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

Guidance Notes for High-Value Dealers (HVDs)

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: June 2017
Updated: July 2019
Version: 2.3

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 and combatting the financing of terrorism.

1.2 What is money laundering and terrorist financing (ML/TF)?

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.

The buying and selling of high value goods in cash is recognised as a major avenue for money laundering activity. Whereas high value goods transactions that are done via electronic payment can be easily tracked by law enforcement, transactions that involve large sums of cash are virtually invisible, making them very attractive to criminals seeking to launder illicit funds. These activities assist the financing of terrorism and organised crime.

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 guidance notes?

The OFT is responsible for ensuring that dealers who receive large cash payments for goods comply with their legal AML/CFT obligations as set out in the Proceeds of Crime Act 2015 (see section 2 below). It is issuing these guidance notes to help these businesses (see 1.6 below) prevent ML/TF taking place through their trade in high value goods. These guidance notes therefore give an overview of their legal responsibilities and explain how the OFT will supervise their compliance with these. They should also use them to identify high risk transactions and customers.

1.4 Are these guidelines relevant to all cash payments?

No. Only large cash payments which are above the monetary threshold (see 1.5 below). They do not apply to cash payments for tobacco either (see 1.11 below).

1.5 What is the monetary threshold?

The OFT will consider cash payments in any currency with a value which is equal to, or greater than, £8,000 (eight thousand pounds) as a large cash payment. This amount is referred to as the monetary threshold and includes any currency equivalents, based on the exchange rate at the time the transaction is made.

Monetary threshold = £8,000

1.6 Who do these guidance notes apply to?

These guidance notes apply to three types of dealers:

1. High-Value Dealers (**HVDs**)

   Businesses that accept cash payments in any currency above the monetary threshold in exchange for goods;

2. Potential HVDs

   Businesses which are open to accepting cash payments in any currency above the monetary threshold in exchange for goods, but have yet to receive such payments (see Chapter 9 below); and

3. High Risk Dealers (**HRDs**)

   Businesses that are considered to have a higher inherent risk and vulnerability to ML/TF due to the nature of the goods they trade (see Chapter 10 below).

The guidance notes also apply to the employees of the above-mentioned businesses.

1.7 Is it prohibited to accept cash payments above the monetary threshold?

No. There is nothing wrong with accepting payments in cash above the monetary threshold.

Before accepting these cash payments however, the business will be required to collect and record information about the buyer of the goods and to risk assess the client and/or the transaction (see Chapter 6 below). If there is knowledge or suspicion that ML/TF will take place it must then report it (see 5.6 and 5.7 below).

1.8 Do all payments in cash above the monetary threshold need to be reported?

No. Only those payments which, having been risk assessed, are known or suspected of being made in connection with ML/TF (see 5.6 and 5.7 below).

1.9 Is the monetary threshold passed if cash is received over a period of time?

The monetary threshold is passed if the business receives:

1. a single cash payment of £8,000 or more;
2. a series of linked cash payments totalling £8,000 or more from the same customer (including payments on account); and/or
3. cash payments totalling £8,000 or more which appear to have been broken down into smaller amounts to fall below the £8,000 limit.

1.10 Do these guidance notes apply to card payments and bank transfers?

No. They apply to payments in cash only, i.e. money in coins or notes.

1.11 Do these guidance notes apply to the sale of tobacco?

No. The supervisory authority for the trade in tobacco is HM Customs (see 11.3 below).

1.12 What are the responsibilities of HVDs?

HVDs' responsibilities include, but are not limited to:

1. Carrying out a risk assessment of their business's attractiveness and vulnerability to ML/TF (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 money laundering reporting officer (**MLRO**) who understands the business's risks and responsibilities, its AML/CFT policies and who shall be responsible for all AML/CFT matters (see Chapter 5 below);
4. Carrying out risk assessments of its customers on a risk-based approach and keeping relevant documentation (see Chapter 6 below); and
5. Keeping appropriate AML/CFT records and submitting annual reports to the OFT (see Chapter 7 below); and
6. Training staff to ensure they are aware of ML/TF risks and of the business's AML/CFT polices (see Chapter 8 below).

For responsibilities of Potential HVDs and HRDs see Chapters 9 and 10 respectively.

1.13 What is the OFT's role?

As a Supervisory Authority under POCA (see Chapter 2 below), the OFT is responsible for ensuring that HVDs, are compliant with their AML/CFT obligations under POCA in order to reduce the risk of ML/TF in this sector as set out in the NRA.

Furthermore, the OFT is required to report evidence of ML/TF to the Gibraltar Financial Intelligence Unit (**GFIU**).

1.14 Do these guidance notes contain all I need to know?

No. These guidance notes are for information purposes only so that HVDs, Potential HVDs, HRDs 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).

1.15 How can I avoid complying with POCA and these guidance notes?

If a goods dealer is:

1. not a HRD (see Chapter 10 below); and
2. has an established policy not to accept cash payments above the monetary threshold;

it need not comply with these guidance notes at all.

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 ML/TF. 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 following a link contained in the 'Documents' section of '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 laws website (www.gibraltarlaws.gov.gi) by searching for "Proceeds of Crime"

2.3 Is all of POCA applicable?

All of POCA is applicable generally, however the most relevant part is Part III, 'Measures to prevent the use of the financial system for ML/TF purposes'. For ease of reference, HVDs 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. HVD Risk Assessments

3.1 What is a risk assessment?

A risk assessment is the process of assessing the ML/TF 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?

HVDs must subjectively assess the relevant ML/TF risks to their business. When undertaking their risk assessment, the following questions should be considered:

1. Does the business understand how and why criminals may wish to launder illicit funds through the purchase of high value goods?
2. How does the business's:
   i) customer base;
   ii) type and value of goods traded; and
   iii) geographical area, impact its level of risk?
3. Are the business's customers buying for themselves or on behalf of a third party? Does the dealer know who these third parties are?
4. Does the business deal with any overseas sellers or buyers who are not local?
5. Does the business have systems in place to regularly monitor and detect any behavioural patterns or activities of its customers which could possibly be ML/TF schemes (see Schedule 1 below)?
6. Are the business's customer due diligence methods appropriate and sufficient to minimise the risk (see Chapter 6 below)?
7. Have the employees of the business received any training which might mitigate the risk of the business being used to launder illicit funds?

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

For example, an international wholesale operation with overseas clients presents a completely different risk profile to a high street jeweller in Main Street. However, both may be targeted by criminals if they have little or no AML/CFT controls in place. The environment in which business is carried out affects the individual customer's risk assessment. If a business has many high net-worth customers or deals with people from a particular country or region, this will influence the business wide assessment.

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

Dealers in precious metals and stones, diamonds and gold can find more in depth guidance on the risk-based approach to combatting ML/TF from the Financial Action Task Force through links in 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?

HVDs have the responsibility of regularly conducting risk assessment as a means of focusing on risks specific to the business at that time and ensuring that AML/CFT systems and policies in place continue to be effective.

4. AML/CFT Policies & Procedures

4.1 Risk based policies and procedures.

Policies and procedures to protect and prevent HVDs from being used as a tool for ML/TF must be in place.

All HVDs must have a clear written AML/CFT policy based on the degree of risk associated to the specific business (see Chapter 3 above).

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 ML/TF risks.

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 be in place?

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

1. assess the risk of their business being used by criminals for ML/TF (in accordance with Chapter 3 above);
2. carry out customer due diligence (Chapter 6 below) and monitor customers' business activities;
3. submit annual reports to the OFT and reply to audit queries (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 (Chapter 8 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 suspicious activity to the MLRO (see 5.4 below).

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

4.4 What if I have multiple businesses?

AML/CFT policies and procedures should be applicable to all the business in the same group, and should be appropriate to each of the business.

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.

4.5 I have a policy, I now comply right?

It is important that the policy is put into operation. If a HVD has the best policy in the world, but it is not used, then it is of no use

and the HVD 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 HVDs must nominate a money laundering reporting officer or MLRO.

MLROs must be registered with the OFT by completing and submitting an MLRO nomination form. The form is available to download in the 'AML/CFT' section of the OFT'S website: www.oft.gov.gi.

5.2 Who must be appointed MLRO?

A MLRO must be 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 Chapters 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 ML/TF. 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 HVD 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 whether or not these are below the monetary threshold.

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 ML/TF 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 4 above);
2. training staff in preventing ML/TF within the business;
3. keeping records of customer due diligence and risk assessments (see 7.1 below); and
4. ensuring the HVD's workers are not part of a ML/TF scheme.

5.5 How does a MLRO identify ML/TF 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 a person is engaged, 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 ML/TF 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, the transaction may take place.

5.10 Should the suspicious transaction be allowed to go ahead?

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

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

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

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

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

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

5.12 Sanctions

Sanctions are legal restrictions imposed by the United Nations, European Union, United Kingdom or Gibraltar against states, 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 HVDs to have policies, controls and procedures in place to check all of its customers on the international sanctions lists. Furthermore, HVDs 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 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 HVD'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 (**CDD**, 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 proposed cash transaction.

A HVD 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.

HVDs are prohibited from carrying out transactions above the monetary threshold for anonymous customers or customers which have provided aliases or fictitious names.

6.2 Who needs to be checked?

Appropriate CDD must always be completed on the person wishing to purchase goods above the monetary threshold either in one, or multiple, related transactions (see 1.9 above).

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 6.3 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 HVD's customer is entering into a transaction on behalf of another person the HVD 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 HVD's or 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 CDD checks?

CDD needs to be carried out before carrying out a cash transaction above the monetary threshold.

6.5 What happens if I have been unable to collect CDD?

If any person or entity is unable or unwilling to submit the relevant CDD documents requested and the HVD is unable to carry out appropriate due diligence measures it should not proceed with the transaction and, where applicable, it must terminate the business relationship. If the relationship is not terminated this should be recorded.

Furthermore, the HVD must submit a SAR to the GFIU in relation to the customer (see paragraphs 5.8 to 5.10 above).

6.6 How do I carry out CDD?

The level of CDD required will depend on the ML/TF risk posed to the business by the customer and the transaction. The risk must be assessed by considering the identity of the customer, the type of goods being purchased and any other information or concerns the business may have about the customer or transaction.

The identity of Customers should be verified on the basis of original documents, data or information obtained from reliable and independent sources.

CDD however goes beyond simply carrying out identity checks. People which are well known to the business may become involved in illegal activity e.g. if their personal circumstances change or they face some new financial pressure. CDD measures should reduce this risk and the opportunities for staff to be corrupted.

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 ML/TF risks see Schedule 1.

6.7 Low risk customers: An example of simplified CDD.

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.

HVDs must keep copies of due diligence documents (see Chapter 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 ML/TF. MLROs must keep records as to why, in their view, the need for enhanced CDD is appropriate to the risk posed by the business relationship.

Examples 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.

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

6.9 What am I looking for?

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

This information will permit the HVD's MLRO to assess the AML/CFT risk posed and whether to report suspicious activity to the GFIU.

Some examples of suspicious activity specific to HVDs include:

1. A customer appears unwilling to submit any identification documents;
2. A purchaser seems uninterested in the value of the good nor viewing and inspecting the goods before purchase;
3. A purchaser acquires several high value goods within a short period of time which are ordinarily only bought once by other customers;
4. A customer requests information from the business reference its AML/CFT policies; and
5. A purchaser wishes to make the payment through a company without explanation.

For more guidance on ML/TF risks please see Schedule 1.

6.10 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 on paragraph 3 of Schedule 1). These individuals are at a higher risk of being connected to ML/TF due to the position and influence they hold and because they can be susceptible to corruption.

HVDs 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 HVD must:

1. carry out enhanced due diligence (see 6.8 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.

6.11 Risk assessments

HVDs are required to keep a written risk assessment in respect of every transaction

(or a series of linked transactions, see 1.9 above) above the monetary threshold and the action taken in respect of any suspicious activity detected.

The OFT encourages all HVDs to keep a risk assessment file as they must be able to demonstrate to the OFT that the extent of the CDD measures it has applied is appropriate to the client and the transaction in view of the risks of ML/TF that have been identified. Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution or criminal activity.

6.12 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 an SAR! (See paragraphs 5.8 to 5.10)

6.13 Ongoing monitoring

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

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

6.14 Records.

HVDs must keep copies of the documents requested while conducting CDD 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 HVDs must have appropriate systems in place for recording and storing:

1. detailed invoices of every transaction (or set of series of linked cash transactions) above the monetary threshold (see 7.2 below);
2. the written risk assessment of every transaction (or set of related transactions) above the monetary threshold (see 6.11 above);
3. customer due diligence documents and information (see Chapter 6 above);
4. the action taken in respect of any suspicious activity detected; and
5. staff training records (see 8.3 below).

HVDs must keep these records for inspection for five years after the date of the relevant transaction or the date when staff training was delivered.

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

7.2 What type of data must be collected about transactions?

As much data and information as you can about the transactions.

Every transaction should have a detailed invoice specifying:

1. a description of the good(s) sold;
2. the quantity of the goods sold, by unit or otherwise (e.g. weight);
3. the relevant serial number for the goods;
4. the full name of the person purchasing the goods as stated in their passport/ID;
5. the cash paid in exchange for the goods;
6. an identifying reference for the goods to the HVD's stock records; and
7. account files and business correspondence where relevant.

You must also keep 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, HVDs are required to submit annual reports to the OFT providing information and data about transactions carried out by the business during that year which should correspond with the HVD'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 HVD's records at any time. HVDs 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 the amount and type of high value transactions carried out by the HVD and more generally in Gibraltar;
2. identify suspicious trends and ML/TF schemes; and
3. monitor HVDs' 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 HVDs?

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 ML/TF. This data will also help the OFT analyse each HVD on a risk based approach to determine the likelihood of the HVD being targeted by money laundering criminals.

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

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

7.6 When are the Annual Reports due?

To make it easy for HVDs 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 HVD to the Income Tax Office.

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

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

Additionally, employers have a duty to ensure that its employees have sufficient training to help them both recognise and report potential ML/TF. Staff must be made aware and understand the following:

1. what ML/TF is;
2. the laws concerning money laundering and terrorist financing, including POCA, and the requirements in these guidance notes;
3. the ML/TF risks to which the trade sector generally is exposed;
4. the specific ML/TF risk to which the HVD is exposed (see Chapter 3 above);
5. the HVDs AML/CFT policies and procedures including customer due diligence measures (see Chapter 4 above);
6. how to manage transactions on a risk based approach (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.

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.

HVDs 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 HVDs have?

Employees of HVDs must:

1. know who the MLRO is and what the MLRO's role is;
2. be able to detect suspicious activity and report it to the MLRO;
3. be aware of the steps taken by the business to ensure it is not used for ML/TF;
4. 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 HVD to provide adequate training to its employees (see 8.1 above).

9. Potential High Value Dealers

9.1 Who are Potential HVDs?

Potential HVDs are dealers in goods which have not yet received a payment in cash above the monetary threshold but are open to accepting such cash payments.

9.2 Why do Potential HVDs have responsibilities?

Potential HVDs need to be prepared for the moment that they do receive large payments even if this has not yet happened. As soon as the business receives a payment above the monetary threshold it will automatically be a HVD and these guidance notes will be applicable to that business in full.

9.3 What are the responsibilities of Potential HVDs?

Potential HVDs' responsibilities include, but are not limited to:

1. Carrying out a risk assessment of the business's attractiveness and vulnerability to ML/TF (see Chapter 3 above);
2. Establishing appropriate AML/CFT policies and procedures commensurate to the business's ML/TF risks (see Chapter 4 above);
3. Appointing a MLRO who understands the business's ML/TF risks, is acquainted with POCA and who shall be responsible for all AML/CFT matters (see Chapter 5 above); and
4. Training staff to ensure they are aware of the HVD's ML/TF risks and of the business's AML/CFT polices (see Chapter 8 above).

References to HVDs in Chapters 3 to 8 of these Guidance Notes should be read, where relevant, as also applying to Potential HVDs.

9.4 Can a Potential HVD avoid these responsibilities?

Yes. If a dealer is:

1. not a High Risk Dealer (see Chapter 10 below); and
2. has a written policy not to accept cash payments above the monetary threshold; and
3. has notified the OFT of this policy,

it need not comply with these guidance notes at all.

10. High Risk Dealers (HRDs)

10.1 What is a High Risk Dealer (HRD)?

High Risk Dealers are businesses that:

1. are not HVDs because they have not received a payment above the monetary threshold; and
2. are dealers in goods which are considered to have a higher inherent risk and vulnerability to ML/TF (see 10.2 below).

Despite not being HVDs these businesses are required to have AML/CFT measures in place due to the nature of the goods they trade even if they are not accepting cash payments above the monetary threshold.

10.2 Which businesses are HRDs?

The following businesses are considered HRDs:

1. Dealers in precious stones and metals;
2. Car and motorbike dealers;
3. Marine craft dealers; and
4. Antique and arts dealers.

10.3 What are the responsibilities of a HRD?

1. HRDs must Apply the general AML/CFT principles of these guidance notes to all its cash transactions. In particular, HRDs should:
   i) Carry out a risk assessment of the business's attractiveness and vulnerability to ML/TF (see Chapter 3 above);
   ii) Establish appropriate AML/CFT policies and procedures (see Chapter 4 above and 10.4 below);
   iii) Appoint a MLRO who understands the business's ML/TF risks, is acquainted with POCA and who shall be responsible for all AML/CFT matters (see Chapter 5 above);
   iv) Train staff to ensure they are aware of the business's ML/TF risks and the business's AML/CFT polices (see Chapter 8 above).
2. HRDs must provide the OFT with:
   i) a written ML/TF risk assessment for their business; and
   ii) an appropriate AML/CFT policy.
3. HRDs must record every cash transaction above £1,000 for any of the goods listed in 10.2 in a detailed invoice specifying:
   i) a detailed description of the good(s) sold;
   ii) the quantity of the goods sold, by unit or otherwise (e.g. weight);
   iii) the relevant serial number for the goods;
   iv) the full name of the person purchasing the goods as stated in their passport/ID;
   v) the cash paid in exchange for the goods; and
   vi) an identifying reference for the goods to the HRD's stock records.
4. HRDs must regard all transactions in cash for the goods listed in 10.2 by a person, or group of associated persons, as a series of linked cash transactions for determining whether they cumulatively go above the monetary threshold.

10.4 What policies need to be put in place?

The AML/CFT policies implemented by HRDs, including how they carry out their risk assessments on their customers and related transactions, needs to be appropriate and proportionate to mitigate the inherent risks of trading in those goods. HRDs will be required to assess all of their cash transactions and clients more generally than HVDs to determine what policies are appropriate to ensure that their business is not used for ML/TF.

10.5 Reporting suspicious activity.

Where a HRD's MLRO identifies suspicious activity they must report it to the GFIU as specified in 5.8 above.

11. Useful Contacts

11.1 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

aml.oft@gibraltar.gov.gi

www.oft.gov.gi

11.2 Gibraltar Financial Intelligence Unit

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

Suite 832, Europort, Gibraltar

Tel: (+350) 20070211

Fax: (+350) 20070233

gfiu@gcid.gov.gi

www.gfiu.gov.gi

11.3 HM Customs Gibraltar

HM Customs Gibraltar is the supervisory authority for the trade in tobacco in Gibraltar.

Customs House, Waterport, Gibraltar

Tel: (+350) 20078879/20079988

Fax: (+350) 20049278

financial.investigations@hmcustoms.gov.gi

www.hmcustoms.gov.gi

Schedule 1 – How to Identify ML/TF Risks

1. Identifying risk factors

This schedule sets out a number of common factors that a HVD or its employees may take into account when carrying out a ML/TF 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 ML/TF is, or will be, taking place. They will however assist the HVD 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.

If more information is required it should be requested before proceeding with a transaction to ensure that there is no ML/TF risk 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;
4. existing customers where:
   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,

   (see paragraph 5 below).
5. complex business ownership structures with the potential to conceal underlying beneficial owners;
6. politically exposed persons (these will always require enhanced customer due diligence, see 3 below); and/or
7. persons from high-risk jurisdictions (a list of these 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 high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
5. Members of courts of auditors or of the boards of central banks;
6. Ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
7. Members of the administrative, management or supervisory bodies of State-owned enterprises; and

8. Directors, deputy directors and members of the board or equivalent function of an international organisation.

(Note however that middle-ranking or junior officials carrying out a public function referred to in 1 to 9 are not regarded as PEPs).

These individuals, who may be local or international PEPs, are at a higher risk of possible connection to money laundering and terrorist financing due to the position and influence they hold and will require enhanced due diligence. 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 6.10 of the guidance notes.

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. an unwillingness to disclose the source of funds;
4. suspicion about the source of funds disclosed e.g. does not tally with type of individual;
5. multiple purchases of the same high value goods which are normally only bought once by other customers;
6. an unusually big cash or foreign currency transaction for the goods purchased;
7. a willingness to bear very high or uncommercial penalties or charges;
8. no apparent reason for using your business's services, e.g. another business is better placed to handle the transaction;
9. situations where the customer's source of funds are unclear; and/or
10. the unusual involvement of third parties particularly where the customer appears to have a low income.

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. the pattern of an existing customer has changed since the business relationship was established;
4. there has been a significant or unexpected improvement in an existing customer's financial position and the customer can't give a proper explanation of where money came from;
5. peaks of activity at particular locations or properties; and/or
6. unfamiliar or atypical types of customer or transaction.

6. Enhanced due diligence and reporting.

The indicators above may, when assessed by the HVD 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 HVD's MLRO, having considered all the factors surrounding the customer and the transaction, knows or suspects that ML/TF is taking place, they should submit a suspicious activity report (see 5.6 to 5.8 of the guidance notes).

Schedule 2 – Glossary of Abbreviations

AML/CFT	Anti-money laundering and countering the financing of terrorism
Cash	Money in coins or notes.
CDD	Customer due diligence
FATF	Financial Action Task Force
GFIU	Gibraltar Financial Intelligence Unit
HVD	High-value dealer
HRD	High risk dealer
ID	Personal identification document
ML/TF	Money laundering and terrorist financing
MLRO	Money laundering reporting officer
NRA	National Risk Assessment
OFT	Office of Fair Trading
PEP	Politically exposed person
SAR	Suspicious activity report
UBO	Ultimate beneficial owner