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

Guidance Notes for Real Estate Agents (REAs)

Contents

Disclaimer

The information contained in these guidelines is not intended to be legal advice and is for guidance and information purposes only. For the definitive authority on your legal obligations regarding anti-money laundering and combatting the finance of terrorism, please refer to the Proceeds of Crime Act 2015.

Issued: April 2018
Updated: n/a
Version: 1.0

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 (see section 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, or REAs, are businesses that carry out one or both of the following activates:

1. Property sale transactions

   The REA represents either the buyer or the seller during the selling or purchase of a property. The agent'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. This includes property developers selling their own properties directly.

   A REA representing a buyer will assist in the search of the property and advice 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 contact the REA.

2. Property rental

The REA 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 services related to the sale and/or rental of real property in Gibraltar.

1.6 What is the OFT's role?

As a Supervisory Authority under POCA (see Chapter 2 below), the OFT is responsible for ensuring that REA's are compliant with their AML/CFT obligations under POCA in order to reduce the risk of money laundering and terrorist financing in this sector 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**).

1.7 What are a REA's Responsibilities?

REAs' responsibilities include, but are not limited to:

1. Carrying out a risk assessment of their business's misuse for the laundering of money and/or the financing of terrorism (see Chapter 3 below);
2. Establishing appropriate policies and procedures commensurate to the business's risks to prevent their business being used to launder money or finance terrorism (see Chapter 4 below);
3. Appointing a nominated officer who understands the business's risks and responsibilities under POCA and 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. Training staff to ensure they are aware of AML/CFT risks and of the business's AML/CFT polices (see Chapter 8 below); and
6. Keep appropriate AML/CFT records and submit annual reports to the OFT (see Chapter 7 below).

1.8 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 the POCA?

This Act may be found in the 'AML/CFT' section 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 Government's Gibraltar laws website by searching for "Proceeds of Crime" (www.gibraltarlaws.gov.gi)

3. REA risk assessments

3.1 What is a risk assessment?

A risk assessment is the process of assessing the level of risk that your business could be exposed to money laundering and terrorist financing. As a result of this analysis the appropriate systems and policies must be established and introduced by the business with the objective of mitigating these risks.

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

REA's must subjectively assess the relevant risks to the business with regards to AML/CFT. 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 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?
4. Are the business's customer due diligence methods appropriate and sufficient to minimise the risk (see 6 below)?
5. How does the business's:
   a. customer base;
   b. methods of financial transactions;
   c. methods of communication with customers;
   d. nature or services provided; and
   e. 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 seller 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: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachforrealestateagents.html

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.

All REAs must have a clear AML/CFT policy based on the degree of risk associated to the specific business (see Chapter 3 above). The policy will assist 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 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. It must be made available to all employees of the business and the OFT.

4.2 What controls and procedures must REAs have in place?

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

1. assess the risk of their business being used by criminals to launder money (in accordance with section 3 above);
2. carry out customer due diligence (see 6 below) and monitor customers' business activities;
3. submit annual reports to the OFT and reply to audit queries (see 7 below);
4. report suspicious clients or transactions with a high money laundering risk (see 5.8 below);
5. keep customer, transactional and staff training records (see 7 below);
6. ensure employees:
   a. are aware of POCA and these guidance notes;
   b. are aware of the business's AML/CFT policy;
   c. have the necessary training; and

d. report to the nominated officer should suspicious activity be detected (see 8.3 below);

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

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.

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 someone who works in the business. They play an important role, so they must be someone who:

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

5.3 What is the MLRO's role?

The MLRO is generally responsible for dealing with any AML/CFT matters, including carrying out appropriate risk assessments of the business and its customers (in accordance with sections 3 and 6 respectively) and ensuring all AML/CFT policies and procedures are adhered to and understood by all employees.

The nominated officer 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 GFIU by submitting a Suspicious Activity Report (**SAR**) (see 5.8 below).

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

1. putting in place and operating AML/CFT controls and procedures;
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).

5.5 How does an 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 knows, suspects or has reasonable grounds to suspect that another person is engaged in money laundering, or is attempting to launder money they must report this to GFIU at the earliest possible opportunity using an SAR.

5.6 What is meant by 'knowledge'?

An 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 REA's customer 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 REA's customer to support their evaluation.

5.8 How does the MLRO report to GFIU?

Reports from MLROs to 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) and submitted to GFIU by e-mail (gfiu@gcid.gov.gi) or delivered by hand to their offices at Suite 832, Europort.

5.9 Must the MLRO prevent a suspicious transaction taking place?

The MLRO must seek consent from GFIU before proceeding with a transaction it suspects is being carried out to launder money or finance terrorism.

A nominated officer may also ask GFIU for consent in advance to continue with any transactions that they've reported to avoid continuing a transaction illegally.

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

No! The MLRO must NOT inform the person they have reported to GFIU who is suspected of laundering money or financing terrorism. Tipping off is an offence under Section 5(1), POCA.

5.11 What happens in the nominated officer's absence?

A MLRO's duties can be temporarily delegated to someone else. This does not however relieve the nominated officer 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 GFIU.

6. Customer risk – assessment and monitoring

6.1 What is customer due diligence?

Customer due diligence, sometimes known as 'know your customer' or KYC, involves verifying the identity of your 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.

6.2 Who needs to be checked?

Appropriate customer due diligence must always be completed on both parties in a property sale or rental transaction.

Where your customer is 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. The UBO is the individual who ultimately owns the company and will benefit from the transaction.

If the customer is acting on behalf of someone else, appropriate identification of that third party must also be requested.

Due diligence is not required for banks, EU listed companies or Governmental entities.

6.3 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.

6.4 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 customers level of risk as assessed by the REA;
2. the due diligence is current and up to date; and
3. copies of the due diligence are 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!

6.5 What if a customer does not provide due diligence?

If any person or entity is unable or unwilling to submit the relevant customer due diligence documents requested by the REA, you must consider terminating any current business relationship with the individual or entity and submit a Suspicious Activity Report (see 5.8 above).

6.6 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 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.

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 risk will require a simplified due diligence process and a high risk transaction or customer will require an enhanced due diligence process. For guidance on how to apply appropriate levels of customer due diligence commensurate to the customer risk level please see Schedule 1.

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

This includes collecting the following basic information:

1. Full Name;
2. Date of Birth;
3. Residential address; and
4. A copy of the customer's Passport/ID (or any other Government-issued photographic document).
5. Recording the customer's source of income or wealth (e.g. employment)

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

6.8 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 7 below).

6.9 What am I looking for?

Due diligence documentation, along with all other surrounding factors 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 requesting a mortgage or loan from a financial lending entity;
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.

6.10 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.

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

6.11 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 7.1 below)

7. Record keeping & annual reports

7.1 What records must be kept?

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

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. The OFT encourages all REAs to keep a Suspicious Activity Transaction File; and
4. staff training records (see 8.2 below).

REA's 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 in order to prove the business is adhering to its AML/CFT obligations.

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. 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?

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.

The Annual Report form can be found in the 'AML/CFT' section of the OFT's website (www.oft.gov.gi).

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 prevent money laundering and terrorism financing schemes;
3. monitor REAs compliance with their obligations under POCA and these guidance nots.

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 GFIU and other regulating entities to monitor the market and uses various sources to acquire information and determine whether the business is complying with their AML/CFT requirements. This data will also help the OFT analyse each REA on a risk based approach to determine the likelihood of the REA being used by money laundering criminals.

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

7.6 When are the Annual Reports due?

To make it easier for REAs to prepare and submit these reports, the OFT has linked the reporting date to the date for submission of accounts and tax returns.

The Annual Return is therefore due nine months after the REA's financial year end.

Annual Report must be submitted for data 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 Annual Reports. Those REA's who have failed to fulfil their POCA 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?

Employers have a duty to ensure that client facing employees have effective training programmes available to help them both recognise and deter potential money laundering. Staff must be made aware of the following:

1. laws concerning money laundering and terrorist financing, including POCA and the requirements in these guidance notes;
2. the AML/CFT risk to which the REA sector generally is exposed;
3. the AML/CFT risk to which the REA is exposed (see 3 above);
4. the REAs AML/CFT policies and procedures including due diligence requirements (see 4 above);
5. how to manage business transactions on a risk based approach and identify high risk customers and/or high risk behaviour (see 6 above);
6. How to report suspicious activity to the MLRO.

7. penalties for committing offences under POCA and related legislation.

8. Relevant data protection requirements

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.

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 1 for examples of money laundering methods and schemes through REAs).

8.2 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.

8.3 What responsibilities do employees of REA's 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, procedures and risk assessments; 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

8.1 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

8.2 Gibraltar Financial Intelligence Unit

The Gibraltar Financial Intelligence Unit (GFIU) receives, analyses and disseminates financial intelligence gathered from Suspicious Activity Reports (SARs) (see 6.6 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 risk.

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. complex business ownership structures with the potential to conceal underlying beneficial owners; and/or
5. politically exposed persons or persons from high-risk jurisdictions (these will always require enhanced customer due diligence, see 6.8 of the guidance notes).

3. Who are politically exposed persons?

A politically exposed persons (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is or has been entrusted with a prominent public function. These individuals 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 close associates. Some examples of PEPs are the following;

1. Head of Governments;
2. Ministers (including Deputy of Assistant Ministers);
3. Members of Parliament and Political Parties;
4. Ambassadors;
5. Armed Forces officers within high rank positions; and
6. Members of the Supreme Court or other judicial bodies.

4. What is high-risk behaviour?

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 6.8 of the guidance notes).

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 assessments 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 launder by making the repayments.

Use of REA services to reduces 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 report on Money Laundering & Terrorist Financing through the Real Estate Sector: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20through%20the%20Real%20Estate%20Sector.pdf

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 anonymously by contacting the OFT