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

Guidance Notes for Real Estate Agents (REAs)

Contents

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.

Issued: April 2018
Updated: July 2019
Version: 1.4

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

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.

The vulnerabilities and risks of money laundering and terrorist financing in Gibraltar are set out in the National Risk Assessment (**NRA**) published by HM Government of Gibraltar. 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 compliance with the AML/CFT obligations set out in the Proceeds of Crime Act 2015 (**POCA**) (see Chapter 2 below) by Real Estate Agents. As a result, it is issuing these guidelines to assist REAs and their employees and to give an overview of their legal obligations as set out in POCA. 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 all REAs who are operational in Gibraltar and to REAs' employees.

1.5 What are Real Estate Agents?

Real Estate Agents (**REAs**) are businesses that carry out one or both of the following activities:

1. Property sale transactions

   The business 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 REA representing a buyer will assist in the search of the property and may advise on the fairness of the price.

   A REA 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.

2. Property rental

   The business provides services relating to the rental, leasing, letting or other similar property transaction.

A REA representing the landlord, head-lessor or other persons wishing to rent the property will list and advertise the property for rental to try to secure a tenant. The REA may provide additional services including the collection of rental proceeds, the management of the property and the holding of any deposits once the property is rented.

The REA representing the tenant will advise the client on property rental prices and assist in successfully securing the rental of a property.

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

1.6 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 carried out by a third party which is not the owner of the property however then that third party will be considered an REA. This will be the case irrespective of whether the developer and the REA 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.

1.7 What is the OFT's role?

As Supervisory Authority under POCA (see Chapter 2 below), the OFT is responsible for ensuring that REAs are compliant with their AML/CFT obligations under POCA in order to reduce the money laundering and terrorist financing risk for REAs as set out in HM Government of Gibraltar's AML/CFT National Risk Assessment.

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

1.8 What are a REA's Responsibilities?

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 Chapter 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 Chapter 4 below);
3. Appointing a MLRO who understands the business's risks and responsibilities under POCA and who shall be responsible for all AML/CFT matters (see Chapter 5 below);
4. Carry out appropriate risk assessments of customers on a risk-based approach and keep relevant documentation (see Chapter 6 below); and
5. Keep appropriate AML/CFT records and submit annual reports to the OFT (see Chapter 7 below); and
6. Training staff to ensure they are aware of AML/CFT risks and of the business's AML/CFT polices (see Chapter 8 below).

1.9 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 Chapter 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 following a link contained 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 is Part III. Measures to prevent the use of the financial system for purposes of money laundering and terrorist financing. For ease of reference, REAs are defined as "relevant financial business" in Section 9 of POCA.

2.4 If I read these guidance notes, do I need to bother with POCA?

These guidance notes should be regarded as regulatory standards for the purposes of the Proceeds of Crime Act 2015. They should be read in conjunction with your legal AML/CFT obligations as set out in POCA.

3. REA risk assessments

3.1 What is a risk assessment?

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.

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 and finance terrorism please see Schedule 2 below.)
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 Chapter 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 8.1 and 8.2 below)

4. Are the business's customer due diligence methods appropriate and sufficient to minimise the risk (see Chapter 6 below)?
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.

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

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 on the FATF's website: http://www.fatf-gafi.org

You can also find a link to the report on the 'AML/CFT' section of the OFT's website (www.oft.gov.gi).

3.4 I have carried out my business's risk assessment. I'm done, right?

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 the effectiveness of AML/CFT systems and policies in place.

4. AML/CFT policies and procedures

4.1 Risk based policies and procedures.

REAs need to establish policies and procedures to protect and prevent their business from being used as a tool for money laundering and terrorist financing.

All REAs must have a clear written AML/CFT policy based on the degree of risk associated to the specific business (see Chapter 3 above). The policy should contain procedures to identify and manage its money laundering and terrorist financing risks. This policy must have well-defined procedures on how the business and its employees are expected to deal with customers in order to minimise the business's AML/CFT risk exposure. The policy should also contain procedures to identify and manage its money laundering and terrorist financing risks.

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

4.2 Who implements the policy?

The AML/CFT policy must be adopted by the Board as well as a director, executive or other member of the business's senior management who will also have been assigned responsibility for AML/CFT.

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 to launder money (in accordance with Chapter 3 above);
2. carry out customer due diligence (see Chapter 6 below) and monitor customers' business activities;
3. submit annual reports to the OFT and reply to audit queries (see Chapter 7 below);
4. 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 5.8 below);
5. keep customer, transactional and staff training records (see Chapter 7 below);
6. 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 to the MLRO should suspicious activity be detected (see 8.4 below);

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?

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

4.5I have a policy, I now comply right?

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, then it is of no use and the REA will not be meeting its AML/CFT responsibilities.

It must therefore be made readily available to all employees and they should be trained about how to implement it (see Chapter 8 below).

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

You must also have an independent audit function to test your policies and ensure they are appropriate.

4.6 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. If not in writing you must be able to explain your business's ML/TF risk and its AML/CFT policies to the OFT upon request.

5. MLROs & their responsibilities

5.1 What is an MLRO?

All REAs must nominate a money laundering reporting officer or 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 on 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.

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 (Chapter 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.

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?

Reports from MLROs to the GFIU may be made by completing a Suspicious Activity Report (SAR). SAR forms can be downloaded from the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

SARs should be submitted to the GFIU by e-mail (gfiu@gcid.gov.gi) or delivered by hand to their offices at Suite 832, Europort.

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

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 Chapter 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 Sanctions

Sanctions are legal restrictions imposed by the United Nations, European Union, United Kingdom or Gibraltar against people, businesses, organisations and financial institutions in appropriate cases to achieve specific international policy or security objectives.

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 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.

The Act requires REAs to have policies, controls and procedures in place to check all of its customers on the international sanctions lists. Furthermore, REAs must ensure that appropriate ongoing checks are carried out on both new and existing clients as and when the sanctions lists are updated.

For more information refer to the 'Sanctions' section of the GFIU's website (www.gfiu.gov.gi/sanctions) where you will have access to the GFIU's Financial Sanctions Guidance Notes and to the sanctions lists.

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

5.13 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.

5.14 Is there more guidance for MLROs?

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

6. Customer due diligence & assessing risk

6.1 What is customer due diligence?

Customer due diligence (also known as 'know your customer' or KYC) is a process whereby a business carries out checks about its customers to establish who they are and whether there is a risk that they are involved in ML/TF.

It also involves obtaining information on the purpose and intended nature of the business relationship.

A REA must therefore verify the identity of their customers before doing business with them. It usually involves collecting identification documents and other personal information to allow the business to carry out a risk assessment.

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

6.2 Who needs to be checked?

Appropriate customer due diligence must always be completed on your customer.

Note however that an REA is also 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 a seller or a Landlord it will also therefore have to collect customer due diligence on both parties in the property transaction.

6.3 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 UBO, of the company is (see 6.4 below).

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 UBOs), 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 6.4 below).Due diligence is not required for banks, EU listed companies or Governmental entities.

6.3 What is an ultimate beneficial owner (UBO)?

A UBO is an individual:

1. on whose behalf a transaction or activity is being conducted; and/or
2. who ultimately owns or controls the customer.

That individual is the person who will ultimately benefit from 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 UBO.

Where an individual either owns or has control over a company, a trust or firm (or

similar non-legal arrangement) who is the REA's customer, that individual will be a UBO.

Broadly speaking a person is a UBO of a company, a trust or firm (or similar non-legal arrangement) if they directly or indirectly:

1. hold more than 25% of the shares in the company;
2. hold more than 25% of the voting rights in the company;
3. hold the power to appoint or remove a majority of the board of directors of the company;
4. have the right to exercise a significant influence or control over the company; or
5. have the right to exercise a significant influence or control over a trust or firm (or similar non-legal arrangement) where that trust or firm meets one or more of the criteria in points 1 to 4 above.

A person is also a UBO where they are in agreement with another UBO and they jointly meet one or more of the criteria in points 1 to 5 above.

For more guidance about UBO's 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.

6.4 When must I carry out due diligence checks?

Due diligence needs to be carried out before entering into a business relationship. A business relationship is formed when an offer for the purchase or rental of a property is accepted.

Due diligence must be performed before any financial transactions take place.

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

If a REA is satisfied that a third party has already collected appropriate due diligence on its customers they may rely on that due diligence as long as they are satisfied that:

1. the due diligence is appropriate to the customer's level of risk as assessed by the REA; and
2. the due diligence is current and up to date.

Copies of the due diligence documentation should be provided by the third party to the REA prior to the REA providing their services to the Customer.

The responsibility to collect due diligence and keep records on its customers shall always ultimately remain with the REA.

It is not possible to rely on third parties' risk assessments!

6.6 What happens if I have been unable to collect due diligence?

If any person or entity is unable or unwilling to submit the relevant customer due diligence documents requested and the REA is unable to carry out appropriate due diligence 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 5.8 above).

6.7 How do I carry out customer due diligence?

Customer due diligence allows 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 customer due diligence 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 customer due diligence 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 customer due diligence 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.

6.8 Low risk customers: An example of simplified customer due diligence.

This includes, but may not be limited to, collecting the following basic information:

1. Full Name;
2. date of birth;
3. residential address;
4. make a copy of the customer's original Passport/ID (or any other Government-issued photographic document); and
5. record the customer's source of income or wealth (e.g. employment)

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 Chapter 7 below).

6.9 High risk customers: an example of enhanced due diligence.

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 customer due diligence 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; and
3. Proof of the customer's source of funds commensurate to the transaction.

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

6.10 What am I looking for?

Due diligence 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.

Some examples of suspicious activity specific to the REA include:

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

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

6.11 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 3 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.

REAs must have risk management systems in place to determine whether a customer or the UBO 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.

Before entering into a transaction with a PEP, their family member or their close associate, the REA must:

1. carry out enhance due diligence (see 6.9 above);
2. have approval from senior management;
3. take adequate measures to establish the source of wealth and funds which are involved in the proposed transaction.

6.12 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.

6.13 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 5.6 above) or is suspicious (see 5.7 above) that ML/TF is or may be taking place.

If in doubt, submit a SAR! (see 5.8 above)

6.14 Ongoing monitoring

REAs are required to carry out ongoing due diligence with existing clients including:

1. scrutinising transactions to ensure that they are consistent with the REA's knowledge of the customer, their business and risk profile; and
2. ensuring that existing CDD (documents and data) collected is up to date and relevant, particularly for high risk customers.

6.15 Records.

REAs must keep copies of the documents requested while conducting customer due diligence procedures along with all relevant documents appertaining to the business relationship (see Chapter 7 below).

7. Record keeping & annual reports

7.1 What records must be kept?

All REAs must have appropriate systems in place for recording and storing:

1. customer due diligence documents and information (see Chapter 6 above);
2. details of property sale and property rental transactions (see 7.2 below);
3. written risk assessment of all customers and the action taken in respect to any suspicious activity detected (see 6.11 above);
4. the action taken in respect of any suspicious activity detected; and
5. staff training records (see 8.2 below).

REAs must keep these records for inspection for five years after the date of the relevant transaction, the date the relationship with the Customer is terminated or the date when staff training was delivered.

The documents must be readily available to the OFT for inspection.

7.2 What type of data must be collected about transactions?

As much data and information as you can about the business relationships and transactions. This includes account files and business correspondence where relevant. As a minimum you must keep at least sufficient data to allow you to complete and submit an Annual Report. (see 7.3 below).

7.3 What will the records be used for?

It is a legal requirement pursuant to section 25 of POCA to maintain appropriate records.

Additionally, REAs are required to submit annual reports 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 Report form can be found in the 'AML/CFT' section of the OFT's website: www.oft.gov.gi.

The OFT may use it powers to request copies of the REA's records at any time. REAs should ensure that all CDD information and transaction records are made available to the OFT swiftly.

7.4 What will the OFT do with the Annual Report?

The information will allow the OFT to:

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

The data may be provided to other POCA supervisory authorities and law enforcement bodies.

7.5 How does the OFT monitor compliance by REAs?

The OFT works closely with the GFIU, law enforcement bodies and other supervisory authorities to monitor the market and uses various sources to acquire information and determine whether the business is complying with their AML/CFT requirements or is being used for money laundering or terrorist financing. 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 money laundering criminals.

The OFT may carry out audits of the REAs based on the information in the Annual Reports to ensure that these are being completed accurately by REAs. The OFT may also request REAs records to examine and investigate any suspicious activity.

Failure to submit an Annual Report is an automatic act of non-compliance by the REA.

7.6 When are the Annual Reports due?

To make it easier for REAs to prepare and submit these reports, the OFT has made this the same day as the due date for submission of accounts and tax returns by the REA to the Income Tax Office.

If the REA is a company, the Annual Return is due nine months after the REA's financial year end.

If the REA is a sole trader it is due on 30th November of each year.

Annual Report must be submitted for data of transactions from 1st July 2017 onwards.

7.7 What if I miss the deadline?

We strongly urge that you take the appropriate steps to ensure that your business submits its Annual Reports. Those REAs who have failed to fulfil their responsibilities will be subject to enforcement action by the OFT. This may include:

1. financial penalties up to EUR 1 million;
2. the suspension or revocation of their business licence;
3. temporary bans for persons in managerial positions; and/or
4. a direction to the business to take/ refrain from taking action.

8. Employer & employee responsibilities

8.1 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 client facing 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. laws concerning money laundering and terrorist financing, including POCA, and the requirements in these guidance notes;
3. the AML/CFT risk to which the REA sector generally is exposed (see Schedule 2);
4. the AML/CFT risk to which the REA is exposed (see Chapter 3 above);
5. the REA's AML/CFT policies and procedures including due diligence requirements (see Chapter 4 above);
6. how to manage business transactions on a risk based approach and identify high risk customers and/or high risk behaviour (see Chapter 6 above);
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).

8.2 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.

8.3 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 Chapter 7 above).

8.4 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 money laundering or terrorist financing;
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 8.1 above).

9. Useful contacts

9.1 Office of Fair Trading

The Office of Fair Trading (OFT) has been appointed as a supervisory authority under the Proceeds of Crime Act 2015. Additionally it is responsible for business licensing and for consumer protection in Gibraltar.

Suite 975 Europort, Gibraltar

Tel: (+350) 20071700

Fax: (+350) 20071950

E-mail: aml.oft@gibraltar.gov.gi

9.2 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 .

Schedule 1 - How to identify AML/CFT risk & apply commensurate customer due diligence

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.

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 to ensure that there are no suspicions before proceeding.

2. Who are high risk customers?

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 do not make commercial sense, e.g. selling properties at an undervalue;
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 customer due diligence, see 6.8 of the guidance notes); 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 Financial Action Task Force (**FATF**) website: http://www.fatf-gafi.org.

3. Who are politically exposed persons?

A politically exposed persons (**PEP**) is defined in Section 20A of 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

(no public function referred to in 1. to 9. above shall be understood as covering middle-ranking or more junior officials).

These individuals, who may be local or international PEPs, are usually at a higher risk of possible connection to money laundering and terrorist financing due to the position and influence they hold. 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 6.11 above.

4. What is high-risk behaviour?

When determining risk and to what extent to apply customer due diligence 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; and/or
4. situations where the customer's source of funds are unclear.

5. 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.

6. 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 6.9 of the guidance notes).

7. 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 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 (chapter 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.

Accumulation of cash deposits

Criminals make regular cash deposits to different bank accounts under the reporting monetary threshold. This process usually involves a high number of deposits and accounts making it very hard to detect the suspicious activity. Once these funds have been integrated into the legitimate financial system, cheques are then made to purchase properties.

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.

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 Financial Action Task Force's (**FATF**) report on Money Laundering & Terrorist Financing through the Real Estate Sector on the FATF's website: http://www.fatf-gafi.org

You can also find a link to the report on 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.