Anti-money laundering and combatting the financing of terrorism (AML/CFT)

Guidance Notes for Real Estate Agents and Letting Agents (REAs)

Contents

Issued: April 2018
Updated: January 2022
Version: 1.6

Office of Fair Trading • HM Government of Gibraltar • Suite 975, Europort • Gibraltar GX11 1AA
t (+350) 20071700 f (+350) 20071950 e oft@gibraltar.gov.gi w oft.gov.gi

Legal Notice

These guidance notes should be regarded as regulatory standards for the purposes of the Proceeds of Crime Act 2015 (**POCA**) and are issued pursuant to Section 11(3) of the Supervisory Bodies (Powers Etc.) Regulations 2017 (**SBPR**). Compliance with these guidance notes is enforceable pursuant to the provisions of POCA and of SBPR.

These guidance notes should not be construed as legal advice. If you are unsure about your obligations, you should take independent legal advice. The Office of Fair Trading (**OFT**) accepts no responsibility for reliance on any information contained within these guidance notes and excludes any liability for action taken based on this information.

1. Introduction/FAQ

1.1. What is AML/CFT?

AML/CFT stands for anti-money laundering (AML) and combatting the financing of terrorism (CFT).

1.2. What is AML/CFT all about?

Money laundering is the process of transforming and concealing the profits generated by criminal activity and corruption (such as drug trafficking, market manipulation, fraud, tax evasion) into a 'clean'/legitimate asset. Money laundering can be performed in many ways.

The manipulation of real estate transactions is an established method of money laundering and has been identified as a predominant and attractive business area for money laundering activities. Due to the high value of property transactions, it offers criminals seeking to launder monies the ability to integrate and conceal large sums of illicit funds into the legitimate economy.

Terrorist financing is defined in section 1ZA of the Proceeds of Crime Act 2015 (**POCA**). It involves:

1. the use of funds or assets;
2. the making available of funds or assets; or
3. the acquisition, possession, concealment, conversion or transfer of funds,

for the purposes of terrorism. For more information about terrorist financing, and for Counter Terrorist Financing Guidance visit: www.gfiu.gov.gi/what-is-terrorist-financing.

The vulnerabilities and risks of money laundering and terrorist financing (**ML/TF**) in Gibraltar are set out in the National Risk Assessment published by HM Government of Gibraltar (**NRA**). You can find a copy of the NRA in the 'AML/CFT' section of the OFT's website (www.oft.gov.gi).

1.3. Why is the OFT issuing these guidelines?

The OFT is required to regulate Real Estate Agents' and Letting Agents' (**REAs**) compliance with their AML/CFT obligations as set out in POCA (see Section 2 below). As a result, it is issuing these guidelines to assist REAs and their employees and to give an overview of their legal obligations. In addition, these guidance notes should not only help REAs comply with their legal obligations and requirements regarding

AML/CFT, but also help you identify high risk real estate transactions and indicators by providing useful information on money laundering schemes, methods and vulnerabilities.

1.4. Who do these guidelines apply to?

These guidelines apply to:

1. all REAs that conduct business in or from Gibraltar and/or in relation to Gibraltar real property; and
2. REAs' employees.

1.5. What is an REA?

The term 'REA' describes businesses that are Real Estate Agents and/or Letting Agents.

1.6. What businesses are Real Estate Agents?

Real Estate Agents are businesses that represents either the buyer or the seller during the selling or purchase of a property. The business's purpose within the transaction may extend to facilitating the sale and negotiating and arranging the purchase contract and any other documentation appertaining to the property transaction.

A Real Estate Agent representing a buyer will assist in the search of the property and may advise on the fairness of the price.

A Real Estate Agent representing the seller will advise the seller about property price, will market the property through advertising and will promote it to any interested buyers who contacts the business.

The above is a non-exclusive list of services and a business will be considered as a Real Estate Agent where they provide relevant services related to the sale of real property in Gibraltar.

1.7. What businesses are Letting Agents?

The definition of Lettings Agents is set out in section 7(1) 0f POCA. Lettings Agents are businesses that provide services relating to the letting, rental leasing other similar property transactions.

A Letting Agent may be instructed by either a prospective landlord or a prospective tenant for the letting of land for a term of more than a month.

A Letting Agent may publish advertisements or disseminate information about the property to try to secure a rental..

The above is a non-exclusive list of services and a business will be considered as a Letting Agent where they provide relevant services related to the rental of real property in Gibraltar.

1.8. Are property developers REAs?

If a developer is the owner of a property and is selling or renting that property directly then it is not considered to be an REA.

If the sales or rental of that property is being advertised and arranged through a third party which is not the owner of the property however then that third party may be considered aReal Estate Agent or Letting Agent respectively. This will be the case irrespective of whether the developer and the Real Estate Agent or Letting Agent are two companies ultimately owned by the same person(s).

Where an initial deposit payment towards an off-plan property is paid through an REA, that transaction will be covered by these guidance notes. Subsequent stage payments paid directly by the buyer to the developer shall not.

1.9. What are a REA's obligations?

REAs' responsibilities include, but are not limited to:

1. Carrying out a risk assessment of their business's attractiveness and vulnerability to money laundering and terrorist financing (see Section 3 below);
2. Establishing appropriate policies and procedures commensurate to the business's risks to prevent the business being used to launder money or finance terrorism (see Section 4 below);
3. Appointing a money laundering reporting officer (MLRO) who understands the business's risks and responsibilities under POCA and who shall be responsible for all AML/CFT matters (see Section 5 below);
4. Carrying out appropriate risk assessments of customers on a risk-based approach and keeping relevant documentation (see Section 6 below); and
5. Keeping appropriate AML/CFT records and submit annual returns to the OFT (see Section 8 below); and
6. Training staff to ensure they are aware of AML/CFT risks and of the business's AML/CFT polices (see Section 9 below).

1.10. What is the OFT's role?

As Supervisory Authority under POCA (see Section 2 below), the OFT must effectively monitor REAs and take necessary measures to:

1. secure compliance by REAs with the requirements of POCA;
2. prevent such REAs from engaging or otherwise being concerned in (directly or indirectly) with ML/TF, or otherwise knowingly or recklessly assisting or facilitating such conduct by any other person;
3. identify and assess the ML/TF risk for REAs as set out in the NRA, a copy of which can be found on the OFT's website: www.oft.gov.gi.

Furthermore, the OFT is required to report evidence of money laundering to the Gibraltar Financial Intelligence Unit (**GFIU**).

1.11. How does the OFT monitor compliance by REAs?

The OFT risk assesses all REAs compliance with their AML./CFT obligations based on:

1. documents submitted annually to the OFT, including:
   a. risk assessments (see section 3);
   b. policies controls & procedures (section 4); and
   c. annual returns submitted (see section 8); and
2. regular onsite visits carried out by the OFT on all REAs in order to ensure that they are meeting their AML/CFT obligations in practise. The OFT works closely with the Gibraltar Financial Intelligence Unit, law enforcement bodies and other AML/CFT supervisory authorities to monitor the market and uses various sources to acquire information and determine whether the business is complying with their AML/CFT obligations or is being used for ML/TF.

1.12. Do these guidance notes contain all I need to know?

No. These guidelines are for information purposes only so that REAs and their employees are given an overview of their legal obligations. For the definitive authority on your legal obligations regarding AML/CFT please refer to the Proceeds of Crime Act 2015 (see Section 2 below).

2. Proceeds of Crime Act 2015 (POCA)

2.1 What is POCA?

POCA is a Gibraltar law aimed at preventing the abuse of the financial system for money laundering and terrorist financing. It also sets out processes relating to the confiscation, investigation and recovery of the proceeds of unlawful conduct.

2.2 Where can I find POCA?

The full body of the Act may be found by in the 'Documents' section of the 'AML/CFT' page of the OFT's Website (www.oft.gov.gi) along with a pdf copy of these guidance notes.

It can also be found on the HM Government of Gibraltar's Gibraltar laws website (www.gibraltarlaws.gov.gi) by searching for "Proceeds of Crime".

2.3 Is all of POCA applicable to REAs?

All of POCA is applicable, however the most relevant part for REAs is Part III: 'Measures to prevent the use of the financial system for purposes of money laundering, terrorist financing and proliferation financing'. For ease of reference, REAs are defined as "relevant financial business" in section 9(1)(h) of POCA.

2.4 If I read these guidance notes, do I need read the Act?

Yes! These guidance notes only set out some of the most relevant provisions of POCA to the REA sector. These focus on ML/TF only as these are the criminal activities which REAs are most at risk of being exposed to and where the OFT has therefore focussed its guidance efforts. There are however other obligations in POCA that may not be referred to in this document, most notably in relation to proliferation financing.

You should not therefore regard this document as an exhaustive authority and should instead read it in conjunction with your legal AML/CFT obligations as set out in POCA.

2.5 What is proliferation financing (PF)?

PF refers to the act of providing funds or financial services which are used for the manufacture, acquisition, possession, development, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery. This is not an exhaustive definition and is indicative only.

REAs should understand PF and their obligations in relation to PF as set out in local and international legislation. For more information and guidance regarding PF please refer to the Counter-Proliferation Financing Guidance Notes on the GFIU's website: http://gfiu.gov.gi/uploads/docs/X86Ru_CPF_Guidance_Notes_v1.1.pdf .

3. REA risk assessments

3.1 What is a risk assessment?

Section 25A POCA sets out the requirement to risk assess their business. A risk assessment is the process of assessing the money laundering and terrorist financing risk that your business could be exposed to. Once the risks are understood appropriate systems and policies can be put

in place to mitigate these risks see section 4).

3.2 What do I need to consider when carrying out the risk assessment?

REAs must subjectively assess the relevant money laundering and/or terrorist financing risks to their business. When undertaking their risk assessment the following questions should be considered:

1. Is the business well informed and familiar with the methods and systems used by criminals wishing to launder illicit funds via REAs and is this information kept up to date? (for examples of how REAs may be used to launder money please see Schedule 2.)
2. Does the business have systems in place to regularly monitor and detect any behavioural patterns or activities which could possibly be money laundering schemes? (see Section 4 below)
3. Have the employees of the business received any training which might mitigate the risk of the business being used to launder illicit funds? (see 10.1 and 10.2)
4. Are the business's customer due diligence methods appropriate and sufficient to minimise the risk (see Section 6)?
5. How does the business's:
   i. customer base;
   ii. methods of financial transactions;
   iii. methods of communication with customers;
   iv. nature or services provided; and
   v. geographical area,
   impact its level of risk?
6. Are the business's customers companies which have complex legal structures making it hard to determine their beneficial owners?
7. Does the business deal with any overseas sellers or buyers who are not local to the business?
8. Does the business accept large sums of cash? If so, are proof of funds requested?
9. Does the business take payments from third parties?

This list is not exhaustive and a risk based approach will require analysing the business's individual characteristics carefully.

For example, a locally based international REA with high net-worth overseas customers presents a very different risk profile to a small REA who mainly deals with the sale of affordable housing scheme properties. However, both may be targeted by criminals if they have little or no AML/CFT controls in place. The environment in which a business is carried out affects the individual business's risk assessment. If a business has many high net-worth customers or deals with people from a particular country or region, this will influence the business wide assessment.

3.3 Is there more guidance to help my business carry out its risk assessment?

For detailed and specific guidance about carrying our risk assessments refer to the OFT's Risk Assessment Guidance Notes which can be found in the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

For in depth guidance of high level principles and procedures for REAs on the risk-based approach to combatting Money Laundering and Terrorist Financing please refer to the guidance from the Financial Action Task Force (**FATF**) which can be

found in the 'AML/CFT' section of the OFT's website (www.oft.gov.gi).

3.4 Ongoing obligations

Each REA has the responsibility of regularly conducting an effective risk assessment as a means of focusing on risks specific to the business at that time and ensuring that AML/CFT policies, controls and procedures that are in place continue to be effective.

4. AML/CFT policies, controls and procedures

4.1 Risk based policies and procedures.

Pursuant to section 26 POCA, REA's must establish and maintain appropriate and risk-sensitive AML/CFT policies, controls and procedures. These policies and procedures should protect the business and prevent it from being used as a tool for ML/TF.

All REAs must have a clear written AML/CFT policy based on the ML/TF risks associated to the specific business. These can be determined after carrying out a risk assessment of the business (see Section 3 above). The policy shall be proportionate to the nature and size of the REA.

The policy should contain well-defined controls and procedures to identify and manage the business's and its customers' ML/TF risks.

It must be made available to all employees of the business and to the OFT.

4.2 Who approves the policy?

Pursuant to section 26A POCA the AML/CFT policy must be approved and adopted by the business's senior management who will include the board of director, executives and/or other senior managers..

4.3 What controls and procedures must REAs have in place?

REAs must develop internal policies and procedures that allows it to:

1. assess the risk of their business being used by criminals for ML/TF (in accordance with section 3 above);
2. carry out customer due diligence measures (see section 6) and monitor customers' business activities;
3. carry out ongoing CDD measures (see section 7 below);
4. carry out targeted financial sanctions screening (see section 8 below);
5. submit annual returns to the OFT (see section 9 below);
6. report suspicious clients or transactions to the GFIU where it suspects, or has reasonable grounds to suspect, that a transaction is related to ML/TF (see section 5.8);
7. keep customer, transactional and staff training records (see section 9);
8. ensure employees:
    i. are aware of POCA and these guidance notes;
    ii. are aware of the business's AML/CFT policy;
    iii. have the necessary training; and
    iv. report suspicious activity to the MLRO (see section 10.4);

A complete list of the legal requirements are set out in section 26 POCA.

REAs must also ensure they have the necessary management control systems in place and the required resources to implement the policy.

4.4 What if the REA is part of a group?

Pursuant to section 26(1B) POCA, AML/CFT policies and procedures should be applicable to all branches and majority-owned subsidiaries of the group and should be appropriate to each of the REAs in the group.

Such AML/CFT policies and procedures should be implemented effectively at the level of branches and majority-owned subsidiaries. Group AML/CFT policies and procedures should allow for sharing information required for the purposes of CDD and the assessment and management of ML/TF risk by all the group's businesses. The MLRO of each business in the group should be provided with customer, and transaction information from the other businesses when necessary for AML/CFT purposes. Adequate safeguards on the confidentiality and use of information exchanged should be in place. Refer to the full set of requirements in Section 26(1B) POCA.

If you have branches and subsidiaries outside of Gibraltar you should note the requiems of Section 21 POCA.

4.5 Do I comply fully once I have a policy?

It is important that the policy is put into operation. If a REA has the best policy in the world, but it is not used or it is not appropriate to their business, then it is of no use and the REA will not be meeting its AML/CFT obligations.

It must therefore be based on the findings of the business's risk assessment (see section 3) and be made readily available to all employees who should be trained about how to implement it (see section 9 below).

A copy of the policy must also be provided to the OFT.

Pursuant to section 26(1A) POCA REA's must also undertake an independent audit function for the purposes of testing their AML/CFT policies, controls and procedures and ensure they are appropriate.

4.6 Undertaking an audit

Audits must have regard to the nature and size of the REA (section 26(1A) POCA) and should happen at regular intervals or where a deficiency with the business's AML/CFT policy, controls or procedures is identified. The frequency and scale of the audit shall be proportionate to the size and nature of the business as well as findings and recommendations from previous audits and any other relevant AML/CFT considerations.

Audits must be independent but there is no requirement to engage the services of a third party in order to carry out this function. It can also be performed by a person from within the business. Whoever carries out the audit the REA must ensure their independence. The auditor must not:

1. have been involved in carrying out the REA's risk assessment;

2. have been involved in the development of the REA's AML/CFT policies, controls and procedures; and/or

3. be involved in applying the REA's AML/CFT policies, controls and procedures.

The person must provide an independent, objective and impartial view on the efficacy of the policies, controls and procedures. It is

the responsibility of the business to determine the independence of the individuals and this should to be evaluated at least annually.

The REA must also ensure that the person conducting the audit has sufficient knowledge of the REA's AML/CFT obligations to assess the efficacy of the business's policies, controls and procedures.

4.7 Do I need a policy if I work alone?

Yes. You must implement a policy, however this need not be in writing until you are working with someone else. The OFT nevertheless recommends that written policies are created if you work alone as this will help you carry out your AML/CFT and targeted financial sanctions obligations (see section 8). If a policy is not in writing you must be able to explain to the OFT upon request:

1. your business's ML/TF risks and vulnerabilities;
2. your business's AML/CFT policies, controls & procedures to mitigate those risks; and
3. your business's procedures to carryout sanctions screening.

5. MLROs & their responsibilities

5.1 What is an MLRO?

All REAs must nominate a money laundering reporting officer (**MLRO**).

REAs must register their MLRO with the OFT. They must do so by completing and submitting an MLRO nomination form. The form is available to download in the 'AML/CFT' section of the OFT'S website: http://www.oft.gov.gi/index.php/aml-cft

5.2 Who must be appointed MLRO?

A MLRO must be a director, senior manager or partner of the business. They play an important role, so they must be someone who:

1. can be trusted with the responsibility;
2. has access to all customer files and records;
3. can give necessary instructions to other employees; and
4. is autonomous enough to decide whether they need to report suspicious activities or transactions.

If you work alone, you are the MLRO.

5.3 What is the MLRO's role?

The MLRO is generally responsible for dealing with any AML/CFT matters and is the OFT's liaison for the business.

They must carry out appropriate risk assessments of the business and its customers (in accordance with sections 3 and 6 respectively) and ensure all AML/CFT policies and procedures are adhered to and understood by all employees (see sections 4 and 9).

The MLRO must also be aware of daily transactions and monitor any suspicious activities involving the business that might be linked to money laundering or terrorist financing. Where necessary the MLRO must report such activities or risks to the GFIU by submitting a Suspicious Activity Report (**SAR**) (see 5.8 below).

Where a REA suspects, or has reasonable grounds to suspect, that a transaction is related to ML/TF it is required to report it

promptly to the GFIU. This includes attempted transactions.

5.4 What are the MLRO's responsibilities?

MLROs must receive reports of suspicious activity from any employee in the business. They must then evaluate the reports for any evidence of money laundering or terrorist financing and carry out an appropriate risk assessment based on the report and the customer's due diligence records.

The MLRO may also be responsible for other tasks to ensure the business complies with POCA, e.g.:

1. putting in place and operating AML/CFT controls and procedures (Section 4above);
2. training staff in preventing money laundering and terrorist financing within the business;
3. keeping records of customer due diligence and risk assessments (see 7.1 below); and
4. ensuring the REA's workers are not part of a ML/TF scheme.

The MLRO must also carry out targeted financial sanctions screening (see section 8).

5.5 How does a MLRO identify a money laundering or terrorist financing risk?

The MLRO must consider all of the information about the customer, business relationship and the transaction which is intended to be carried out. If the MLRO has knowledge, suspects or has reasonable grounds to suspect that a person is engaged in, or is attempting to, launder money or finance terrorism they must report this to the GFIU at the earliest possible opportunity using a SAR (See 5.8 below).

5.6 What is meant by 'knowledge'?

A MLRO has 'knowledge' if they actually know something to be true. The MLRO may however infer this from surrounding circumstances, including the due diligence process and by asking questions.

If in doubt, the MLRO should seek clarification or ask for evidence from the person to support their evaluation.

5.7 What constitutes suspicion?

Suspicion must be assessed both subjectively and objectively. It must extend beyond mere speculation and must be based on some foundation. To be suspicious MLROs must have a degree of satisfaction that money laundering may be taking place which, does not necessarily amount to knowledge (see 5.6 above), but at least extends beyond speculation.

If in doubt, the MLRO should seek clarification or ask for evidence from the suspected person to support their evaluation.

5.8 How does the MLRO report to the GFIU?

For more information about how to do this visit https://www.gfiu.gov.gi/reporting. This will allow the MLRO to sign up to the GFIU's Themis online system. This will allow the MLRO to submit SARs and to report positive sanctions matches (see section 8).

Alternatively, SARs may be made to the GFIU by completing a downloaded Suspicious Activity Report form and submitting it to the GFIU by e-mail (gfiu@gcid.gov.gi) or delivered by hand to their offices at Suite 832, Europort. The form can downloaded from the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

5.9 What happens once a SAR has been submitted?

Once a SAR is submitted the MLRO must ensure the transaction does not take place. The GFIU has fourteen days to assess the information submitted in the SAR and reach a decision about how to proceed. They may seek further information from you.

At the end of the fourteen days if you have not received any further notice from the GFIU then nothing further is required and the transaction may take place.

5.10 Should the suspicious transaction be allowed to go ahead?

No. The MLRO must seek consent from the GFIU before proceeding with a transaction it suspects is being carried out to launder money or finance terrorism.

5.11 Should the person being reported be made aware of their report?

No! It is a criminal offence for anyone to say or do anything that may prejudice an investigation or 'tip off' another person that a suspicion has been raised, a SAR has been submitted or that a money laundering or terrorist financing investigation may be carried out. It is also an offence to falsify, conceal or destroy documents relevant to investigations.

Nobody should tell or inform the person involved in the transaction or anyone else that:

1. the transaction is being or was delayed because a suspicion has been raised;
2. details of a transaction have or will be reported to the GFIU; or
3. law enforcement agencies are investigating the customer.

Where a MLRO forms a suspicion of money laundering or terrorist financing, and they reasonably believe that applying CDD measures (see section 6 below) will 'tip-off' the customer, then the MLRO should not apply such measures and instead submit a SAR to the GFIU.

5.12 Tipping off through CDD measures

Pursuant to section 11(5A) POCA, where, during the course of applying customer due diligence measures (see section 6 below), a REA knows, suspects or has reasonable grounds to suspect that the person subject to such measures or another person is engaged in ML/TF or proliferation financing, or is attempting any one or more of those acts, the REA must, where it is of the opinion that to continue would result in the tipping-off of the person, cease applying customer due diligence measures, and shall make a relevant disclosure to the GFIU without delay.

5.13 Targeted financial sanctions

It is an offence under section 9 of the Sanctions Act 2019 to breach, or to assist a breach, of an international sanction. You are not therefore allowed to deal with persons or entities subject to a sanction unless you have a licence, permit or other authorisation to do so issued in accordance with Section 10 of the Act.

An MLRO is responsible for ensuring that REAs screen their customers against sanction lists and MLROs are required to report positive sanction matches to the GFIU.

For more information about targeted financial sanctions refer to section 8.

5.14 What happens in the MLRO's absence?

A MLRO's duties can be temporarily delegated to someone else. This does not however relieve the MLRO of their responsibility. A deputy or alternate may only be appointed during periods of absence.

A MLRO's absence should not restrict the REA's ability to monitor risk and submit SARs to the GFIU.

5.15 Is there more guidance for MLROs?

The GFIU has produced AML/CFT guidance notes on SARs for MLROs & Reporters and guidance notes on Financial Sanctions. For access to this document please contact the GFIU or request a copy via email: admin@gfiu.gov.gi.

For more information visit the GFIU's website: https://www.gfiu.gov.gi/reporting.

6. Customer due diligence & assessing risk

6.1 What are customer due diligence measures?

Customer due diligence (**CDD)** measures (also known as 'know your customer' or KYC) refer to processes whereby a business carries out checks on its customers to establish who they are and to understand the purpose of the transactions they want to carry out. This allows the business to determine whether there is a risk that they are linked to ML/TF. A full definition of CDD measures is set out in Section 10 of POCA.

CDD measures involves:

1. identifying the customer and establishing who they are;
2. understanding the ownership and control structure of the customer;
3. understanding and obtaining information on the purpose and intended nature of the business relationship or occasional transaction;
4. taking a risk-based approach to the verification of the identity of the customer and all beneficial owners (see 6.3 below)
5. determining whether the customer, or its beneficial owner, is a politically exposed person (see 6.13 below);
6. taking a risk-based approach to the verification of the source of funds and source of wealth of the customer and beneficial owners; and
7. understanding the ownership and control structures of customers that are corporate or legal entities, trusts, foundations and other legal arrangements.

CDD therefore involves collecting documentation and information to allow the business to understand who it is dealing with, what the transaction is about and who is benefiting from the transaction. This in turn allows the business to carry out a ML/TF risk assessment of the customer before providing their service to them.

6.2 When are CDD measures carried out?

CDD must be performed before any financial transactions take place.

Pursuant to section 11(1) and 13(2) POCA REAs must apply CDD measures and verify

the identity of the customer (and any beneficial owner) before:

1. it establishes a business, professional or commercial relationship with a customer which is expected, at the time when contact is established, to have an element of duration. A business relationship is formed when an offer for the purchase or rental of a property is accepted.; and/or
2. it carries out occasional transactions above £12,000, whether the transaction is carried out in a single operation or in several operations which appear to be linked.

REAs must also apply CDD measures where it suspects ML/TF or proliferation financing in any circumstances.

REAs are also required to carry out ongoing monitoring and due diligence of existing business relationships (see section 7).

6.3 What are my CDD obligations?

REAs must undertake sufficient monitoring of the transactions and business relationships they enter into to enable the detection of unusual or suspicious transactions.

Pursuant to section 11 (3) POCA a REA must determine the extent of CDD measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. In doing so the REA must at least, take into account the following list of risk variables:

1. the purpose of an account or relationship;
2. the level of assets to be deposited by a customer or the size of transactions undertaken; and
3. the regularity or duration of the business relationship.

The REA must also be able to demonstrate to the OFT that the extent of the measures is appropriate in view of the risks of ML/TF that have been identified.

6.4 Who needs to be checked?

Appropriate CDD must always be completed on your customer.

Section 8(3) POCA specified that an REA is to be treated as entering into a business relationship:

1. with a purchaser (as well as with a seller), at the point when the purchaser's offer is accepted by the seller; and
2. with a tenant (as well as with a landlord), at the point when the tenant's offer is accepted by the landlord.

Where a REA represents the landowner (the seller or landlord) it will also therefore have to apply CDD measures to both parties in the property transaction.

Where an REA is the sole agent involved in a transaction it will have to do CDD on both parties. This is because contractually the landowner is usually the REAs' customer and the other party is the applicant.

In transactions with more than one REA (e.g. where commissions are split), the REA representing an applicant will only have to carry out CDD on their customer (the purchaser or tenant). An REA representing the landowner will have to carry out CDD on both.

REAs must also apply ongoing CDD measures to existing business relationships (see section 7).

6.5 Identifying the customer.

REAs are required to understand the nature of their customer's business and its ownership and control structure.

Where your customer represents a company, then not only must you know the person you are dealing with, but also who the ultimate beneficial owner, or BO, of the company is (see section 6.6).

Where your customer is the trustee of a trust (or other similar legal arrangement) you must not only verify the identity of the beneficiaries (the BOs), but also that of the settlor, the trustee(s) and the protector (if any).

The identity of the Customer must be known and their identity must be verified through appropriate original documentation.

Similarly, the identity of any ultimate beneficial owner must be known and verified (see section 6.6).Due diligence is not required for banks, EU listed companies or Governmental entities.

6.6 What is a beneficial owner (BO)?

The definition of 'beneficial owner' is set out in section 7(1A) POCA.

A BO is an individual (or 'natural person') who will ultimately benefit from a transaction or business relationship.

Where an individual is conducting a transaction or activity for their own benefit then they are the beneficial owner (POCA section 7.(1A)(a)(i)).

If, however, a transaction is being carried out by a customer on behalf of another person then the BO is the individual

1. on whose behalf a transaction or activity is being conducted (POCA section 7.(1A)(a)(ii)); and/or
2. who ultimately owns or controls the customer entering into the transaction.

Where a REA's customer is entering into a transaction on behalf of another person the REA must identify and verify who that other person is. That person is the BO.

Broadly speaking where an individual either owns or has control over 25% of a company or is a settlor, trustee, protector or beneficiary of a trust (or similar) that is the REA's customer, that individual will be a BO.

For detailed and specific guidance about BOs and how to identify them refer to the OFT's Beneficial Ownership Guidance Notes which can be found in the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

Pursuant to section 11(4A) POCA, where a REA is required to apply CDD measures to a trust, corporate or legal entity it shall collect proof of registration (or an excerpt) of the BO's registration on the Gibraltar Register of Ultimate Beneficial Owners (https://uboregister.egov.gi).

6.7 What happens if I have difficulties or am unable to collect due diligence?

In relation to companies, you must exhaust all possible means to determine who its BO is. This will involve making appropriate and proactive enquiries. You must be able to demonstrate the efforts made to do so to the OFT.

However, if after having exhausting all possible means:

1. there is doubt as to who the BO is; or
2. no person is identified as the BO,

then the BO shall be the individual exercising control over the company via other means (POCA s7(c)(ii)).

If, after having exhausted all possible means, there is still doubt about who the individual exercising control is, then the BO shall be the individual who holds the senior

management position in the customer (POCA s7(c)(ii) & (iv)).

More generally, pursuant to section 15(1) POCA, Pursuant to section 15(1) POCA, if any person or entity is unable or unwilling to submit the relevant CDD documents requested and the REA is unable to carry out appropriate CDD measures it should not proceed with the transaction and, where applicable, terminate the business relationship. If the relationship is not terminated this should be recorded.

Furthermore, the REA must submit a SAR to the GFIU in relation to the customer (see sections 5.8 to 5.10).

REAs should also keep a record of any difficulties encountered during the CDD process (POCA section 10(l)).

REAs are prohibited from carrying out transactions for anonymous customers or customers which have provided aliases or fictitious names.

6.8 Applying CDD measures.

CDD measures allow a REA to assess a customer's AML/CFT risk and whether a transaction may proceed without a real risk of the REA being involved in a transaction which is intended to launder money or finance terrorism. The identity of Customers should be verified on the basis of original documents, data or information obtained from reliable and independent sources.

The level of CDD the REA must apply in each business relationship will depend on the level of AML/CFT risk. The risk must be assessed by considering each party to the transaction, the type of transaction and the nature of the business relationship.

REAs must determine the extent of CDD measures on a risk-sensitive basis depending on the type of customer, business relationship and transaction. Therefore, the approach a REA takes to the level of CDD must reflect the AML/CFT risk faced by the business during that business relationship.

A low AML/CFT assessment will require a simplified due diligence process and a high risk transaction or customer will require an enhanced due diligence process with medium risks requiring elements of both depending on the risk. For guidance on how to identify money laundering and terrorist financing risks please see Schedule 1.

6.9 Low risk customers: Simplified customer due diligence.

Pursuant to section 16 POCA, where a REA, having applied CDD measures:

1. identifies areas of lower risk;
2. has ascertained that the business relationship or the transaction presents a lower degree of risk; and
3. has not identified a suspicion or knowledge of ML/TF, or proliferation financing,

it may record the reasons why it perceives a reduced risk and apply simplified customer due diligence measures. For guidance on how to identify low risk customers see Schedule 1.

Simplified CDD can include, but may not be limited to, collecting the following basic information:

1. Full Name;
2. date of birth;
3. residential address;
4. a copy of the customer's original Passport/ID (or any other Government-issued photographic document); and

5. the customer's source of income or wealth (e.g. employment) and a supporting document.

For companies you must collect:

1. an up to date company profile issued by Companies House or the following corporate documents:
   i. Certificate of incorporation;
   ii. Register of Members; and
   iii. Register of Directors; and
2. the address of the registered office and, if different, a principal place of business.

Where a transaction involves a trust (or other similar legal arrangement) you must collect a copy of the trust deed (or other similar legal document) establishing and setting out the nature of that arrangement.

REAs must keep copies of due diligence documents (see Section 7 below).

6.10 High risk customers: Enhanced CDD measures.

REAs must apply enhanced CDD measures to appropriately manage and mitigate risks when dealing with -

1. customers identified as being high risk (see Schedule 1, paragraph 3);
2. natural persons or legal entities established in third countries identified by the European Commission as high risk third countries; and
3. politically exposed person, or their family members and close associates (see 6.10 below); and
4. in other circumstances as set out in Section 17(1) POCA.

For guidance on how to identify high risk customers see Schedule 1.

When dealing with high risk customers it is important to perform enhanced due diligence as a result of the increased risk of money laundering. MLROs must keep records as to why, in their view, the need for enhanced CDD is appropriate to the risk posed by the business relationship.

Example of enhanced due diligence:

1. A copy of the customer's Passport/ID which is certified as true copy of the original by a third party professional;
2. Proof of the customer's address provided in a document such as a utility bill or bank statement;
3. Proof of the customer's and the BO's source of funds commensurate to the transaction (see section 6.13); and
4. Additional information on:
   i. the customer and on the beneficial owners, including their source of wealth and source of funds where appropriate;
   ii. the intended nature of the business relationship; and
   iii. the reasons for the transactions.

REAs must also apply specific enhanced CDD measures in relation to:

1. business relationships or transactions involving high-risk third countries as set out in section 17(6) POCA; and
2. politically exposed persons as set out in section 20 and 20B POCA (see section 6.13).

REAs must obtain the approval of senior management for establishing or continuing a business relationship with a customer requiring enhanced CDD.

REAs must keep copies of due diligence documents (see Section 7 below).

6.11 What am I looking for?

CDD documentation, along with all other surrounding factors and information about the customer and the type of transaction. REAs are also required to understand the nature of their customer's business and its ownership and control structure.

This information will permit the REA's MLRO to assess the AML/CFT risk posed by a customer or a transaction and whether to report suspicious activity to the GFIU.

Some examples of suspicious activity specific to the REA include occasions where a customer:

1. appears unwilling to submit any identification documents or having his details in any document related to the property;
2. seems uninterested in the property value or viewing and inspecting the property;
3. acquires several properties within a short period of time;
4. wishes to proceed with a transaction without the assistance of a lawyer or legal representative;
5. requests information from the business reference AML/CFT requirements;
6. intends to pay the full property price without requiring financing (mortgage/loan);
7. wishes to make the property payment through various transactions involving complex legal structures which do not make any commercial sense; and
8. asks whether rental payments can be made or received in cash only.

For guidance on how to identify ML/TF risks please see Schedule 1.

6.12 Non face-to-face transactions

Pursuant to Section 18 POCA, Where the customer has not been physically present for identification purposes, REAs must take specific and adequate measures to compensate for the higher risk this presents. This may for instance include:

1. ensuring that the customer's identity is established by additional documents, data or information;
2. applying measures to verify or certify the documents provided, e.g. requiring a third party professional with AML/CFT expertise to certify them e.g. a lawyer; and
3. ensuring that any payments are carried out through an account opened in the customer's name with a bank.

6.13 Politically exposed persons.

A politically exposed person (**PEP**) is a person who is or has been entrusted with a prominent public function locally or internationally (see definition is paragraph 4 of Schedule 1). These individuals are at a higher risk of being connected to money laundering and terrorist financing due to the position and influence they hold and because they can be susceptible to corruption.

Pursuant to section 26(2)(c) POCA a REA must have policies, controls and procedures in place determine whether a customer or the BO of a customer is a PEP, a PEP's 'family member' or 'a person known to be their close associate' (as defined in Section 20A POCA). Given Gibraltar's small size and the closeness of its community, this is potentially a large group of persons and this may therefore make it easier for these persons to be identified.

Pursuant to section 20 POCA, before entering into a transaction with a PEP, a

PEP's family member, a PEP's close associate or a customer whose BO is a PEP, the REA must:

1. carry out enhance due diligence (see section 6.10);
2. have approval from senior management;
3. take adequate measures to establish the source of wealth and funds which are involved in the existing or proposed transaction.

Section 20B POCA also sets out the additional continuing obligations with regard to PEPs.

For in depth guidance on PEPs please refer to the FATF's guidance which can be found in the 'AML/CFT' section of the OFT's website (www.oft.gov.gi)

6.14 What is meant by source of funds and source of wealth?

A customer's source of funds and source of wealth can be good indicators that they are involved in criminal activity.

Source of wealth describes how the customer, or their family, has acquired their total wealth. Examples include investments, business interests, employment income and inheritances.

Source of funds refers to the origin of money that is used for a specific transaction. Examples include personal savings, pension releases, dividends, property sales, gambling winnings, inheritances and gifts. In establishing source of funds REAs must seek to understand not only where funds come from (i.e. the account from which they were transferred) but also the activity from which the funds were generated, e.g. employment, the sale of property or an inheritance.

Where a customer's source of funds and source of wealth do not match a customer's other CDD information, their background, risk profile or other pertinent characteristics e.g. their transaction history, REAs should use that information to inform their AML/CFT response, including collecting further appropriate CDD e.g. scrutinising customer bank statements to support the information provided.

6.15 Risk assessments

REAs are required to keep a written risk assessment in respect of all its customers and the action taken in respect of any suspicious activity detected.

The OFT encourages all REAs to keep a risk assessment file as they must demonstrate to the OFT that the CDD measures it has applied are appropriate to the client and the transaction in view of the risks of money laundering and terrorist financing identified. Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution or criminal activity.

6.16 Can I rely on someone else's due diligence?

If a REA is satisfied that a third party has already carried out appropriate CDD measures on its customers, they may rely on that CDD as long as they are satisfied that:

1. the CDD measures are appropriate to the customer's level of risk as assessed by the REA; and
2. the CDD measures are current and up to date.

Copies of the CDD documentation must be provided by the third party to the REA. The REA is required to carry out its own risk assessment on the customer based on the CDD documentation received prior to the REA entering into a transaction or business

relationship with the customer. It is not possible for the REA to rely on the third parties' risk assessments!

The responsibility to carry out CDD measures, to risk assess and to keep records on its customers shall always ultimately remain with the REA.

6.17 When do I report suspicious activity?

This will depend on the risk assessment carried out and is ultimately a question for the MLRO, having considered all information it has about the customer and the transaction through the CDD measures. It should be made where the MLRO has either knowledge (see section 5.6) or is suspicious (see section 5.7) that ML/TF is or may be taking place.

If in doubt, submit a SAR! (see sections 5.8 to 5.10).

6.18 Tipping off

Pursuant to Section 11 (5A) POCA where, during the course of applying CDD measures, the REA knows, suspects or has reasonable grounds to suspect that the person subject to such measures or another person is engaged in ML/TF or proliferation financing, or is attempting any one or more of those acts, the REA must, where it is of the opinion that to continue would result in the tipping-off of the person, cease applying CDD measures, and shall make a relevant disclosure to the GFIU without delay.

6.19 Ongoing monitoring

Where REAs have ongoing business relationship with its customers they are required to carry out ongoing monitoring and CDD of that business relationships. (see section 7 below).

6.20 Records.

REAs must keep copies of the documents requested while conducting CDD procedures along with all relevant documents appertaining to the business relationship (see Section 9 below).

7. Ongoing monitoring

7.1 Ongoing monitoring

REAs are required to carry out ongoing monitoring and due diligence of existing business relationships. This requirement is set out in section 12 POCA.

Ongoing monitoring does not apply to occasional, one-off transactions in relation to which REAs provided services to a customer in respect of a single sale or initial rental of a property. It may however apply to customers who have been provided such services more than once or on an ongoing basis (e.g. ongoing services in relation to the rental or a property).

7.2 What are business relationships?

It means a business, professional or commercial relationship which is connected with the REA's activities and which is expected, at the time when contact is established, to have an element of duration.

As set out in section 8 (3) POCA:

1. a REA is to be treated as entering into a business relationship with a purchaser (as well as with a seller), at the point when the purchaser's offer is accepted by the seller; and
2. a Letting Agent is to be treated as entering into a business relationship with a tenant (as well as with a landlord), at

the point when the tenant's offer is accepted by the landlord.

7.3 What does ongoing monitoring involve?

Ongoing monitoring means:

1. scrutinising transactions undertaken throughout the course of the business relationship to ensure that they are consistent with the REA's knowledge of the customer, their business, their risk profile and their source of funds; and
2. undertaking reviews of existing records (and updating these where necessary) to ensure that the documents, data or information obtained for the purpose of applying CDD measures is kept up-to-date and relevant.

REAs must determine the extent of ongoing monitoring on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. You must be able to demonstrate to the OFT that the extent of the measures is appropriate in view of the risks of ML/TF that have been identified.

7.4 When do I need to do this?

Ongoing monitoring must be carried out at regular intervals. As an indicator the OFT would expect that:

1. high risk business relationships are reviewed at least every year;
2. medium risk business relationships are reviewed every two year; and
3. low risk business relationships are reviewed every three years.

These time frames are indicative only and you must adapt your ongoing monitoring to your business's and the customer's risk as determined and recorded by your business.

When dealing with high risk transactions or customers requiring enhanced CDD, REAs must conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

REAs must also carry out targeted financial sanction screening on existing customers as and when the sanctions lists are updated. REAs must therefore have systems to be notified when this happens. Refer to section 8.5 for more information.

Further monitoring and CDD measures must also be carried out when the relevant circumstances of a customer change. When this occurs the REA must apply CDD measures to the existing customer on the basis of materiality and on a risk sensitive basis (POCA section 11(2)(a))

7.5 When do the relevant circumstances of a customer change?

Any material change to a customer will trigger the need for a REA to reapply CDD measures. A material change is one which would require a reasonable REA to reassess the ML/TF risk of the business relationship in light of those changes. There is no exhaustive list for what a material change is, however material changes can include:

1. a change in the nature or regularity of the transactions carried out by the business (See Schedule 1, paragraph 5, patterns of business); or
2. a change to the ownership or management of the customer.

REAs should not just take into consideration the risk profile of the existing customer but also the impact that that customer's business may have on the REA as a whole. For example, a customer may be considered

low risk but their business represents a substantial part of the REA's turnover. A trigger event that would not be material for smaller customers may be material for a REAs large customers, triggering the need apply CDD measures once again.

Applying a risk based approach, REAs should take into consideration the evolving risk profile of existing customers when assessing their AML/CFT risk. While customers with a consistent risk profile are not exempt from ongoing CDD measures, resources should be focussed on those which are more recent, or those with changes in the pattern of business or type of properties they are interested in.

8. Targeted Financial Sanctions

8.1 What are sanctions?

Targeted financial sanctions (**TFS**) are legal restrictions imposed by the United Nations, European Union, United Kingdom or Gibraltar against states, people, businesses, organisations and financial institutions (the **designated persons**) in appropriate cases to achieve specific international policy or security objectives. TFS include both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons.

TFSs can be issued in relation to Terrorist Financing (see section 1.2) or Proliferation Financing (see section 2.5).

8.2 Why do I need to know about sanctions?

It is an offence under section 9 of the Sanctions Act 2019 to breach, or to assist a breach, of an international sanction. You are not therefore allowed to deal with designated persons that are subject to a TFS unless you have a licence, permit or other authorisation to do so issued in accordance with Section 10 of the Act.

8.3 What are my sanctions obligations?

REAs must have policies, controls and procedures in place to check all of its customers on the international sanctions lists.

The OFT recommends that REAs subscribe to the consolidated lists of UN, UK and EU sanctions and that they carry out checks using the lists in the 'Sanctions' section of the GFIU's website (www.gfiu.gov.gi/sanctions). Here you will also have access to the GFIU's Financial Sanctions Guidance Notes to assist you further.

8.4 Who needs to be checked?

Every person in relation to which a REA is required to carry out CDD measures as set out in Section 6 and every entity involved in the transaction.

8.5When do I carry out these checks?

REAs must carry out TFS checks:

1. When they have a new customer or business relationship; and
2. on existing customers as and when the TFS lists are updated. REAs must therefore have systems to be notified when this happens. The OFT recommends that REAs subscribe to the consolidated lists of UN, UK and EU

sanctions. The GFIU's Themis online system provides updated TFS lists.

8.6 What do I do if I have a positive hit?

If you have a positive hit you must:

1. immediately freeze any identified assets or funds held or controlled by that person or entity without delay;
2. not deal with the assets or make them available to the designated person or entity;

You must also report to the GFIU as soon as practicable if you know or have reasonable cause to suspect that a person is a designated person. When reporting you must include:

1. the information or other matter on which the knowledge or suspicion is based;
2. any information you hold about the person ort designated person by which they can be identified;
3. details of any funds and economic resources that you have frozen.

8.7 Is everything I need to know about sanctions contained in this guidance?

No! These guidance notes only set out brief overview of the applicability of the Sanctions Act to the REA sector. There are other obligations in the Sanctions Act that are not referred to in this document. You should not therefore regard this document as an exhaustive authority. The full body of the Act may be found in the 'Documents' section of the 'AML/CFT' page of the OFT's Website (www.oft.gov.gi).

The OFT recommends that REAs read the GFIU's Financial Sanctions Guidance Notes that can be downloaded from the 'Sanctions' section of the GFIU's website (www.gfiu.gov.gi/sanctions).

9. Record keeping, data & annual returns

9.1 What records must be kept?

REAs must keep records and data about:

1. All transactions and business relationships (section 9.2 and 9.3); and
2. staff training (section 10.3).

The records and data must be readily available for inspection by the OFT on request.

9.2 Transactions and business relationships

REAs' general record keeping obligations are set out in section 25 POCA. All REAs must have appropriate systems in place for recording and storing:

1. a copy of the documents and information collected while applying CDD measures (see section 6);
2. the supporting evidence and records of of all property sale and property rental transactions (see section 9.3);
3. the written risk assessment of all customers and business relationships the action taken in respect to any suspicious activity detected (see section 6.14); and
4. the action taken in respect of any suspicious activity detected (see section 5.5 to 5.7).

In addition, REAs must also keep the records of any difficulties encountered

during the CDD process (POCA section 10(l)).

9.3 What type of data must be collected about these transactions?

As much data and information as you can about the transactions, including account files and correspondence, as well as any other information that may reasonably be necessary to identify such transactions. The evidence and records must be sufficient so as to permit the reconstruction of individual transactions so as to provide evidence for the prosecution of criminal activity where necessary (Section 25 (2A) POCA).

You must also keep sufficient data to allow you to complete and submit Annual Returns to the OFT (see section 9.6).

9.4 How long must I keep the records for?

REAs must keep these records for inspection for five years after the date of the relevant transaction or the date when staff training was delivered (Section 25(3) POCA).

9.5 What will the records be used for?

The OFT may use it powers to request copies of the REA's records at any time. REAs should be able to provide the records and data to the OFT swiftly.

REAs are also required to review their CDD records in accordance with ongoing requirements of section 12(2)(b) POCA (see section 7).

Additionally, REAs are required to submit annual returns to the OFT providing information and data about established business relationships and financial transactions received by the business during that year which should correspond with the REA's records. The annual return form can be found in the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

9.6 When are the Annual Returns due?

Two returns will be submitted annually:

1. Financial data return - The new REA annual return process requires that financial data be submitted by REAs. The reporting period shall be from 1 January to 31 December of the previous year. The returns must be submitted by 31 March every year. This amended reporting period allows the OFT to collect more up to date, uniform and easily comparable data from each REA annually.
2. Non-financial data - Prior to the renewal of their business licence REAs will receive a business licence renewal notice which shall require them, as part of the renewal process, to provide non-financial data for the licence term which is due to expire.

9.7 What if I miss the deadline?

We strongly urge that you take the appropriate steps to ensure that your business submits its annual returns on time. REAs who have failed to fulfil their responsibilities may not be allowed to renew their business licence. They may also be subject to enforcement action by the OFT that may include:

1. a fine;
2. the suspension or revocation of their business licence; and/or
3. temporary bans for persons in managerial positions.

9.8 What will the OFT do with the Annual Return?

The information will allow the OFT to:

1. collect data about REA transactions;
2. monitor REAs' compliance with their obligations under POCA and these guidance notes; and
3. identify suspicious trends and money laundering and terrorism financing schemes .

This data will also help the OFT analyse each REA on a risk based approach to determine the likelihood of the REA being targeted by criminals.

The OFT may carry out onsite visits and seek information from REAs in relation to the information contained in annual returns to ensure that these are being completed accurately. The OFT may also request REAs records to examine and investigate any suspicious activity.

The failure by a REA to submit an Annual return is automatically considered as non-compliance by the OFT.

The data may be provided to other AML/CFT supervisory authorities and law enforcement bodies as permitted under the law.

10. Employer & employee responsibilities

10.1 What are my responsibilities as an employer?

REAs must ensure that they have screening procedures to ensure high standards when hiring employees.

Additionally, employers have a duty to ensure that its employees have received appropriate training to help them both recognise and report potential money laundering. Staff must be made aware of the following:

1. what money laundering and terrorist financing is;
2. the laws concerning AML/CFT, including POCA, and the requirements in these guidance notes;
3. the ML/TF risk to which the REA sector generally is exposed (see Schedule 2);
4. the ML/TF risk to which the REA is exposed (see section 3);
5. the REA's AML/CFT policies, controls and procedures including CDD measures (see sections 4 and 6);
6. how to manage business transactions on a risk based approach and identify high risk customers and/or high risk behaviour (see section 6);
7. how to report suspicious activity to the MLRO;
8. the penalties for committing offences under POCA and related legislation; and
9. relevant data protection requirements.

It is essential to also train employees to understand how money laundering and terrorist financing schemes could take place through the business by providing examples of this (See Schedule 2 for examples of money laundering methods and schemes through REAs).

10.2 How often does training need to be given?

Employee training must be an ongoing exercise which is regularly under review. Risk assessments and polices must be regularly updated and circulated to members of staff.

10.3 Records.

REAs must keep a staff training record to demonstrate to the OFT that its staff are aware of the business's AML/CFT policies and procedures (see Section 9).

10.4 What responsibilities do employees of REAs have?

Employees of REAs must:

1. know who their MLRO is and what the MLRO's role is;
2. be able to detect suspicious activity and report it to the MLRO;
3. be aware of the steps taken by the business to ensure it is not used for ML/TF;
4. have access to and familiarise themselves with all of the business's AML/CFT policies and procedures; and
5. be aware of the penalties for committing offences under POCA and related legislation.

It is the responsibility of the REA to provide adequate training to its employees (see sections 10.1 to 10.2).

11.Reporting Ownership & Management Changes

11.1 REA reporting requirements.

REAs are required to report to the OFT where there is a change to their ownership or management.

11.2 What changes must be reported?

The OFT must be notified of a change to:

1. the BO of a REA, including, but not limited to shareholders, partners and silent partners;
2. the board of directors, an executive and/or another senior manager of a REA;
3. a person holding or appearing to the OFT to intend to hold a management function in a REA; and
4. a person in accordance with whose wishes or directions any person involved in the carrying on of the business of a REA acts or it appears to the OFT will act.

11.3 When do I need to report the change?

The OFT must be notified in writing within seven days of the relevant change.

11.4 What will the OFT do with the information?

Upon receipt of a notification the OFT shall conduct a fit and proper assessment of that person.

12. Useful contacts

12.1 Gibraltar Financial Intelligence Unit

The Gibraltar Financial Intelligence Unit (GFIU) receives, analyses and disseminates financial intelligence gathered from Suspicious Activity Reports (SARs) (see 5.8 above).

Suite 832, Europort, Gibraltar

Tel: (+350) 20070211

Fax: (+350) 20070233

E-mail: gfiu@gcid.gov.gi .

13. Schedule 1 - How to identify customer ML/TF risk

1. Identifying risk factors.

This schedule sets out a number of common factors that a REA or its employees may take into account when carrying out an AML/CFT risk assessment of a customer or a transaction.

For assessing a REA's ML/TF risk please refer to section 3.

It is important to note however that these are only indicators to consider when assessing risk. The identification of one of these factors need not necessarily mean that money laundering is, or will be, taking place, but they will assist the REA and its employees in applying the risk based approach and ultimately deciding whether the activity, when considered with the rest of the information at their disposal, is suspicious.

The factors listed in this schedule are not an exhaustive list and the REA and its employees should take into account all of the information at their disposal to determine if there is money laundering or terrorist financing risk. If more information is required, it should be requested before proceeding with a transaction.

2. Assessing low risk customers?

Pursuant to Section 16 (3) and (5) POCA, when assessing the risks of ML/TF relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels, a REA must take into account at least:

1. the factors of potentially lower risk situations set out in Schedule 6 POCA; and
2. the risks identified within any information that is made available to the REA pursuant to the National Coordinator for Anti-Money Laundering and Combatting Terrorist Financing Regulations 2016.

3. Who are high risk customers?

Pursuant to Section 17 (4) POCA, when assessing the risks of ML/TF REAs must take into account at least the factors of potentially higher- risk situations set out in Schedule 7 POCA.

The following are indicators of high risk customers:

1. brand new customers carrying out large one-off transactions;
2. customers engaged in a business which involves the constant movement of significant amounts of cash;
3. customers who carry out transactions that:
   i) do not make commercial sense, e.g. selling properties at an undervalue;
   ii) have an unusual pattern; and/or
   iii) are complex.
4. for existing customers:
   i) the transaction is different from the normal business of the customer;
   ii) the size and frequency of the transaction is different from the customer's normal pattern;
   iii) the pattern has changed since the business relationship was established; and

iv) there has been a significant or unexpected improvement in the customer's financial position and the customer can't give a proper explanation of where money came from.

5. complex business ownership structures with the potential to conceal underlying beneficial owners (REAs are required to understand the nature of the customer's business and its ownership and control structure);
6. politically exposed persons (these will always require enhanced CDD, see section 6.13 of the guidance notes and paragraph 4 below); and/or
7. persons:

   i) from high-risk jurisdictions;

   ii) transferring money from banks in high-risk jurisdictions; and/or

   iii) making payments in the currency of high-risk jurisdictions.

A list of high-risk jurisdictions can be found on the FATF's website: http://www.fatf-gafi.org.

4. Who are politically exposed persons?

A politically exposed persons (**PEP**) is defined in section 20A POCA as a person who is or has been entrusted with prominent public functions and includes the following:

1. Heads of State, heads of government, ministers and deputy or assistant ministers;
2. Members of parliament or of similar legislative bodies;
3. Members of the governing bodies of political parties;
4. Members of supreme courts, of constitutional courts or of other;
5. High-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
6. Members of courts of auditors or of the boards of central banks;
7. Ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
8. Members of the administrative, management or supervisory bodies of State-owned enterprises; and
9. Directors, deputy directors and members of the board or equivalent function of an international organisation

(Note however that middle-ranking or junior officials carrying out a public function referred to in 1 to 8 are not regarded as PEPs).

These individuals, who may be local or international PEPs, are usually at a higher risk of possible connection to money laundering due to the position and influence they hold and will require enhanced CDD measures to be applied. This also includes the PEP's 'family members' and 'persons known to be close associates' (see definition in section 20A POCA).

For more information about transacting with PEPs see section 6.13 of the guidance notes.

5. What is high-risk behaviour?

When determining risk and to what extent to apply CDD measures a REA must, at least, take into account the following risk variables:

1. the purpose of the relationship;
2. the size of the transaction undertaken; and
3. the regularity or duration of the business relationship (POCA s. 11(5)).

The following are indicators of high-risk behaviour:

1. an unwillingness to produce evidence of ID or the production of unsatisfactory evidence of ID;
2. where the customer is, or appears to be, acting on behalf of another person, an unwillingness to give the name(s) of the person(s) they represent;
3. a willingness to bear very high or uncommercial penalties or charges;
4. an unwillingness to disclose the source of funds or source of wealth; and/or
5. situations where the customer's source of funds are unclear.

6. Monitoring patterns of business.

Risk assessments must also include the review and monitoring of business patterns and unusual transactions. Monitoring these business patterns is essential to the implementation of an effective risk-based approach, for example:

1. a sudden increase in business from an existing customer;
2. uncharacteristic transactions which are not in keeping with the customer's financial situation;
3. peaks of activity at particular locations or properties; and/or
4. unfamiliar or untypical types of customer or transaction.

For more information on typical money laundering methods and schemes see Schedule 2.

7. Enhanced due diligence and reporting.

The indicators above may, when assessed by the REA or its employees, require enhanced due diligence to ensure that the AML/CFT risk is understood appropriately and the necessary risk assessment is carried out (see section 6.10 of the guidance notes).

8. Using this information

If the REA's MLRO, having considered all the factors surrounding the customer and the transaction, believes there is a risk of money laundering, they should submit a suspicious activity report (see sections 5.6 to 5.8 of the guidance notes).

Schedule 2 - Money laundering methods & schemes

1. Money laundering through REAs.

Criminals wishing to launder illicit funds through the services provided by REAs use numerous schemes and complex procedures. In order to ensure the implementation of robust and adequate systems for the deterrence and detection of these schemes it is important for REAs to understand how their services can be manipulated and utilised by these criminals.

2. Common money laundering schemes

This schedule provides examples of common money laundering and terrorist financing schemes identified internationally. They are provided to illustrate examples of how Gibraltar REAs may be miss-used. It is important to note however that while these are only some of the more common schemes they are not an exhaustive list. Furthermore, they do not offer examples of money laundering schemes which have been identified in Gibraltar. REAs must therefore be vigilant of the AML/CFT risks specific to the REA sector in Gibraltar generally and conduct an appropriate risk assessment to identify the AML/CFT risk which are specific to the businesses (Section 3 of the guidance notes).

3. Examples

Property improvements and development:

Criminals wishing to increase the amount of money that can be laundered through the purchase of a property sometimes pay for improvements within the property with the use of illicit funds, enabling these funds to be integrated into the legitimate financial system once the property is sold at a higher price.

Loans and mortgages:

Criminals obtain loans or mortgages from lending entities as a cover to launder the criminal proceeds. The mortgage or loan is then paid in lump sums of cash repayments. This process hides the true nature of the funds and makes the cash payments used to make the repayments seem completely legitimate.

Third party property purchase:

Criminals provide illicit funds to third party individuals who purchase properties on behalf of the criminal. These individuals are usually family members of acquaintances who have no previous criminal records, ensuring the risk of suspicious activity detection is kept at a minimal.

Successive sales:

In order to decrease the level of detection even further, many criminals also make quick successive sales of properties at a much higher value to companies or trusts who are ultimately owned by the criminal or third parties associated to the criminal. This gives the criminal an opportunity to launder illicit funds whilst still maintaining the property under their 'possession'. It also conceals the criminal's ownership of the property, again reducing the risk of detection.

Non-local criminals investing in local property:

Non-local criminals may also try to purchase away from their home jurisdiction. This both conceals the illicit funds from regulating entities in their homeland and also avoids confiscation within their jurisdiction should their suspicious activity be detected.

Falsification of property value:

Criminals sell or buy properties at a value way below or above the property's true market price. When the property is under-evaluated the difference in value is then settled between the buyer and the seller through a private cash payment of illicit funds which is kept undisclosed to the REA. When a property is over evaluated this helps the criminal obtain a larger mortgage or loan from the lender, the mortgage or loan repayments are made using illicit funds. The higher the lending amount, the higher the amount of illicit funds which can be laundered by making the repayments.

Use of REA services to reduce suspicious activity detection:

Many services provided by REAs may unknowingly assist the criminal in the execution of their money laundering scheme. The criminal may request the business receive or transfer large amounts of cash on his behalf, deal with his loan or mortgage arrangements and hence use the REA to reflect legitimacy and professionalism within his scheme.

Rental and leasing:

Criminals may lease out properties and provide the tenant, in turn associated with the criminal, illicit funds to pay for the lease. In this process illicit funds are integrated into the system as legitimate rental income. Alternatively the property may not be leased at all yet an arrangement is in place for the owner to receive false rental payments from non-existent tenants.

A full or large payment of a long let rental is made in cash up front.

4. More examples and information?

For more information and concrete case studies on how the real estate sector can be used for money laundering or terrorist financing REAs can consult the FATF's report on Money Laundering & Terrorist Financing through the Real Estate Sector which can be found in the 'AML/CFT' section of the OFT's website (www.oft.gov.gi).

The study explores the means by which illicit money is channelled through the real-estate sector to be integrated into the legal economy and identifies some of the control points that could assist in combating this phenomenon.

5. Newly identified local schemes

In order to assist REAs with their AML/CFT regulatory requirements the OFT will update these guidance notes when it uncovers specific money laundering schemes which are using REAs in Gibraltar.

In the meantime, if any REA would like to highlight identified money laundering schemes or circumstances which may potentially lead to money laundering they may do so by contacting the OFT. The OFT will not disclose any sources to third parties other than to enforcement bodies and other relevant AML/CFT authorities.

Schedule 3 – Glossary of Abbreviations

AML/CFT	Anti-money laundering and countering the financing of terrorism
BO	Beneficial owner
Cash	Money in coins or notes.
CDD	Customer due diligence
FATF	Financial Action Task Force
GFIU	Gibraltar Financial Intelligence Unit
ID	Personal identification document
ML/TF	Money laundering and terrorist financing
MLRO	Money laundering reporting officer
NRA	National risk assessment
OFT	Office of Fair Trading
PEP	Politically exposed person
PF	Proliferation financing
REA	Real estate agent and letting agent
SAR	Suspicious activity report
TFS	Targeted financial sanctions