electronic, wire transfer or cheque
  - geographical areas of operation, for example, location of business premises, source or destination of customers' funds
- 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.

Businesses can decide for themselves how to carry out their risk assessment, which may be simple or sophisticated in accordance with the business they operate.

A risk assessment will often result in a stylised categorisation of risk, for example, high, medium and low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the level of identification, verification, additional customer information and ongoing monitoring, in a way that minimises complexity.

Where a REB meets the minimum risk based approach measures outlined in this guidance, it is sufficient for them to develop a business risk assessment that takes into account the level of complexity of their business, and implemented policies and procedures specific to their business. However, if a REB is a more complex business or wishes to adopt practices different to those outlined in these guidance notes, it must develop and document ready for inspection by the Superintendent its own business risk assessment, policies, procedures and practices that meets the regulatory requirements for their business.

Risk assessment

A risk-based approach starts with the identification and assessment of the risk that has to be managed. Appendix 3 proposes a risk tool that allows REB to assess their ML/TF risks by identifying higher risk customers and activities. For these higher risk customers and activities additional vigilance and control measures should be applied as described in the managing and mitigating the risk section below.

Managing and mitigating the risk

The higher the risk a REB faces from any particular combination of customer, product, service, transaction, delivery channel or geographic connection, the stronger and/or more numerous the mitigation measures must be.

Examples of risk mitigation measures include:

- applying customer due diligence measures to verify the identity of customers and any beneficial owners
- obtaining additional information on customers
- conducting ongoing monitoring of the transactions and activity of customers with whom there is a business relationship[7]
- having systems to identify and scrutinise unusual transactions and activity to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may be taking place.

A more extensive list of mitigation and control measures can be found at Appendix 3.

Ongoing monitoring and improving the effectiveness of controls

The assessment of ML/TF risk is not a static exercise. Risks that have been identified may change or evolve over time due to any number of factors, including shifts in customer conduct, the development of new technologies, and changes in the marketplace, including the rise of new threats. Each REB should re-evaluate and update its risk-based approach on a regular basis, at a minimum every two years and each time the risk factors change.

Registered REBs should ensure that their AML/ATF policies and procedures and business risk assessment are reviewed to assess the implications of:

- Delivery channels;

[7] See the Appendix 5 for definition of "business relationship".

- New ML/TF trends or typologies;
- New regulatory guidance;
- Changes in customer portfolios or conduct;
- Changes in delivery channels;
- Changes in business practices; and
- Changes in the law.

REBs should pay special attention to any money laundering or terrorist financing risks that may arise from sale and purchase transactions, delivery channels, or geographic connections that might favour anonymity. REBs should take appropriate measures, where risk dictates, to prevent their use for money laundering or terrorist financing purposes.

Appointment of Reporting Officer, Compliance Officer

Reporting Officer

REBs (other than sole REBs) must appoint a Reporting Officer[8] with the authority to carry out the following duties:

- Receive suspicious activity and cash threshold disclosures from the REB's employees;
- Access all necessary records in a timely manner;
- Make final determinations on whether disclosures should be reported to the FIA; and
- Where appropriate, make external reports to the FIA.

The Reporting Officer may be, but is not required to be a member of management. At a minimum, however, the REB must ensure its Reporting Officer is adequately trained to carry out this role.

The Reporting Officer would be subject to the fit and proper under Section 11A of the SEA Act.

Compliance Officer

REBs must appoint a Compliance Officer[9], who must be a member of management with sufficient authority to:

- Oversee the establishment, maintenance and effectiveness of the REB's AML/ATF policies, procedures and controls;
- Monitor compliance with the relevant Acts, Regulations and guidance; and
- Access all necessary records in a timely manner.

The Compliance Officer and Reporting Officer may be the same individual (but they must be a member of management team in such a case). The Compliance Officer would be subject to the fit and proper test under Section 11A of the SEA Act.

[8] Regulation 17.
[9] Regulation 18A.

Appointment of Compliance Officer and Reporting Officer should be documented. All relevant employees of the REB should be aware of the identity of the Compliance Officer and Reporting Officer and any deputies, and that all relevant employees are aware of the procedures to follow when suspicion arises.

REB should notify the Superintendent of the name and contact information of the Compliance Officer, Reporting Officer and any deputies, and of any subsequent changes. Receipt of such information enhances the Superintendent's ability to communicate effectively with REBs. Information should be sent via realestatelicense@gov.bm.

7. Customer due diligence

When is customer due diligence applied?

REBs must apply customer due diligence[10] (CDD) on every transaction.

REBs must –
Identify and verify the customer's identity of both individuals and legal persons and entities.

Identify both buyer and seller

- Identify the beneficial owner, verify the beneficial owner's identity, and, where relevant, understand the ownership and control structure of the customer; and
- Understand the purpose and intended nature of the business relationship.

When to identify customer?

- When you carry out an occasional transaction;
- When you establish a business relationship;
- When you suspect money laundering and terrorist financing;
- When you have doubts about the veracity or adequacy of documents

Identification should occur when a contractual relationship is established, that is, when –

- There is a listing agreement;
- There is an agreement of purchase and sale;
- At the latest, at the time of sale for other party involved in the transaction.

For Individuals:

- Use government issued documentation such as driver's licence, passport and voter's identification;
- The identification document must be original. Copies are not acceptable;

[10] The term "customer" in the real estate sector refers to customers of the real estate broker or agent.

- Must identify existing customers when the identification document that was recorded has expired; and
- Must obtain and understand the purpose and intended nature of the business relationship.

For legal persons or arrangements:

- The customer/client who is conducting the transaction;
- Verifying that the person who is conducting the transaction is in fact authorized to act on behalf of the customer and identifying and verifying the identity of that person;
- Identifying the name and verifying the identity of the chief executive or similar position;
- Beneficial owner who owns or controls the legal person or arrangement (must identify a natural person);
- Understanding the ownership and control structure of legal person, trust or arrangement
- Must obtain and understand the purpose and intended nature of the business relationship.

IF THE CDD MEASURES CANNOT BE COMPLETED, THE TRANSACTION SHALL NOT BE CARRIED OUT AND SERIOUS CONSIDERATION SHOULD BE GIVEN TO REPORTING AN SAR TO THE FIA.

CDD for legal persons or legal arrangements

The following information must be recorded:

- Full name and trade name;
- Date and place of incorporation, registration or establishment;
- Registered office address, and if different, mailing address;
- Whether and where listed on stock exchange;
- Official identification/registration number (where applicable)
- Name of regulator (where applicable)
- Legal form, nature and purpose (e.g. discretionary, testamentary, bare); and
- Control and ownership

Customers that are not physically present

Non-face-to-face customers are higher risk, therefore one or more of the following additional steps must be implemented:

- Verifying the customer's identity with additional information;
- Supplementary measures to verify or certify documents supplied or requiring confirmatory certification by an AML/ATF regulated financial institution;
- Ensuring that the first payment is carried out through an account opened in the customer's name with a banking institution.

Reliance on third parties[11]

REBs are permitted to rely on a third party to identify customers provided that:

- The REB relies on financial institutions or independent professionals that are subject to AML/ATF requirements in Bermuda with equivalent requirements abroad;
- The person must consent to be relied upon;
- The REB must immediately obtain information sufficient to identify customers;
- The REB must be satisfied that reliance is appropriate given the level of risk for the jurisdiction in which the party to be relied upon is usually a resident;
- The REB cannot rely on a person if it is likely that access to information will be impeded by confidentiality or data protection restrictions.

Please note, however that ultimately, the responsibility for customer due diligence rests with REBs.

Finally, third parties must make available identification information as soon as practicable.

Outsourcing[12]

REBs are permitted to outsource some of their AML/ATF systems and controls, however involving other entities in the operation of a REB brings an additional dimension to the risk that the REB faces and this risk must be actively managed.

REBs cannot contract out their legal responsibilities, and therefore remain responsible for systems and controls in relation to the activities outsourced.

Such verification may be completed during the establishment of a business relationship if:

- this is necessary not to interrupt the normal conduct of business; and
- there is little risk of money laundering or terrorist financing occurring, provided that the verification is completed as soon as practicable after contact is first established; and
- any money laundering or terrorist financing risks that may arise are effectively managed.

REBs must review the documents, data and information they hold in relation to a customer to ensure that the records are up-to-date, adequate, and relevant to the business relationship or transaction. Once the REB has verified the identity of a customer and any beneficial owners, it should re-verify where:

- Doubts exist as to the veracity or adequacy of the evidence previously obtained for the purposes of identifying and verifying the customer and any beneficial owners;
- There is suspicion of money laundering or terrorist financing in relation to the customer;

[11] Regulation 8
[12] Regulation 9

- The customer's activities are inconsistent with the REB's understanding of the purpose and intended nature of the business relationship;
- There is a material increase in the risk rating assigned to the customer, or to the products, services, delivery channels, or geographic connections with which the customer engages.

What is on-going monitoring?

REBs must conduct on-going monitoring where there is a business relationship with a customer. **This will not apply to one-off transactions/occasional transactions.**

On-going monitoring of a business relationship means:

- Investigating transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the REB's knowledge of the customer and the customer's business and risk profile;
- Investigating the background and purpose of all complex or unusually large transactions, and unusual patterns of transactions which have no apparent economic or lawful purpose and recording in writing the findings of the investigation; and
- Reviewing existing documents, data and information to ensure that they are relevant, sufficient, and up-to-date for the purpose of applying CDD measures.

Why is it necessary to apply CDD measures and on-going monitoring?

The CDD and on-going monitoring obligations under the Regulations are designed to make it more difficult for REBs to be used for money laundering or terrorist financing.

REBs need to know the identities of their customers in order to guard against impersonation and other types of fraud, and to avoid committing offences under the POCA and the ATFA relating to ML/TF.

Carrying out CDD and on-going monitoring allow REBs to:

- Be reasonably satisfied that customers are who they say they are;
- Know whether a customer is acting on behalf of another;
- Be aware of changes to the customer's risk profile;
- Identify any legal barriers (e.g. international sanctions) to providing the product or service requested;
- Maintain a sound basis for identifying, limiting and controlling risk exposure of assets and liabilities; and
- Assist law enforcement by providing information on customers or activities being investigated.

In those instances where an REB has established a business relationship, on-going monitoring is an integral part of a REB'S AML/ATF program and supports several objectives:

- Maintaining a proper understanding of a customer's activities;
- Ensuring that CDD documents and other records are accurate and up to date;

- Providing accurate inputs for the REB's risk assessment processes;
- Testing the outcomes of the REB's risk assessment processes; and
- Detecting and scrutinizing unusual or suspicious transactions.

On-going monitoring of a business relationship includes:

- Scrutinising transactions undertaken throughout the course of the relationship (including, where necessary, the source of wealth and/or source of funds) to ensure that the transactions are consistent with the REB's knowledge of the customer and his risk profile;
- Investigating the background and purpose of all complex or unusually large transactions, and unusual patterns of transactions which have no apparent economic or lawful purpose, and recording in writing the findings of the investigation; and
- Reviewing existing documents, data and information to ensure that they are up-to-date, adequate and relevant for the purpose of applying CDD measures.

These guidance notes describe a minimum level of acceptable CDD and on-going monitoring measures. In practice, REBs often require additional information for the purposes of managing risks and providing products and services.

Standard customer due diligence measures for individuals[13]

Customer identification and verification of individuals

A customer is generally the natural person (individual or individuals) with whom a business relationship is established, or for whom a one-off transaction is carried out.

Transactions separated by an interval of three months or more need not be treated as linked, provided there is no evidence of a link and the transactions do not otherwise give rise to a business relationship.

Standard identification requirements for individuals

In those instances when CDD must be applied, a REB must obtain the following information in relation to each private individual:

- Full name, any former names (e.g. maiden name) and other names used;
- Principal residential address;
- Date of birth;
- Place of birth;
- Nationality;
- Gender; and
- A personal identification detail (number or other unique identifier contained in a valid government-issued document, issuing authority, date of issue, expiry date).

[13] Regulation 5.

Documentary verification

A REB should verify the information provided by the customer based upon:

- Either a valid government issued document, such as a passport, national identity card, or driving licence that incorporates the individual's full legal name and photograph and at least one of the following:
  - Principal residential address;
  - Date of birth
- or a government issued document lacking a photograph, such as a birth certificate, which incorporates the individual's full legal name, supported by one or more additional documents which incorporate the individual's full legal name and cumulatively provide both of the following:
  - Principal residential address; and
  - Date of birth.

International sanctions check

REBs must check the customer against the sanctions lists. Links to the various consolidated lists for sanctions check to be performed are available on the International Sanctions page of the website of the National Anti-Money Laundering Committee. The web address is https://www.gov.bm/international-sanctions-measures .

Identification of beneficial owners

A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. In respect of customers who are private individuals, the customer himself is the beneficial owner, unless there are features of the transaction or surrounding circumstances that indicate otherwise.

Screening

It is recommended that REBs should at least perform an internet based search on the individual for negative information, or information that may suggest there may be a non-legitimate source of the funds or purpose for the transaction. If possible this search should be performed prior to the transaction occurring, or be performed within 5 working days of the transaction.

Enhanced customer due diligence measures for individuals[14]

Customer identification and verification of individuals

Enhanced CDD is the application of additional CDD measures where necessary to ensure that the measures in place are commensurate with higher ML/TF risks (the standard CDD measures are still required to be performed).

[14] Regulation 11.

REBs must apply enhanced CDD on a risk sensitive basis in circumstances where there is a higher ML/TF risk which may arise due to factors associated with a customer or the products, services, delivery channels, or geographic location of counterparties with which the customer engages.

In selecting the appropriate additional measures to be applied, REBs should obtain additional information, including the following:

- Occupation and name of employer/source of income; and
- Details concerning any public or high-profile positions held.
- Additional information on the source of funds and source of wealth of the customer;

The Regulations prescribe specific types of relationship in respect of which enhanced CDD measures must be applied. Those that are applicable to REBs are:

- Where the customer has not been physically present for identification purposes; and
- Transactions with a PEP.

Non face-to-face customers identification and verification[15]

The extent of verification in respect of non-face-to-face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering or terrorist financing risk presented by the customer. Additional measures would also include assessing the possibility that the customer is deliberately avoiding face-to-face contact. It is therefore important to be clear on the appropriate approach in these circumstances.

Where the customer has not been physically present for identification purposes, a REB must take specific and adequate measures to compensate for the higher-risk, for example by applying one or more of the following measures:

- Ensuring that the customer's identity is established by additional documents, data or information;
- Supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by an institution in an equivalent jurisdiction; or
- Ensuring that the first payment of the operation is carried out through an account opened in the client's name with a bank.

Politically exposed persons (PEPs)[16]

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

- Have appropriate risk-based procedures to determine whether a customer is a PEP[17];
- The requirements of Regulation 11(4), which stipulate the Enhanced Due Diligence measures, do not apply to Domestic PEPs[18], unless the transaction or relationship with that Domestic PEP is determined to pose a higher risk ML/TF. The Enhanced Due Diligence measures in Regulation 11(4) are mandatory for all Foreign PEPs.

[15] Regulation 11(2).
[16] Regulation 11(4)-(7).
[17] See Appendix 4 for further details on who is a PEP.
[18] Regulation 11(6B)

- Obtain appropriate senior management approval for establishing a business relationship with such a customer;
- Take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship, occasional or unusual transactions; and
- Conduct on-going monitoring of the business relationship.

The nature and scope of a particular institution's business will generally determine whether the existence of PEPs in their customer base is an issue for the REBs, and whether or not the business needs to screen all customers for this purpose. In the context of this risk analysis, it would be appropriate if the REB's resources were focused in particular on products and transactions that are characterized by a high-risk of ML or TF.

Documentary verification and approval

In selecting the appropriate additional measures to be applied, REBs should obtain additional documentation to perform verification measures and higher level of approval for the transaction to proceed including the following:

- Documentation to verify either the source of funds or source of wealth of the customer;
- Approval of management to commence or continue the business relationship.

8. Record keeping[19]

Record-keeping is an essential component of establishing an audit trail. Proper record-keeping enables AML/ATF processes to keep criminal funds out of the financial system and, when required, detect criminal funds and ensure their confiscation by the authorities. Proper record-keeping also serves to demonstrate the work REB have undertaken in complying with their legal and regulatory obligations.

To comply with the Regulations and these guidance notes, the records a REB keeps should be such that:

- The REB's managers and auditors will be able to assess the effectiveness of the REB's AML/ATF policies and procedures (training and compliance monitoring including information about the effectiveness of the training);
- Any transactions or instructions effected via the REB on behalf of any particular customer can be reconstructed;
- Any customer can be properly identified and located;
- A customer profile can be established for all customers for whom CDD was conducted;
- All suspicions identified internally and all SARs made externally can be understood; and
- The REB can satisfy, within a reasonable time frame, any authorised information requests or court orders from the appropriate authorities.

[19] Regulations 15, 16.

Customer information[20]

In relation to the evidence of a customer's identity, REB must keep a copy of, or the references to, the evidence of the customer's identity obtained during the application of CDD measures.

A REB may often hold additional information in respect of a customer obtained for the purposes of enhanced CDD or on-going monitoring.

Transactions

All transactions which require the REB to conduct CDD must be recorded with the REB's records. Transaction records in support of the entries in the accounts, in whatever form they are used, should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect customer.

Internal and external reports

REBs should make and retain:

- Records of actions taken under the internal and external reporting requirements; and
- When the Reporting Officer has considered information or other material concerning possible money laundering or terrorist financing, but has not made a report to the Intelligence Unit of the FIA, a record of the other material that was considered.

In addition, the REB should retain copies of any SARs made to the Intelligence Unit of the FIA.

Other records

A Registered REB's records should include:

(a) in relation to training:

- Dates AML/ATF training was given;
- The nature of the training;
- The name(s) of the person(s) giving the training;
- The names of the staff who received training; and
- The results of the tests undertaken by staff, where appropriate.

(b) in relation to Reporting Officer/Compliance Officer monitoring –

- Reports by the Reporting Officer/Compliance Officer to management; and
- Records of consideration of those reports and of any action taken as a consequence.

A REB must establish and maintain systems which enable it 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.

[20] Regulation 15(2), (3), (4).

Forms in which records have to be kept

Most businesses have standard procedures which they keep under review, and will seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be:

- By way of original documents;
- By way of photocopies of original documents;
- On microfiche;
- In scanned form; or
- In computerized or electronic form.

The record retention requirements are the same, regardless of the format in which they are kept, or whether the transaction was undertaken by paper or electronic means.

Timing[21]

REBs must keep specified records **for a period of at least five years** following the date on which the business relationship ends or in the case of an occasional transaction, following the date on which the transaction or the last in a series of transactions is completed. Whilst the Regulations do not state where the relevant records should be kept, the overriding objective is for REBs to be able to retrieve this information without undue delay.

9. Reporting of suspicious sale and purchase transactions

General provisions

Under POCA and ATFA, REBs must report suspicious activity[22]. The requirement for a REB to report a suspicious transaction applies if the REB has knowledge or suspicion[23] that another person is engaged in money laundering or terrorist financing. This applies when the information comes to the REB in course of his trade, profession, business or employment and not only when the financial transaction has been completed, but also when it has been attempted.

Where a transaction or activity giving rise to knowledge or suspicion of money laundering or terrorist financing has been completed, a person does not commit an offence if after doing the act (or after information about the doing of the act comes to his attention) and on his own initiative he makes an external report as soon as it is reasonable for him to make it. This principle applies equally to an employee of a REB who makes an internal report to the Reporting Officer about his knowledge or suspicion, in accordance with the REB's policies, procedures and controls, provided that the report is made on his own initiative as soon as it is reasonable for him to make it.

[21] Regulation 15.
[22] Section 46 of POCA, Schedule 1 of ATFA.
[23] Refer to the Appendix 8 for the details regarding the terms "knowledge" and "suspicion".

Consent[24]

Under POCA and ATFA, a person does not commit a money laundering or terrorist financing offence if, prior to carrying out the transaction or activity, he makes an external report to the Intelligence Unit of the FIA and later carries out the transaction or activity with the express consent of the FIA.

Where the consent of the FIA is not forthcoming, REBs may seek guidance from the FIA regarding information that can be provided to the customer in relation to any delay in or enquiries into the carrying out the transaction or activity. Any guidance provided by the FIA does not constitute legal advice.

Consent applies only where there is prior notice to the FIA of the transaction or activity. The FIA cannot provide consent after the transaction or activity has occurred.

Internal reporting[25]

REBs must require that anyone in the business to whom information or other matter comes in the course of business as a result of which they know or suspect, that a person is engaged in money laundering or terrorist financing, complies with section 46 of the POCA or Schedule 1 Part 1 of the ATFA (as the case may be). This includes staff having an obligation to make an internal report to the Reporting Officer as soon as is reasonably practicable after the information or other matter comes to them.

Any internal report should be considered by the Reporting Officer, in the light of all other relevant information, to determine whether or not the information contained in the report does give rise to knowledge or suspicion of money laundering or terrorist financing.

REBs are expected to use its existing customer information effectively by making such information readily available to its Reporting Officer.

In most cases, before deciding to make a report, the Reporting Officer is likely to need access to the REB's relevant business information. REBs should therefore take reasonable steps to give its Reporting Officer access to such information. Relevant business information may include details of:

- the financial circumstances of a customer or beneficial owner, or any person on whose behalf the customer has been or is acting; and
- the features of the transactions, including, where appropriate, the jurisdiction in which the transaction took place, which the institution entered into with or for the customer (or that person).

In addition, the Reporting Officer may wish:

- to consider the level of identity information held on the customer, and any information on his personal circumstances that might be available to the REB; and
- to review other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship and identification records held.

[24] Section 44(3)(b)(i); 45(5)(b) of POCA; Section 12 of ATFA.
[25] Regulations 16, 17; Section 46 of POCA, Schedule 1 of ATFA.

If the Reporting Officer concludes that the internal report does give rise to knowledge or suspicion of money laundering or terrorist financing, he must make a report to the Intelligence Unit of the FIA as soon as is reasonably practicable after he makes this determination.

If the Reporting Officer decides that the internal report DOES NOT warrant a suspicious report being filed with the FIA, then the reasons for not doing so should be clearly documented and retained with the internal report.

External reporting[26]

How to make a suspicious activity report

All employees, regardless of whether they have a compliance function, are obliged to report to the Reporting Officer within the office of the REB each instance in which they have knowledge or suspicion that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing.

Each internal report to the Reporting Officer should be documented or recorded electronically and retained.

Each internal report should include full details of the customer and the suspicious and/or unusual transaction and as full a statement as possible of the information or activity which gave rise to the knowledge or suspicion.

The Reporting Officer must have the ultimate authority to evaluate internal suspicious activity reports and to determine whether an external suspicious activity report is appropriate under the AML/ATF Acts and Regulations. Where, after evaluating an internal suspicious activity report, the Reporting Officer determines that there is knowledge or suspicion that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing, the Reporting Officer must file an external suspicious activity report with the Intelligence Unit of the FIA via the goAML system, which is available at www.fia.bm.

In order that an informed overview of the situation may be maintained, all contact between particular departments/branches and the Intelligence Unit of the FIA or law enforcement should be controlled through, or reported back to a single contact point, which will typically be the Reporting Officer. In the alternative, it may be appropriate to route communications through an appropriate member of staff in the REB's legal or compliance department.

A SAR's intelligence value is related to the quality of information it contains. A REB needs to have good base data from which to draw the information to be included in the SAR; there needs to be a system to enable all the relevant information to be produced in hard copy for the Intelligence Unit of the FIA, or law enforcement, if requested under a court order. A REB should include in each SAR as much relevant information about the customer, transaction or activity as it has in its records.

[26] Regulation 16, 17, Section 46 of POCA, Schedule 1 of ATFA.

Transactions following a disclosure

REBs must remain vigilant for any additional transactions by, or instructions from, any customer in respect of which a disclosure has been made, and should submit further disclosures, to the FIA, as appropriate[27].

The disclosure provisions within POCA and the ATFA protect persons making SARs from any potential breaches of confidentiality, however imposed. These provisions apply to any person who makes a report and includes reports that are made voluntarily, in addition to reports made in order to fulfill reporting obligations.

Whether to terminate a business relationship is essentially a commercial decision, and a REB must be free to make such judgments. However, in the circumstances envisaged here a REB should consider liaising with the Intelligence Unit of the FIA to consider whether it is likely that termination would alert the customer or prejudice an investigation in any other way. If there is continuing suspicion about the customer or the transaction or activities, and there are funds which need to be returned to the customer at the end of the relationship, REBs should seek guidance from the Intelligence Unit of the FIA before repatriating the funds.

10. Tipping-off

Section 47 of POCA and Section 10A of ATFA contain tipping-off offences.
It is an offence if a person knows or suspects or has reasonable grounds that an internal or external report has been made to the Reporting Officer or to the FIA and the person discloses to any other person:

- Knowledge or suspicion that a report has been made; or
- Any information or other matter likely to prejudice any investigation that might be conducted following such a disclosure.

It is also an offence if a person knows or suspects or has reasonable grounds that a police officer is acting or proposing to act in connection with an actual or proposed investigation of money laundering or terrorist financing, and the person discloses to any other person any information or other matter likely to prejudice the actual or proposed investigation.

Reasonable enquiries of a customer regarding the background and purpose of a transaction or activity that has given rise to suspicion, form an integral part of CDD and on-going monitoring. Where such enquires are conducted in a manner that does not indicate any suspicion, they should not give rise to tipping-off.

Where a REB has reason to be concerned that CDD enquiries may tip-off the customer or otherwise prejudice an investigation, the REB should not perform the CDD and should file a suspicious activity report with the Intelligence Unit of the FIA in lieu of performing the CDD[28].

[27] Sections 44(3)(a), 45(5)(a), 46(1) of POCA and Schedule 1 of ATFA.
[28] Regulation 6(5) and 6(6).

11. Staff awareness, training and employee screening

REBs must take appropriate measures[29] so that all relevant employees of it are—

- made aware of the law relating to money laundering and terrorist financing;
- regularly given training in how to recognise and deal with transactions which may be related to money laundering or terrorist financing; and
- screened prior to hiring to ensure high standards.

Management of REBs is responsible for the oversight of the REB's AML/ATF systems and controls which include trainings its employees in relation to ML/TF. REBs are liable to civil penalties if they do not have adequate training and awareness programmes in place for their employees. REBs must also take steps to assess the effectiveness of its training.

Who should be trained?

For the purposes of these guidance notes, the term 'employee' includes any person working for a REB including real estate agents. A relevant employee is one 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 funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing; or
- At any time plays a role in implementing and monitoring compliance with AML/ATF requirements.
- All customer-facing staff will require training to recognize and handle suspicious transactions.
- The relevant employee includes an individual working on a temporary basis whether under a contract of employment, contract for services or otherwise.

What should the training cover?

REBs must take appropriate measures to ensure that relevant employees:

- Are aware of the AML/ATF Acts and Regulations;
- Undergo training on how to identify transactions which may be related to ML/TF;
- Know how to properly report suspicions regarding transactions that may be related to ML/TF.

Each REB must also ensure that relevant employees receive appropriate training on its AML/ATF policies and procedures relating to:

- Customer due diligence measures;
- On-going monitoring;
- Reporting of suspicious and cash transactions;
- Record-keeping;
- Internal control;
- Risk assessment and management.

[29] Regulation 18.

A REB's training programme should be on-going, and should take into consideration the risks the REB has identified through its business risk assessment. AML/ATF training should be done at least annually for all staff and management team members. A REB should ensure that employees receive appropriate training as their job functions and work sites change. Training methods and assessments should be determined by the individual REB according to the size and complexity of its business.

12. Independent audit[30]

The independent audit function should provide for an internal audit of the REB's AML/ATF policies, procedures and controls. REBs should conduct an audit to monitor and sample test the implementation, integrity and effectiveness of their AML/ATF policies, procedures and controls on a regular basis. This means at least once a year and more frequently when management becomes aware of any gap or weakness in the AML/ATF policies, procedures or controls, or when management deems it necessary due to the REB's assessment of the risks it faces.

Where appropriate, having regard to the risk of ML/TF and the size of the business, the audit may be undertaken by the compliance and/or internal auditing departments. The audit should be adequately resourced to help ensure AML/ATF compliance and it should be carried out independently of any general audit. The independent audit does not require the establishment of a separate dedicated department or section, only that the audit itself is sufficiently separate and distinct, focused solely on AML/ATF matters and not found within the general audit.

The audit function should:

- Evaluate the risk ratings the REB has assigned with respect to its size, customers, products, services, transactions, delivery channels, outsourcing arrangements and geographic connections;
- Assess the adequacy of the REB's AML/ATF policies, procedures and controls including:
  - Risk assessment;
  - Customer due diligence;
  - Risk mitigation and other measures to manage higher risks;
  - On-going monitoring;
  - Detecting and reporting suspicious activity;
  - Record-keeping and retention; and
  - Reliance and outsourcing relationships;
- Test compliance with the relevant laws and regulations;
- Test the AML/ATF controls for the REB's transactions and activities, with an emphasis on higher-risk areas;
- Assess employees' knowledge of the relevant Bermuda Acts, Regulations and guidance, the REB's policies and procedures and the role of each employee within the office of the REB; and

[30] Please note that the independent audit required by Regulation 17A is separate and apart from the REB's obligation to submit to the Superintendent a report by the auditors pursuant to section 23(3) of the Act

- Assess the adequacy, accuracy and completeness of employee training and awareness programmes.

The audit should be documented, or recorded electronically, and retained in accordance with the guidance provided in Section XIII. The results of the audit should be included in reports to management and the Board for timely action.

Appendix 1. AML/ATF Acts and Regulations

A full, up-to-date listing of Bermuda legislation is available at www.bermudalaws.bm. Key elements of the AML/ATF framework in Bermuda include:

- Revenue Act 1898
- Criminal Code Act 1907
- Criminal Justice (International Cooperation) (Bermuda) Act 1994
- Proceeds of Crime Act 1997 ("POCA")
- 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
- Financial Intelligence Agency Act 2007
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 ("Regulations")
- Proceeds of Crime Appeal Tribunal Regulations 2009
- Proceeds of Crime (Designated Countries and Territories) Order 1998
- The Extradition (Overseas Territories) Order 2002
- Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008
- The Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011 (An unofficial Consolidation of the Terrorist Asset-Freezing etc. Act 2010 and the above Order is provided on the website for ease of reference)
- Guidance Notes for AML/ATF Regulated Financial Institutions on Anti-Money Laundering & Anti-Terrorist Financing
- International Sanctions Act 2003 and International Sanctions Regulations 2013
- Real Estate Brokers' Licensing Act 2017
- Real Estate Brokers' Licensing Regulations 2017

The AML/ATF framework in Bermuda has been revised pursuant to the following international standards and requirements:

- The FATF Recommendations (as amended November 2017).
- UN Security Council Resolutions 1267 (1999), 1373 (2001), and subsequent resolutions 1333 (2000), 1390 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008), 1904 (2009), 1989 (2011), 2083 (2012), and 2161 (2014).
  http://www.un.org/en/sc/documents/resolutions/2016.shtml

FATF Guidance

- Available at www.fatf-gafi.org

Appendix 2. Template for Anti-Money Laundering/Anti-Terrorism Financing (AML/ATF) Policies and Procedures

This is a proposed template for REB's AML/ATF policies and procedures. The use of this template is not required however the questions outlined below should be addressed when developing your firm's AML/ATF policies and procedures.

Address | City Postal Code| Telephone
Email

Entity Name

Policies and procedures

Describe the following regarding your policies and procedures:

- The role of the compliance officer
- How you will communicate the policies and procedures to employees and staff as well as branches and subsidiaries
- How you will reflect changes to AML/ATF legislative and regulatory requirements
- How often you will update your policies and procedures
- How often you will conduct an independent audit of your AML/ATF compliance program?

Risk Assessment and Risk mitigation (Section 16 of the Proceeds of Crime Act Regulations)

Describe how you will comply with your risk assessment and risk mitigation obligations including:

- Identifying what customers and situations you have identified as higher risk (copy of the risk assessment should be attached)
- What mitigation and control measures you will be implementing to reduce the risk?
- How you will document the risk of any new product or services?
- How often you will update the risk assessment?

Customer due diligence (CDD): (Sections 5, 6 and 8 of the Proceeds of Crime Act Regulations)

Describe how you will comply with CDD requirements including:

- When will you identify the buyer and seller of a real estate transaction?
- What information will you collect when you identify a natural person?
- What information will you collect when you identify legal persons and legal arrangements?
- What identification documents are acceptable?
- Indicate that only original documents will be acceptable
- How will you identify customers that are not physically present?

- What will you do if you cannot complete customer due diligence measures?

Record Keeping (Section 15 of the Proceeds of Crime Act Regulations)

Describe how you will comply with record keeping requirements including:

- How long will you retain records related to real estate transactions?
- What records will you retain?
- Where will records be retained?
- How will you ensure that information can be provided in a timely manner to the Superintendent of Real Estate, the Financial Intelligence Agency and the Bermuda Police Service (BPS)?
- If you are using a third party to conduct customer due diligence measures:
    - How you will ensure that they are properly identifying customers
    - How you will gain access to information in a timely fashion

Enhanced due diligence (Section 11 of the Proceeds of Crime Act Regulations)

Describe how you will comply with enhanced due diligence requirements including:

- What enhanced due diligence measures will be applied to:
    - Persons or transactions involving a country identified as higher risk by FATF?
    - Persons or transactions involving higher risk countries for ML, TF, and corruption or subject to international sanctions?
    - Any other situation representing a higher risk of ML/TF including those that you have identified in your risk assessment?

Politically Exposed Persons (Section 11 (4) of the Proceeds of Crime Act Regulations)

Describe how you will comply with enhanced due diligence requirements to politically exposed persons including:

- A definition of what is a politically exposed person?
- How you will identify politically exposed persons?
- How you will seek approval from senior management?
- How you will take adequate measures to establish source of wealth and source of funds?
- How you will conduct ongoing monitoring?

Ongoing monitoring (Section 7 of the Proceeds of Crime Act Regulations)

Describe how you will comply ongoing monitoring requirements including:

- How you will conduct ongoing monitoring for:
    - Business relationships (after 2 transactions involving purchase or sale of real estate)
    - Complex and unusual transactions
    - Unusual patterns of transactions or activities which have no economic or lawful purpose
- How you will record the findings?

Suspicious Activity Reporting (Sections 46 & 47 of the Proceeds of Crime Act)

Describe how you will comply with suspicious activity reporting requirements including:

- Defining what is a suspicious activity?
- How you and your employees/agents will identify suspicious activities (should refer to ML/TF indicators)
- Who is your reporting officer?
- State your procedures for how employees/agents should raise suspicions to the reporting officer?
- Specify that SARs filed with the FIA are confidential

Training (Section 18 of the Proceeds of Crime Act Regulations)

Describe how you will comply with training requirements including:

- How you will screen employees to ensure high standards before hiring?
- How you will train employees/agents on:
    - How to identify a suspicious transaction?
    - What are the firm's AML/ATF obligations?
    - How to implement your policies and procedures?

Appendix 3. Risk Assessment Form

Name of Real Estate Firm :_____

The *Proceeds of Crime (Money Laundering and Anti-Terrorism Financing) Regulations* requires real estate brokers to conduct a risk assessment of your exposure to money laundering and terrorism financing and apply corresponding mitigation and controls. This checklist is meant to assist you in meeting these obligations. This form is presented as an example only. You may choose to conduct your risk assessment using a different approach.

Instructions: When you answer yes to one of the questions, this situation or customer is considered higher risk and a control measure to reduce the risk should be applied. A suggested control measure is proposed for each higher risk customer or situation. You can adapt the control measures to correspond to your business (see Annex A for list of control measures).

The results of this risk assessment should be communicated to all real estate agents and employees that deal with customers. The training should include a review of what is considered higher risk and the corresponding control measures. The date of the training should be documented. You should review your risk assessment every two years.

Risk Assessment

Higher risk customers and situations	**Yes** Higher risk	**No** Low risk	**Suggested Control Measures**
Customers			
Are your customers foreigners?			• Determine if individuals are politically exposed persons. • Obtain additional information on source of funds or source of wealth.
Do you have customers who are politically exposed persons?			• Obtain broker approval to conduct the transaction. • Obtain additional information on source of funds or source of wealth. • Monitor any future real estate transactions.
Is your customer an intermediate vehicle such as a company, trust, foundation, partnership, LLC or other legal arrangement that makes it			• Obtain name of person(s) behind company, trust, foundation, partnership, LLC or other legal arrangement.

difficult to determine the beneficial owner?			• Obtain additional information on organizational structure. • Obtain additional information on source of funds or source of wealth.
Are your customers intermediaries (i.e. lawyers and accountants acting on behalf of customers)?			• Obtain name of person(s) on whose behalf the transaction is being conducted. • Obtain additional information on source of funds or source of wealth.
Has one of your customers been named in the media as being involved with criminal organizations?			• File Suspicious Activity Report (SAR). • Obtain additional information on source of funds or source of wealth.
Do you have a customer that is purchasing a property that is not within his or her means based on his stated occupation or income?			• Obtain additional information on source of funds or source of wealth.
Do you have customers that engage in activities that are consistent with the indicators identified for Suspicious Activities? (See Annex X for suspicious indicators specific to real estate).			• Consider filing a Suspicious Activity Report (SAR). • Obtain additional information on source of funds or source of wealth.
Geographic Risk			
Are any of your customers or the source funds originate from countries subject to sanctions, embargoes or similar measures issued by Bermuda or International Organizations such as the United Nations ("UN")? Bermuda United Nations: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list			• Obtain broker approval to proceed with the transaction. • Ask for additional form of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth or source of wealth.
Are any of your customers or the source funds originate from countries identified as financial secrecy havens or jurisdictions? http://www.oecd.org/countries/monaco/listofunco-operativetaxhavens.htm http://www.imolin.org/imolin/finhaeng.html#Map.%20%20Major%20Financial%20Havens			• Obtain broker approval to proceed with the transaction. • Ask for an additional form of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.

• Are any of your customers or the source funds originate from countries identified by the Financial Action Task Force (FATF) as having strategic deficiencies in the fight against money laundering or subject to an FATF statement? FATF: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)			• Obtain broker approval to proceed with the transaction. • Ask for an additional form of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.
• Are any of your customers or the source funds originate from countries identified by credible sources as providing funding or support for terrorist activities?			• Obtain broker approval to proceed with the transaction. • Ask for an additional form of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.
• Are any of your customers or the source funds originate from countries identified by credible sources as having significant levels of corruption, or other criminal activity? http://www.transparency.org/news/feature/corruption_perceptions_index_2016			• Obtain broker approval to proceed with the transaction. • Ask for an additional form of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.
Delivery channel and business practices			
Do you accept cash?			• Confirm source of funds • Set limits to cash transaction amounts. • Request bank drafts instead of accepting large amounts of cash.
Do you conduct transactions where you do not meet the customer?			• Deliver comprehensive AML/ATF training specifically focused on customer due diligence requirements • Ask for an additional form of identification to confirm the identity. • Conduct periodic review of records to ensure that customer due

			diligence requirements are adequately implemented
Do you have customers that are referred to you by a third party?			• Conduct customer due diligence measures directly. • Conduct periodic review of records to ensure that customer due diligence requirements are respected by third party.
Do you have short-term or part-time agents?			• Include ML/TF obligations in job descriptions and performance reviews. • Deliver comprehensive AML/ATF training for all new employees
Do you undertake high value transactions (over $5 million)?			• Pay special attention for unusual transaction and ML/TF indicators. • Obtain additional information on source of funds or source of wealth.
Other risk factors: (list any additional factors)			

_____

Signature of the Broker ***Date***

Date of employee training: _____

2. Examples of Risk Control Measures:

1. Obtain broker or compliance officer approval to proceed with the transaction.
2. Ask for an additional form of identification to confirm the identity.
3. Obtain name of person(s) behind corporation, trust, partnership, LLC, foundation or other legal arrangement.
4. Monitor if customer conducts additional real estate transactions.
5. Obtain information on source of funds or source of wealth of the customer.
6. Deliver more frequent employee training.
7. Monitor regulatory changes as per Superintendent of Real Estate industry notices or guidance.
8. Include ML/TF obligations in job descriptions and performance reviews.
9. Set limits to cash transaction amounts in certain situations.
10. Request bank drafts instead of accepting large amounts of cash.
11. Conduct transactions only in person.
12. Obtain appropriate additional information to understand the customer's business or circumstances.

Appendix 4. Politically exposed persons (PEPs)

Individuals who have or have had a high political profile, or hold or have held public office, can pose a higher risk to REB as their position may be abused for money laundering and related predicate offences such as corruption and bribery, as well as for the financing of terrorism and proliferation. This risk also extends to members of their families and to close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, beneficial owner, or other person with an ownership or controlling interest into a higher-risk category.

Definitions of PEPs: including foreign, domestic and international organisation PEPs

A PEP is defined in Regulation 11 as an individual who is or has been entrusted with a prominent public function by a foreign country or territory outside Bermuda (Foreign PEP), by an international organisation (International Organisation PEP), or in Bermuda (Domestic PEP). The application of anti-money laundering and anti-terrorism financing regulations concerning PEPs also extends to members of their immediate families and to close associates.

The application of AML/AFT regulations concerning PEPs extends to the following persons:

- Foreign and domestic PEPs:
- Heads of state, heads of government, ministers and deputy or assistant ministers;
- Members of parliament and senior political party officials;
- Senior government officials including Permanent Secretaries;
- Members of supreme courts, constitutional courts, or 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 and chargés d'affaires;
- High-ranking officers in the armed forces; and
- Members of the administration, management or supervisory bodies of state-owned enterprises.

International organization[31] PEPs include:

- Senior management;
- Directors and deputy directors; and
- Members of the board.

The above categories are not exhaustive but do not include middle-ranking or more junior officials. Public functions exercised at levels lower than national should normally not be considered prominent.

[31] International organisation has its meaning found in Regulation 2 of the Proceeds of Crime Act (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008.

However, when their political exposure is comparable to that of similar positions at national level, REBs should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

Family members of PEPs:

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

Close associates of PEPs:

- Partners outside the family unit such as girlfriends and boyfriends.
- Prominent members of the same political party, civil organisation, labour or employee union;
- Individuals who have joint beneficial ownership of a legal entity or legal arrangement with a PEP;
- Individuals who have sole ownership of a legal entity or legal arrangement that have been set up for the benefit of a PEP; and
- Individuals with any other close business relations with a PEP, including through joint membership of a company board.

In deciding whether a person is a known close associate of a PEP, a real estate brokers and real estate agents need only have regard to information that they hold or is publically known[32].

When does a person stop being considered a PEP?

Although under the definition of a PEP an individual ceases to be so regarded after he has left office for one year, REBs 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.

[32] Regulation 11(7).

Appendix 5. Definitions

Beneficial owner	A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. In respect of customers who are private individuals, the customer himself is the beneficial owner, unless there are features of the transaction or surrounding circumstances that indicate otherwise[33].
Business relationship	A business relationship involves two or more sales or purchases. In other words, a business relationship starts as the third transaction starts, i.e. buying and selling.
Business risk assessment	The risk assessment which the business has undertaken to determine where it is vulnerable to the risk of money laundering or terrorist financing.
Consent	The MLRO has to have consent from the FIA to continue with a suspicious transaction where a disclosure has been made in relation to that transaction.
Customer due diligence	The term used to describe the identification and relationship information that we are required to collect as well as the verification documentation.
Financial Action Task Force (FATF)	The FATF is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. FATF is therefore a 'policymaking body' that works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. You can find more information about the FATF at its web address: www.fatf-gafi.org.
Money laundering	Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities.
Politically exposed person	PEPs are individuals who are or have, at any time in the preceding two years, been entrusted with a prominent public function by a foreign country or territory outside Bermuda (Foreign PEP), by an international organization (International Organization PEP), or in Bermuda (Domestic PEP).
Source of funds	Information about where the money has come from and who is paying it to us.
Source of wealth	Information about the wealth of the customer and how this has been generated.

[33] Regulation 3.

Terrorist financing	Providing or collecting funds which are known or suspected to be used to fund terrorist groups or acts of terrorism.
Tipping off	A tipping off offence is committed under POCA and ATFA if a person knows or suspects a disclosure to the FIA or other appropriate person, or knows and suspects the police are acting or proposing to act in connection with an investigation conducted into ML/TF and they disclose to any other person information which may prejudice any investigation.

Appendix 6. Sample form of the internal suspicious activity report

INTERNAL SUSPICIOUS ACTIVITY TRANSACTION REPORT		
Date of report:		
Name of person(s) making the report:		
Business area:		
Customer name:		
Customer identification information details:		
Customer risk rating:		
If customer is not an individual attach an ownership structure chart and information on registered office and registered number (i.e. a Trust or Corporation):		
Type of money laundering offence suspected:		
Date(s) of transactions:		
Currency and amount of transaction:		
Summarise the activity or transaction that gave rise to the suspicion (attach additional documents related to the suspicion)**:**		
Provide details (e.g. dates and amounts) of any known transactions that are pending or due to occur in the future:		
Person who submitted this report	Signature:	Date:
<u>Reporting Officer Confirmation</u>: **I confirm that I have received this form from the person named above**	Signature:	Date:

Appendix 7. Sample form of the Customer Due Diligence form

***** CUSTOMER IDENTIFICATION TO BE PERFORMED BEFORE A TRANSACTION OCCURS *****

Section 1: Identification information collection

1. **Describe the purpose and intended nature of the business relationship (like "purchase of a car"):**

2. **Fill in the following information based on the customer ID. Ensure that the customer provides you the valid ID.** You are required to make a photocopy of the ID documents provided.

Full name, any former names (e.g. maiden name) and other names used		
Principal residential address		
Date of birth		
Place of birth		
Nationality		
Gender	☐Male	☐Female
Photo ID type	☐Passport ☐National identity card ☐Driving licence ☐Other:_____	
ID number		
ID issuing authority		
ID issue date		
ID expiry date		

3. **Ask the customer whether he/she is a politically exposed person or a PEP related person?**	☐Not a PEP/PEP related. ☐Yes, a PEP/PEP related, then please provide additional information on the PEP and the information on the source of funds/wealth: _____
4. **Check whether the customer has a beneficial owner?**	☐The customer himself/herself is the beneficial owner ☐There are features of the transaction or surrounding circumstances that indicate that the other person ultimately owns or controls the customer /or on whose behalf a transaction or activity is being conducted. Please describe details: _____
5. **Perform sanctions check**[34]	☐Not in the sanction lists ☐Is on the sanction lists. Details: _____

[34] Links to the various consolidated lists for sanctions check to be performed are available on the International Sanctions page of the website of the National Anti-Money Laundering Committee. The web address is https://www.gov.bm/international-sanctions-measures

6. Perform the Internet search using the customer name	☐No negative information is found ☐There is some negative information. Provide details:_____

Section 2. Verification

Ensure you have made a photocopy of the customer's ID documents provided and put it into the appropriate document folder:
☐Yes
☐No

Section 3. Risk level assessment

7. Indicate the customer risk level:

The customer is a PEP/PEP related:	☐Yes	☐No	**<u>High</u> if there is at least one "Yes"**
The customer or transaction originates from a country <u>other than</u>: - Bermuda - The United Kingdom - Canada - The United States	☐Yes	☐No	
Suspicious activity report submitted with regards to the customer	☐Yes	☐No	
Other risk indicators: _____	☐Yes	☐No	
None of the above indicators can be applied:	☐Yes	☐No	**<u>Medium</u> if "Yes"**

8. *For high risk customers is required* Request additional information	Occupation and name of employer	
	Source of funds and wealth	

Section 4. Signoff

9. Person completing the form	Name	
	Date	
	Signature	
10. *For high risk customers is required* Request an approval of management	Name	
	Date	
	Signature	

Appendix 8. What is meant by “knowledge” and “suspicion”?

Knowledge

Having knowledge means knowing the existence of certain facts. In a criminal court, to have knowledge, it must be proved that the individual in fact knew that funds or assets were the proceeds of crime, or that a person was engaged in money laundering or terrorist financing.

However, knowledge can be inferred from the surrounding circumstances. A failure to ask the questions that an honest and reasonable person in similar circumstances would have asked may be relied upon by a jury to imply knowledge.

Section 46 of POCA 1997 and Schedule 1 of ATFA 2004 address knowledge that comes to a person in the course of their trade, profession, business or employment. Although information that comes to persons in other circumstances does not come within the scope of those Acts, persons may nonetheless choose to report such information.

Suspicion

Suspicion is subjective. Suspicion must be more than a vague feeling of unease; it may not be self-induced. At the same time, suspicion does not need to be clear or firmly grounded. Suspicion is sufficiently established when a relevant employee thinks “I have a suspicion but I cannot prove it by fact or hard evidence.”

Reasonable grounds for knowledge or suspicion of ML/TF are likely to be found where it is demonstrated that facts or circumstances were known to an employee, and that an honest and reasonable person in similar circumstances would have inferred knowledge or formed suspicion. This objective standard requires REBs and their employees to be able to demonstrate that they took reasonable steps in the particular circumstances to ensure an adequate and gap-free understanding of the business relationship, including the purpose and nature of the transaction or activity in question.

Appendix 9. Supplementary guidance for REB and customer high risk indicators[35]

Suspicious Activity Indicators for Real Estate Sector

Nature of Transaction

- Transactions involving payments in cash or in negotiable instruments which do not state the true payer (for example, bank drafts), where the accumulated amount is considered to be significant in relation to the total amount of the transaction
- Transactions in which the party asks for the payment to be divided in to smaller parts with a short interval between them
- Transactions in which payment is made in cash, bank notes, bearer cheques or other anonymous instruments
- Transactions which are not completed in seeming disregard of a contract clause penalizing the buyer with loss of the deposit if the sale does not go ahead
- Recording of the sale of a building plot followed by the recording of the declaration of a completely finished new building at the location at an interval less than the minimum time needed to complete the construction, bearing in mind its characteristics
- Transaction is completely anonymous–transaction conducted by lawyer–all deposit cheques drawn on lawyer's trust account
- Transactions carried out on behalf of minors, incapacitated persons or other persons who, although not included in these categories, appear to lack the economic capacity to make such purchases
- A transaction involving legal entities, when there does not seem to be any relationship between the transaction and the activity carried out by the buying company, or when the company has no business activity
- Transactions in which the parties show a strong interest in completing the transaction quickly, without there being good cause
- Transaction is complete through multiple deposits from different sources
- Frequent change of ownership of same property, particularly between related or acquainted parties
- If a property is re-sold shortly after purchase at a significantly different purchase price, without corresponding changes in market values in the same area

Customer Behaviour

- Customer cancels transaction for unexplained reason to obtain return of deposit

[35] Please note this additional guidance must be read in conjunction with the main guidance.

- Customer pays substantially more than asking price which cannot be explained by market conditions
- Customer purchases property without inspecting it
- Customer is known to have paid large remodelling or home improvement invoices with cash, on a property for which property management services are provided
- Customer buys back a property that he or she recently sold
- Customer negotiates a purchase for the market value or above the asked price, but requests that a lower value be recorded on documents, paying the difference “under the table”
- Customer pays initial deposit with a cheque from a third party, other than a spouse or a parent without adequate explanation
- Customer pays substantial down payment in cash and balance is financed by an unusual source (for example a third party or private lender) or offshore bank
- Customer purchases personal use property through his or her company when this type of transaction is inconsistent with the ordinary business practice of the customer
- Customer purchases multiple properties in a short time period, and seems to have few concerns about the location, condition, and anticipated repair costs, etc. of each property
- Customer insists on providing signature on documents by fax or email only
- Customer over-justifies or over-explains the purchase
- Customer's home or business telephone number has been disconnected or there is no such number
- Customer uses a post office box or General Delivery address where other options are available, without adequate explanation
- Customer exhibits unusual concerns regarding the firm's compliance with government reporting requirements and the firm's anti-money laundering policies
- Customer exhibits a lack of concern regarding risks, commissions, or other transaction costs
- Customer persists in representing his financial situation in a way that is unrealistic or that could not be supported by documents
- Customer arrives at a real estate closing with a significant amount of cash
- Customer purchases property in someone else's name such as an associate or a relative (other than a spouse) without adequate explanation
- Customer does not want to put his or her name on any document that would connect him or her with the property or uses different names on Offers to Purchase, closing documents and deposit receipts
- Customer inadequately explains the last minute substitution of the purchasing party's name