GIBRALTAR

Guidance for High-Value Goods Dealers (HVGDs):

- ➢ **Anti-money laundering (AML);**
- ➢ **Combatting the financing of terrorism (CFT); and**
- ➢ **Counter proliferation financing (CPF).**

Contents

Legal Notice
1. About this guidance
2. Applicable legislation
3. HVGD business risk assessments
4. AML/CFT/CPF policies, controls & procedures
5. Money laundering reporting officers & their responsibilities
6. Customer due diligence & assessing risk
7. Ongoing monitoring
8. Targeted financial sanctions
9. Record keeping, data & annual returns
10. Employer & employee responsibilities
11. Reporting ownership & management changes
12. Potential high value goods dealers
13. Art market participants
14. Useful contacts

Schedule 1 - How to identify customer ML/TF/PF Risk
Schedule 2 – Verifying source of funds & wealth
Schedule 3 - Glossary of terms & abbreviations

Issued: June 2017
Updated: March 2025
Version: V 4.3

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

Legal Notice

This guidance should be regarded as regulatory standards for the purposes of the Proceeds of Crime Act 2015.

This document is issued pursuant to S. 11(3) of the Supervisory Bodies (Powers Etc.) Regulations 2017 (**SBPR**).

Compliance with this guidance is enforceable pursuant to the provisions of SBPR.

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

The OFT does not give any express or implied warranty as to the accuracy of the information contained in this document. The OFT does not accept any liability for error or omission.

1. About this guidance

1.1 Why is the OFT issuing this Guidance?

The OFT is the appointed Supervisory Authority under the Proceeds of Crime Act 2015 (**POCA**) for the following businesses:

1. "dealers in all high value goods whenever payment is made or received in cash and in an amount of 10,000 euro or more" – s.9(1)(m) POCA; and
2. "art market participants" – s.9(1)(i) POCA (see 1.2 and section 13).

The OFT is issuing this guidance to these businesses:

1. to assist them in meeting their AML/CFT/CPF legal obligations (see 1.9;
2. to provide guidance about how to identify high risk transactions and customers; and
3. to explain how the OFT will supervise compliance with the business's POCA legal obligations.

For more information about POCA please refer to section 2.

1.2 Who does this guidance apply to?

This guidance applies to the following businesses:

1. <u>High-Value Good Dealers (**HVGDs**)</u>

   Businesses that deal in high value goods (see 1.8) whenever payment is made or received in cash and in an amount of €10,000 or more;

2. <u>Potential HVGDs</u>

   Businesses which are open to accepting cash payments in an amount of €10,000 or more in relation to the sale or purchase of high vale goods, but have yet to receive such payments (see section 13); and

3. <u>Art Market Participants</u>

   Persons who by way of business trade or in act as an intermediary in the sale or purchase of, artistic works and the value of the transaction (or series of linked transactions) is in an amount of €10,000 or more (s. 7(1) POCA) (see section 13).

References in this document to 'HVGDs' should be regarded as applicable jointly to HVGDs, Potential HVGDs and to Art Market Participants as defined in this section unless otherwise indicated.

The guidance notes also apply to directors, managers, partners and employees of the above-mentioned businesses.

1.3 Why does the guidance refer to an amount in euros and not pounds sterling?

The guidance reflects the monetary limit as set out in POCA.

It should be noted however that references in POCA and this guidance to an amount in euros includes reference to an equivalent amount in any currency (s. 1ZC(a) POCA).

The equivalent in sterling (or any other currency) on a particular day of a sum expressed in euros is determined by converting the sum in euros into its equivalent in sterling (or that other currency) using the London closing exchange rate for the euro and the relevant currency for the previous working day (s. 1ZC(b) POCA).

1.4 Does this guidance apply to payments made by card or bank transfers?

No. It only applies to payments made in cash, i.e. money in coins or notes.

Transactions for the purchase of high vale goods carried out with money already in the banking system are not covered by POCA.

1.5 Is this guidance relevant to all cash payments?

No. Only to large cash payments for:

1. high value goods (see 1.8); and
2. which are in an amount of €10,000 or more.

Furthermore, they do not apply to cash payments for tobacco as these are regulated by HM Customs separately (see 1.15).

1.6 Is the €10,000 limit passed if cash is received over a period of time?

Yes. Cash payments will be considered as amounting to €10,000 or more if they are carried out in a single operation or in several operations which appear to be linked (s.11(1)(ba) POCA), including:

1. a series of linked cash payments totalling €10,000 or more from the same customer (including payments on account); and/or
2. cash payments totalling €10,000 or more which appear to have been broken down into smaller amounts to fall below the €10,000 limit, whether or not they have been received from the same person.

1.7 Is it prohibited to accept cash payments of €10,000 or more?

No. It is not prohibited to accept payments in cash in an amount of €10,000 or more.

Before a business accepts such a payment in cash however it must comply with the legal requirements as set out in POCA and proceed according to the risk of ML/TF/PF (see 1.9 to 1.12) that accepting such cash may pose. A business will therefore be required to collect and record information about the buyer of the goods and to risk assess the client and/or the transaction (see section 6). If, having done so, there is knowledge or suspicion of ML/TF/PF (see 1.9) the business must then report it (see 5.6 and 5.7).

1.8 What are high value goods?

There is no definition of "high value goods" in POCA. The OFT however would class a high value good as an item that is expensive, rare, or in high demand due to its quality, scarcity, brand reputation, or importance. These goods often have a higher price per unit. The following goods are examples generally regarded by the OFT as being of a high value:

1. Motor vehicles, including cars and motorcycles;
2. Marine craft, including boats, yachts and jet skis;
3. Gold, silver and other precious metals;
4. Diamonds, sapphires and other precious stones;
5. Jewellery and luxury watches; and
6. Fine art, antiques and other collectibles.
7. Technology such as smartphones, professional cameras, TVs, gaming PCs.

This is not an exhaustive list. Luxury and expensive items are usually however more likely to be considered high value goods.

Furthermore, the OFT will consider any goods with a value of €10,000 or more as a high value good, whether it is sold as an individual item or otherwise (e.g. by weight or volume).

It should be noted that technically any type of goods that are sold in cash for €10,000 or more can be regarded as a high value good, irrespective of the nature of the goods sold.

1.9 What is AML/CFT/CPF?

AML/CFT/CPF refers to laws and systems designed to prevent:

1. money laundering (**ML**) (see 1.10);
2. terrorist financing (**TF**) (see 1.11); and
3. proliferation financing (**PF**) (se 1.12).

AML means anti-money laundering.

CFT means combatting the financing of terrorism.

CPF means counter proliferation financing.

1.10 What is money laundering (ML)?

Money laundering, or ML, is the process of transforming and concealing the profits generated by criminal activity and corruption (such as drug trafficking, market manipulation, fraud, tax evasion and bribery) into a 'clean'/legitimate asset which is in the banking system and where the illicit source of the money cannot be traced.

The buying and selling of high value goods in cash is recognised as a major avenue for money laundering activity which is exploited by organised crime and corrupt officials.

Whereas high value goods purchased by bank transfer or payment card can be easily tracked by law enforcement agencies, transactions that involve large sums of cash are difficult to track. This makes payments in cash very attractive to criminals seeking to launder illicit funds.

1.11 What is terrorist financing (TF)

Terrorist financing, or TF, is defined in s. 1ZA of POCA. It involves:

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

for the purposes of terrorism.

For more information and guidance regarding TF please refer to the Counter Terrorist Financing Guidance Notes on the GFIU's website: www.gfiu.gov.gi.

1.12 What is proliferation financing (PF)?

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

HVGDs should understand PF and their obligations in relation to PF as set out in local and international legislation.

For more information and guidance regarding PF please refer to the Counter-Proliferation Financing Guidance Notes on the GFIU's website: www.gfiu.gov.gi.

1.13 National Risk Assessment

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

The NRA must be considered by HVGDs when risk assessing their business (see section 3) and when carrying out customer due diligence measures (see section 6).

1.14 Do payments in cash in an amount of €10,000 or more need to be reported?

No. Only those payments that the business knows or suspects are being, made in connection with ML/TF/PF need to be reported (see 5.6 and 5.7 below). For these purposes it does not matter whether payments received are in an amount of €10,000 or more.

It is the business's legal obligation however to risk assess its customers and transactions to determine if payments may be made in connection with ML/TF/PF by applying customer due diligence measures (see section 6).

The business should note the instances where payments will be considered to be above the €10,000 limit in 1.6.

1.15 Does this guidance apply to the sale of tobacco?

No. The supervisory authority for the trade in tobacco is HM Customs (see 14.2).

1.16 What are the obligations of HVGDs?

HVGDs' responsibilities include, but are not limited to:

1. Carrying out a risk assessment of their business's attractiveness and vulnerability to ML/TF/PF (see section 3);

2. Establishing appropriate policies and procedures commensurate to the business's risks to prevent the business being used to launder money or finance terrorism (see section 4);

3. Appointing a money laundering reporting officer (**MLRO**) who understands the business's risks and responsibilities, its AML/CFT/CPF policies and who shall be responsible for all AML/CFT/CPF matters (see section 5);

4. Carrying out risk assessments of its customers and transactions on a risk-based approach and keeping relevant documentation (see section 6); and

5. Keeping appropriate AML/CFT/CPF records and submitting annual returns to the OFT (see section 8); and

6. Training staff to ensure they are aware of ML/TF/PF risks and of the business's AML/CFT/CPF polices (see section 10).

For specific obligations of Potential HVGDs and Art Market Participants see sections 11 and 12.

1.17 What is the OFT's role?

As a Supervisory Authority for HVGDS as set out in Schedule 2(g), POCA, the OFT must effectively monitor HVGDs and take necessary measures to:

1. secure compliance by HVGDs with their legal obligations in POCA;
2. prevent HVGDs from engaging or otherwise being concerned in (directly or indirectly) ML/TF/PF, or otherwise knowingly or recklessly assisting or facilitating such conduct by any other person;
3. identify and assess the ML/TF/PF risk for the HVGD sector as set out in the NRA.

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

1.18 How does the OFT monitor compliance by HVGDs?

The OFT risk assesses all HVGDs' compliance with their AML/CFT/CPF obligations based on:

1. documents submitted annually to the OFT, including:
    i. risk assessments (see section 3);
    ii. policies controls & procedures (see section 4); and
    iii. annual returns submitted (see section 9);
2. regular onsite visits carried out by the OFT on all HVGDs in order to ensure that they are meeting their AML/CFT/CPF obligations in practise; and
3. thematic reviews of the HVGD sector to determine the level of compliance in relation to their obligations.

The OFT also works closely with the Gibraltar Financial Intelligence Unit, law enforcement bodies and other AML/CFT/CPF supervisory authorities to monitor the market and uses various sources to acquire information and determine whether HVGDs are complying with their AML/CFT/CPF obligations or are being used for ML/TF/PF.

1.19 Does this guidance contain all I need to know?

No. This guidance is for information purposes only to assist HVGDs, Potential HVGDs and Art Market Participants to understand their legal obligations.

For the definitive authority on these business's legal obligations regarding AML/CFT/CPF please refer to the Proceeds of Crime Act 2015 and other applicable legislation (see section 2).

1.20 Can I avoid the obligations in the Act and this guidance notes?

Yes. Dealers in high value goods do not need to comply with most of Part III of POCA nor this guidance if they:

1. do not accept cash payments in an amount of €10,000 or more;
2. have a written policy not to accept cash payments in an amount of €10,000 or more; and
3. such policy is communicated in writing to the OFT.

The OFT may conduct enquiries to determine whether any such cash policy is being implemented. Any changes to cash policies must be communicated to the OFT.

2. Applicable legislation

2.1 Proceeds of Crime Act 2015 (POCA)

The Proceeds of Crime Act 2015, or POCA, is the main Gibraltar law that is aimed at preventing the abuse of the financial system for ML/TF/PF. It also sets out processes relating to the confiscation, investigation and recovery of the proceeds of unlawful conduct.

While all of POCA is applicable, the most relevant part for HVGDs is Part III: 'Measures to prevent the use of the financial system for purposes of money laundering, terrorist financing and proliferation financing'.

The majority of HVGD's AML/CFT/CPF obligations and the requirements set out in this guidance is derived from POCA.

2.2 Terrorism Act 2018

The Terrorism Act provides for the investigation of terrorist offences and sets out offences related to terrorism, in particular those relating to the financing of terrorism and in respect of Proscribed Organisations. Persons who have obligations under the Act will need to become aware of and provide training and processes for staff to follow.

The Act also creates offence relating to acts of terrorism, travelling in respect of terrorism and provides for the freezing and forfeiture of terrorist property and funds,

The National Coordinator for AML/CFT has issued a newsletter with more information about the Terrorism Act 2018 which can be found in the 'AML/CFT/CPF' page of the OFT's Website (www.oft.gov.gi).

2.3 Sanctions Act 2019

The Sanctions Act 2019 provides for the automatic recognition and enforcement in Gibraltar of UN, EU and UK sanctions and gives effect to numerous international requirements relating to financial and other sanctions. The Act provides a regime to implement both international and domestic sanctions in Gibraltar. These sanctions include financial sanctions, immigration sanctions, trade sanctions, aircraft sanctions and shipping sanctions.

The National Coordinator for AML/CFT has issued a newsletter with more information about the Sanctions Act 2019 which can be found in the 'AML/CFT/CPF' page of the OFT's Website (www.oft.gov.gi).

2.4 The Fair Trading Act 2023

Under the **Fair Trading Act 2023** HVGDs and potential HVGDs in Gibraltar are subject to several provisions that impact their operations, including obligations related to anti-money laundering (AML). Section 30 of the Act specifically addresses the principles for considering licensing applications, including measures to prevent money laundering and the financing of terrorism.

Licensing and Compliance: HVGDs and potential HVGDs must obtain a business licence from the Office of Fair Trading (OFT). As part of the application process, the OFT evaluates whether the business complies with AML requirements.

AML Measures: HVGDs and potential HVGDs must implement and maintain systems to identify, prevent, and report suspicious transactions. This aligns with Gibraltar's broader obligations under AML regulations.

Renewals and Revocations: Licences may be refused, revoked, or subject to additional conditions if HVGDs and potential HVGDs are found to be non-compliant with AML obligations. The OFT actively monitors license holders to ensure ongoing.

Investigations and Sanctions: The OFT has investigatory powers to examine AML compliance as part of its broader mandate to protect consumers and ensure fair trading practices. Non-compliance can lead to penalties or legal actions.

2.5 Register of Ultimate Beneficial Owners, Nominators and Appointors Regulations 2017

The Register of Ultimate Beneficial Owners, Nominators and Appointors Regulations 2017, commonly referred to as 'RUBOR', is a subsidiary legislation made under s. 184 of POCA that establishes a Register of Ultimate Beneficial Owners within Gibraltar. The Finance Centre Director is the appointed Registrar.

2.6 If I read this guidance, do I need read the legislation?

Yes! This guidance only set out some of the most relevant provisions of POCA and other legislation to the HVGD sector. These focus on ML/TF/PF only. There are however other obligations in the legislation that may not be referred to in this document.

You should not therefore regard this document as an exhaustive authority with regard to HVGDs' obligations in respect of AML/CFT/CPF and should instead read it in conjunction with your legal obligations as set out in the legislation.

2.7 Where can I find the legislation?

The full body of the Acts may be found in the 'AML/CFT/CPF' page of the OFT's Website (www.oft.gov.gi) along with a pdf copy of this guidance.

They can also be downloaded on the HM Government of Gibraltar's Gibraltar laws website (www.gibraltarlaws.gov.gi) by searching the name of the laws.

3. HVGD Business Risk Assessments

3.1 What is a business risk assessment?

S.25A POCA sets out the requirement for HVGDs to risk assess their business. A risk assessment is the process of assessing the ML/TF/PF risk that your business could be exposed to. Once the risks are understood appropriate policies, controls and procedures can be put in place to mitigate these risks (see section 4).

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

HVGDs must subjectively assess the relevant ML/TF/PF 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 carry out

ML/TF/PF 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 ML/TF/PF risk?
3. Are the business's customers buying for themselves or on behalf of a third party? Does the business know who these third parties are?
4. Does the business deal with any 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 that could possibly be ML/TF/PF schemes (see Schedule 1)?
6. Are the business's customer due diligence methods appropriate and sufficient to minimise the risk? (see section 6).
7. Have the employees of the business received any training that might mitigate the risk of the business being used for ML/TF/PF? (see section 10).

This list is not exhaustive and a risk based approach will require analysing the business's individual characteristics carefully. These need to be considered alongside the risks identified in the National Risk Assessment (see 1.13).

For example, an international wholesale operation with overseas customers presents a very different risk profile to a high street jeweller who mostly sells to locals in Main Street. However, both may be targeted by criminals if they have little or no AML/CFT/CPF controls in place. The environment in which a business is carried out affects the individual businesses' 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 Determining the business's risk appetite.

Once a thorough risk assessment is carried out the business can determine its risk appetite. This allows it to implement policies to cover the customers and transactions which pose an acceptable risk (see 4.4).

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

For detailed and specific guidance for risk assessing your business please refer to the OFT's Risk Assessment Guidance Notes which can be found in the 'AML/CFT/CPF' section of the OFT's website: www.oft.gov.gi.

Dealers in precious metals and stones, diamonds and gold can find more in depth guidance on the risk-based approach and combatting ML/TF/PF from the FATF through links in the 'AML/CFT/CPF' section of the OFT's website: www.oft.gov.gi.

Art Market Participants can find more in depth guidance on the risk-based approach and combatting ML/TF/PF from the FATF through links in the 'AML/CFT/CPF' section of the OFT's website: www.oft.gov.gi.

3.5 Ongoing obligations.

HVGDs have the responsibility of conducting risk assessment regularly on an ongoing basis. This ensures that businesses are aware of evolving ML/TF/PF risks specific to the business and that AML/CFT/CPF policies, controls and procedures continue to be fit for purpose and effective.

4. AML/CFT/CPF Policies, Controls & Procedures

4.1 Risk based policies, controls and procedures.

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

The policy shall be proportionate to the nature and size of the HVGD.

All HVGDs must have a clear written AML/CFT/CPF policies with well-defined controls and procedures to identify and manage the business's and its customers' ML/TF/PF risks. These risks must be determined after carrying out a risk assessment of the business (see section 3).

Policies, controls and procedures must be made available to all employees of the business and to the OFT.

4.2 Who approves the policy?

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

4.3 What policies, controls and procedures must be in place?

HVGDs must develop internal policies, controls and procedures that allows it to:

1. mitigate identified risks of the business being used by criminals for ML/TF/PF (see section 3);
2. carry out customer due diligence measures (see section 6) and monitor customers' business activities;
3. carry out ongoing CDD measures (see section 7);
4. carry out targeted financial sanctions screening (see section 8);
5. submit annual returns to the OFT (see section 9);
6. report suspicious clients or transactions to the GFIU where it suspects, or has reasonable grounds to suspect, that a transaction is related to ML/TF/PF (see 5.8);
7. keep customer, transactional and staff training records (see sections 9 and 10);
8. ensure employees:
    i. are aware of POCA and this guidance;
    ii. are aware of the business's AML/CFT/CPF policy;
    iii. have the necessary training; and
    iv. report suspicious activity to the MLRO (see 10.4).

A complete list of the legal requirements are set out in s.26 POCA and in the Sanctions Act 2019.

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

4.4 Determining the business's risk appetite.

Once a thorough risk assessment is carried out this can be used to assist the business to determine its commercial appetite to enter into transactions that are higher risk. This will allow it to implement policies to determine what customers or transactions it wants to engage with.

Where implemented, such a policy will facilitate the business to meet its AML/CFT/CPF obligations as the policy can clearly determine:

1. the type of customer due diligence required for different customers and transactions (see section 6); and
2. when the business considers that the ML/TF/PF risks are too high for it.

Such a policy will also make it easier for the business to demonstrate to the OFT and law enforcement how it has met it AML/CFT/CPF obligations.

4.5 What if I have multiple businesses?

Pursuant to s.26(1B) POCA, AML/CFT/CPF policies, controls 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/CPF policies, controls and procedures should allow for sharing information required for the purposes of CDD and the assessment and management of ML/TF/PF 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/CPF purposes. Adequate safeguards on the confidentiality and use of information exchanged should be in place.

Refer to the full set of requirements in s.26(1B) POCA.

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

4.6 Do I comply fully once I have policies, controls and procedures in place?

It is important that the policies, controls and procedures are put into operation. If a HVGD does not implement its policies, controls and procedures, then these are of no use and the HVGD will not be meeting its AML/CFT/CPF obligations.

Inappropriate policies, controls and procedures will similarly mean that the business shall not meet its AML/CFT/CPF obligations.

Policies, controls and procedures must therefore be based on the findings of the business's risk assessment (see section 3) and be appropriately implemented. This includes making them readily available to all employees who should be trained about how to use them (see section 10). A copy of the policies, controls and procedures must also be provided to the OFT.

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

4.7 Undertaking an audit

Audits must have regard to the nature and size of the HVGD (s. 26(1A) POCA) and should happen at regular intervals or where a deficiency with the business's AML/CFT/CPF policy, controls or procedures is identified.

The frequency and scale of the audit shall be proportionate to the size and nature of the business as well as findings and recommendations from the OFT or previous audits and any other relevant AML/CFT/CPF considerations.

4.8 Who can carry out an audit?

Audits must be independent. The person must provide an independent, objective and impartial view on the efficacy of the policies, controls and procedures. It is the responsibility of the business to determine the independence of the individuals.

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

There is no requirement however to engage the services of a third party in order to carry out this function. An audit can be performed by a person from within the business if they meet the independence criteria. The HVGD must however ensure that whoever carries out the internal audit they must not:

1. have been involved in carrying out the HVGD's risk assessment;
2. have been involved in the development of the HVGD's AML/CFT/CPF policies, controls and procedures; and/or
3. be involved in applying the HVGD's AML/CFT/CPF policies, controls and procedures.

4.9 Do I need policies, controls and procedures if I work alone?

Yes. You must implement policies, controls and procedures. If you are working alone however your policies, controls and procedures need not be in writing until you are working with someone else.

The OFT nevertheless strongly recommends that written policies, controls and procedures are created even if you work alone as this will help you meet your AML/CFT/CPF and targeted financial sanctions obligations (see section 8).

A written policy will also help you to demonstrate to the OFT how you are meeting your obligations in onsite meetings or otherwise. If a policy is not in writing you must be able to explain to the OFT upon request:

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

5. MLROs & their responsibilities

5.1 What is an MLRO?

All HVGDs must nominate a money laundering reporting officer (**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/CPF' section of the OFT'S website: www.oft.gov.gi.

5.2 Who should 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
4. has appropriate training and experience regarding AML/CFT/CPF to carry out the role; and
5. 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 also generally responsible for dealing with any AML/CFT/CPF matters and is the OFT's liaison for the business.

The MLRO's main responsibility is to monitor any suspicious activity surrounding the business daily transactions that might be linked to ML/TF/PF. Where necessary the MLRO must report such activities or risks to the GFIU by submitting a Suspicious Activity Report (**SAR**) (see 5.4 to 5.7 below).

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

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/CPF polices, controls and procedures (see section 4);
2. training staff about the business's ML/TF/PF risks and how to prevent ML/TF/PF within the business;
3. keeping customer due diligence and risk assessments records (see 7.1); and
4. ensuring the HVGD's workers are not part of a ML/TF/PF scheme.

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

OFT
GIBRALTAR

5.4 Identifying suspicious activity and submitting SARs.

HVGDs must have systems in place for the MLRO to receive reports of suspicious activity from the business's other staff. The MLRO must then evaluate the reports for any evidence of ML/TF/PF and carry out an appropriate risk assessment based on the report and the customer's due diligence records (sees section 6).

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 (see 5.6), suspects or has reasonable grounds to suspect (see 5.7) that a transaction is related to ML/TF/PF it is required to submit a SAR at the earliest possible opportunity to the GFIU. This includes attempted transactions whether or not these are below an amount of €10,000.

5.5 How does the MLRO report a SAR to the GFIU?

It is strongly recommended that MLROs sign up to the GFIU's Themis online system to submit SARs. For more information and to sign up to the system visit https://www.gfiu.gov.gi/reporting. This will allow MLROs to submit SARs and to report positive sanctions matches (see section 8).

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

For more specific guidance about submitting SARs please refer to the GFIU's website: www.gfiu.gov.gi

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 (see section 6) and by asking questions.

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

5.8 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.

5.9 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 related to ML/TF/PF.

5.10 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 (s.5 POCA). 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 ML/TF/PF, and they reasonably believe that applying CDD measures (see section 6) will 'tip-off' the customer, then the MLRO should not apply such measures and instead submit a SAR (see 5.11).

5.11 Tipping off through CDD measures

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

5.12 Targeted financial sanctions

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

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

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

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 HVGD's ability to monitor risk and submit SARs to the GFIU.

5.14 Is there more guidance for MLROs?

The GFIU has produced guidance notes on SARs for MLROs & Reporters and guidance notes on Financial Sanctions. For more information visit the GFIU's website: https://www.gfiu.gov.gi/reporting.

6. Customer Due Diligence & Assessing Risk

6.1 What is customer due diligence?

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

Applying CDD measures involves:

1. identifying the customer and establishing who they are;
2. understanding the ownership and control structure of the customer, including identifying the customers' beneficial owners (see 6.4);
3. understanding and obtaining information about corporate or legal entities, trusts, foundations and other legal arrangements in the ownership and control structures of customers;
4. verifying that any person purporting to act on behalf of the customer is so authorised and identifying and verifying the identity of that person (s.10A POCA);
5. understanding and obtaining information on the purpose and intended nature of the business relationship or occasional transaction;
6. taking a risk-based approach to the verification of the identity of the customer and all beneficial owners (see 6.5)
7. determining whether the customer, or its beneficial owner, is a politically exposed person (see 6.15); and
8. taking a risk-based approach to the verification of the source of funds and the source of wealth of the customer and beneficial owners (see 6.16);

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

It should be noted that adequate CDD measures cannot be applied by following a checklist approach. This is because CDD must be carried out on a risk-based approach and different risks associated with different goods, customers and transactions will require different CDD to provide a HVGD comfort that there is no ML/TF/PF.

6.2 When are CDD measures carried out?

The application of CDD measures is covered in s.11 POCA. CDD must be performed before any financial transactions take place.

Pursuant to s.11(1) and s.13(2) POCA, HVGDs must apply CDD measures and verify the identity of the customer (and any beneficial owner (see 6.4)) before:

1. it sells high value goods, or any other goods (POCA s. 11(1)(ba)), in cash in an amount of 10,000 euro or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked (see 1.6);
2. it establishes a business, professional or commercial relationship with a customer which is expected, at the time when

contact is established, to have an element of duration (s.8(1) and s.11(1)(a) POCA); and/or
3. it suspects ML/TF/PF, regardless of any derogation, exemption or threshold (s.11(1)(c) POCA);
4. doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification (s.11(1)(d) POCA); and/or
5. any of the other circumstances set out in s.11(1) POCA.

HVGDs must also apply CDD measures where it suspects ML/TF/PF in any circumstances, regardless of whether the payment for goods is in cash and/or surpasses the €10,000 limit.

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

6.3 What are my CDD obligations?

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

Pursuant to s.11(3) and (5) POCA, a HVGD must determine the extent of CDD measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. In doing so HVGDs must, as a minimum, take into account the following list of risk variables:

1. the purpose of the relationship or transaction;
2. the size of the transactions undertaken; and
3. the regularity or duration of the business relationship.

The HVGD must also be able to demonstrate to the OFT that the CDD measures applied is appropriate in view of the identified ML/TF/PF risks.

Pursuant to s.11(3)(b) POCA, HVGDs must be able to demonstrate to the OFT that the extent of CDD measures applied to a customer, business relationship (see 7.2), product or transaction is appropriate in view of the risks of ML/TF/PF that have been identified.

6.4 Who needs to be checked?

Appropriate CDD must always be completed on customers wishing to purchase high value goods in an amount of 10,000 euro or more either in one, or multiple, related cash transactions (see 1.6).

The identity of the Customer must be known and their identity must be verified on the basis of documents, data or information obtained from a reliable and independent source (s.10(1)(e) POCA).

Similarly, the identity of any beneficial owner must be known and verified (see 6.6).

HVGDs must apply ongoing CDD measures to business relationships (see section 7).

6.5 Who does not need to be checked?

No CDD is required on customers wishing to purchase high value goods in an amount of 10,000 euro or more where:

1. they pay for those goods by card or by bank transfer; and
2. they pay in part in cash and that cash is not above 10,000 euro.

OFT GIBRALTAR

6.6 What is a beneficial owner (BO)?

The definition of 'beneficial owner' is set out in s.7(1A) POCA. Identifying all BOs is a specific requirement in s.10(b) POCA.

A BO is an individual (it must be a 'natural person' as opposed to a corporation) who will ultimately benefit from a transaction or business relationship.

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

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

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

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

Broadly speaking where an individual either:

1. owns 25% plus one share of a company or has control of over 25% of a company (s. 7(1B) POCA) that is the HVGD's customer; or
2. is a settlor, trustee, protector or beneficiary of a trust (or similar) (s.7(1A) POCA),

that individual will be a BO.

In a transaction there may be multiple BOs. All must be identified and appropriate CDD completed on a risk-based approach.

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

6.7 The Register of Ultimate Beneficial Ownership

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

Pursuant to Regulation 26A(1) of the Register of Ultimate Beneficial Owners, Nominators and Appointors Regulations 2017, where it becomes apparent to a HVGD that the information obtained from the Register is materially inconsistent with other information in its possession, the HVGD must report this to the Finance Centre Director within 30 days of their discovery.

6.8 What happens if I have difficulties or am unable to collect CDD?

In relation to companies, you must exhaust all possible means to determine who its BO is (s.7(1A) POCA). This will involve making appropriate and proactive enquiries. 'All possible means' is a high threshold and you must be able to demonstrate the efforts made to identify BOs to the OFT. The OFT must be satisfied that these have been sufficient in the circumstances.

However, if after having exhausting all possible means:

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

then the BO shall be the individual exercising control over the company via other means (s.7(1A)(c)(ii) POCA).

If, after having exhausted all possible means, there is still doubt about who the individual exercising control is, then the BO shall be the individual who holds the senior management position in the customer (s.7(1A)(c)(ii) & (iv) POCA).

More generally, pursuant to s. 15(1) POCA, if any person or entity is unable or unwilling to submit the relevant CDD documents requested and the HVGD is unable to carry out appropriate CDD 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 HVGD must submit a SAR to the GFIU in relation to the customer (see 5.8 to 5.10).

HVGDs should keep a record of any difficulties encountered during the CDD process (s.10(l) POCA).

HVGDs are prohibited from carrying out transactions in an amount of 10,000 euro or more for anonymous customers or customers which have provided aliases or fictitious names.

6.9 Applying CDD measures.

CDD measures allow a HVGD to assess a customer's AML/CFT/CPF risk and whether a transaction may proceed without a real risk of the HVGD being involved in a transaction linked to ML/TF/PF.

The level of CDD required is determined on a risk-based approach (s.10, POCA) and will depend on the ML/TF/PF 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.

While verifying the identity of customers is one of its primary goals, CDD 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 also reduce this risk and the opportunities for staff to be corrupted and complicit in ML/TF/PF.

HVGDs are also required to understand the nature of their customer's business and its ownership and control structure.6.10 Applying a risk-based approach

HVGDs must determine the extent of CDD measures taking a risk-based approach to the verification of the identity of:

1. customers (s.10(e) POCA);
2. all beneficial owners (s.10(e) POCA) (see 6.6); and
3. the source of funds and wealth of the customer and beneficial owners (s.10(f) POCA) (see 6.16).

Therefore, the level of CDD measures applied to a particular transaction must reflect the ML/TF/PF risk faced by that type of customer, business relationship and transaction.

Prior to the inception of a business relationship or occasional transaction, a regulated entity must assess the ML, TF and PF related risks posed by each customer. This assessment must take into account customer, country, product and interface risk factors. Together, all four risk elements outlined above must be considered in unison in order to produce an overall risk profile. It is the result of this risk profile that will then determine the level and intensity of the identification, verification and monitoring measures applicable to that business relationship. The risk assessment undertaken for each customer must be refreshed periodically throughout the business relationship to ensure that it remains an appropriate and relevant reflection of the ML, TF & PF risks posed by the business relationship.

A low perceived ML/TF/PF risk assessment by the business will allow it to conduct simplified CDD (se6.11).

A high perceived ML/TF/PF risk assessment shall on the other hand require the business to implement enhanced CDD measures (see 6.12).

Medium perceived ML/TF/PF risks shall require elements of both simplified and enhanced CDD, depending on the risk identified.

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

The OFT strongly recommends that HVGDs introduce an appropriate methodology to effectively and consistently determine what CDD measures need to be applied to customers or transactions based on their ML/TF/PF risk. The OFT has created sample CDD forms that can be downloaded from the 'AML/CFT/CPF section of the OFT's website: www.oft.gov.gi

6.11 Low risk customers: Simplified CDD measures.

Pursuant to s.16 POCA, where a HVGD, having applied CDD measures:

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

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

Simplified CDD can include, but may not be limited to, collecting the following basic information verified on the basis of documents, data or information obtained from a reliable and independent source (s.10(1)(e) POCA):

1. Customers and beneficial owners:
   i. full Name;
   ii. date of birth;
   iii. residential address;
   iv. a copy of the customer's original Passport/ID (or any other Government-issued photographic document); and
   v. the customer's source of wealth (e.g. employment) (see 6.16) and supporting documentation;
2. Companies and other legal entities (s.10(g) POCA):
   i. its name, legal form and proof of existence;
   ii. the powers that regulate and bind the corporate or legal entity;
   iii. the names of the relevant persons having a senior management position in the corporate or legal entity;
   iv. the address of its registered office and, if different, its principal place of business.

For Gibraltar companies an up to date company profile issued by Companies House and an independently verified copy of the company's Memorandum and Articles of Association would be sufficient. If a company profile is not available, the following independently verified corporate documents would assist:

i. Certificate of incorporation;

ii. Register of Members; and

iii. Register of Directors; and

A declaration would be required in relation to the principal place of business of the company if it was different to the address of the registered office;

3. Trusts(s.10(h) POCA):

   i. its name, legal form and proof of existence;

   ii. the powers that regulate and bind the trust;

   iii. the principal place of business of the trustees.

   An independently verified copy of the trust deed (or other similar legal document) establishing and setting out the nature of that arrangement and a declaration regarding the principal place of business of the trustees should be considered;

4. for legal entities such as foundations, and legal arrangements similar to trusts refer to s.10(i) POCA.

HVGDs must keep copies of CDD documents (see section 7).

6.12 High risk customers: Enhanced CDD measures.

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

1. customers or transactions identified as being high risk (see Schedule 1, paragraph 3);
2. natural persons or legal entities established in third countries identified by Gibraltar as high risk third countries (s.17(1)(b) and s. 17(6) POCA); and
3. in other circumstances as set out in s.17(1) POCA.

The OFT would expect to see enhanced CDD when dealing with politically exposed person, or their family members and close associates (s.17(1)(a), s.20 and s.20B POCA) (see 6.15). Pursuant to s.20(1)(c), it is a requirement to carry out enhanced ongoing monitoring of a relationship with a politically exposed person (see 7.4).

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

When dealing with high risk customers it is important to perform enhanced CDD as a result of the increased risk of ML/TF/PF. 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 CDD for customers and beneficial owners include obtaining:

1. two copies of the customer's Passport/ID which is certified as true copy of the original by a third party professional;
2. two independently verified documents, which is no more than 3 months old, demonstrating proof of the customer's address provided in a document such as a utility bill or bank statement . For utility

bills these should demonstrate that there is sufficient usage of the utilities to demonstrate occupation;

3. Additional information on:
   i. the customer's and on the beneficial owners' business and background;
   ii. the intended nature of the business relationship;
   iii. the reasons for the transactions.
4. Documentation establishing the provenance of the customer's and the beneficial owners' source of wealth and source of funds commensurate to their background and the transaction (see 6.16); and

It is recommended that HVGDs should obtain the approval of senior management for establishing or continuing a business relationship with a customer requiring enhanced CDD. This is a requirement in relation to politically exposed person (s.20(1)(a) POCA).

HVGDs must keep copies of CDD documents (see section 7).

6.13 What am I looking for?

HVGDs have to consider all CDD documentation, along with all other surrounding factors and information about the customer and the type of transaction, to determine if there is a risk of ML/TF/PF. This information will permit the HVGD's MLRO to assess the ML/TF/PF risk posed and determine whether the transaction falls within the risk appetite of the business (see 4.4) and whether to report suspicious activity to the GFIU. Essentially the MLRO must be satisfied that there is no risk of ML/TF/PF through the transaction before proceeding.

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

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

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

6.14 Non face-to-face transactions

Pursuant to s.18 POCA, where the customer has not been physically present for identification purposes, HVGDs must take specific and adequate measures to compensate for the higher risk. This may for instance include:

1. ensuring that the customer's identity is established by additional documents, data or information;
2. applying measures to verify or certify the documents provided, e.g. requiring a third party professional with AML/CFT/CPF expertise to certify them e.g. a lawyer.

Where this is not possible HVGDs should not accept cash and instead only accept a card payment or bank transfer.

6.15 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

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

Pursuant to s.26(2)(c) POCA, a HVGD must have policies, controls and procedures in place to determine whether a customer or the BO of a customer is:

1. a PEP;
2. a PEP's 'family member'; or
3. 'a person known to be their close associate',

(as defined in s.20A POCA).

Given Gibraltar's small size and the close nature of its community, there is a high likelihood that a HVGD's potential customer is a PEP, a PEP's family member, a PEP's close associate. These circumstances however may therefore make it easier for such persons to be identified.

Pursuant to s.20(3) POCA, for the purpose of deciding whether a person is a known close associate of a PEP a HVGD eed only have regard to information which is in its possession or is publicly known.

Pursuant to s.20(1) POCA, before entering into a transaction with a PEP, a PEP's family member, a PEP's close associate or a customer whose BO is a PEP, a PEP's family member, a PEP's close associate the HVGD must:

1. have approval from senior management;
2. take adequate measures to establish the source of wealth and source of funds which are involved in the existing or proposed transaction.

The OFT would expect to see enhanced CDD before entering into a transaction with PEPS, their family members and close associates (s.17(1)(a), s.20 and s.20B POCA) (see 6.12).

Pursuant to s.20(1)(c), it is a requirement to carry out enhanced ongoing monitoring of a relationship with a PEPs (see 7.4)

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

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

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

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

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

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

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

CDD e.g. scrutinising customer bank statements to support the information provided.

For more guidance on verifying source of funds and source of wealth please refer to Schedule 2.

6.17 Risk assessments

HVGDs are required to keep a written risk assessment in respect of every transaction (or a series of linked transactions, see 1.9 above) in an amount of 10,000 euro or more and the action taken in respect of any suspicious activity detected.

The OFT strongly recommends that all HVGDs 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/PF 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.

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

If a HVGD is satisfied that a third party falls within the criteria of s.23 POCA and has already carried out appropriate CDD measures on its customers, they may rely on that CDD as long as:

1. the third party consents to being relied on (s23(1)(b) POCA);
2. the HVGD is satisfied that the CDD measures are appropriate to the customer's level of risk as assessed by the HVGD;
3. the HVGD is satisfied that the CDD measures are current and up to date; and

Copies of the CDD documentation should be provided by the third party to the HVGD for its records. Pursuant to s25(5) POCA, if requested to by the HVGD, the third party has an obligation to make available any information about the customer and any beneficial owner (including any identification and verification data and other relevant documents).

The HVGD must carry out its own risk assessment on the customer, any beneficial owner and the transaction based on the CDD documentation received prior to the HVGD selling high value goods to the customer. A HVGD should not rely on the third parties' risk assessments!

In accordance with s.23(1)(b) and s.23(4), the responsibility to carry out CDD measures, to risk assess and to keep records on its customers shall always ultimately remain with the HVGD.

6.19 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) or is suspicious (see 5.7) that ML/TF/PF is or may be taking place.

(If in doubt, see section 5.5)

6.20 Tipping-off

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

Tipping-off is an offence and MLROs and employees should take care not to disclose prohibited information. The OFT strongly recommends that MLROs become acquainted with tipping-off obligations.

6.21 Ongoing monitoring

Where HVGDs have ongoing business relations with its customers they are required to carry out ongoing monitoring of these existing business relationships (see section 7).

6.22 Records.

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

7. Ongoing Monitoring

7.1 Ongoing monitoring

HVGDs are required to carry out ongoing monitoring and due diligence of existing business relationships. This requirement is set out in s.11(2) and s.12 POCA.

7.2 What are business relationships?

Business Relationships are defined in s.8 POCA. It means a business, professional or commercial relationship which is connected with the professional activities of a HVGD and which is expected, at the time when contact is established, to have an element of duration.

Ongoing monitoring does not apply to occasional, one-off transactions. It may however apply to customers who have been sold high value goods in an amount of 10,000 euro or more in cash on more than one occasion or have been sold high value goods below 10,000 euro in cash more than once or on an ongoing basis so that together the purchases are above an amount of 10,000 euro.

7.3 What does ongoing monitoring involve?

Pursuant to s.12(2) POCA, ongoing monitoring means:

1. scrutinising transactions undertaken throughout the course of the relationship to ensure that they are consistent with the HVGD's knowledge of the customer, their business, their risk profile and their source of funds; and
2. undertaking reviews of existing records (and updating these where necessary) to ensure that the documents, data or information obtained for the purpose of applying CDD measures (see section 6) is kept up-to-date and relevant.

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

It should be noted that pursuant to s.20(1)(c) POCA, it is a requirement to carry out enhanced ongoing monitoring of a relationship with politically exposed persons (see 7.4).

7.4 When do I need to do this?

Ongoing monitoring must be carried out at regular intervals on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction (s.12(3) and 11(3)(a) POCA), As with CDD, HVGDs must therefore adapt their ongoing monitoring measures using a risk-based approach (see 6.10 to 6.12).

As an indicator the OFT would expect that:

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

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

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

HVGDs must also carry out targeted financial sanction screening on existing customers as and when the sanctions lists are updated (see section 8). HVGDs must therefore have systems to be notified when this happens (see 8.5).

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

7.5 When do the relevant circumstances of a customer change?

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

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

HVGDs should not just take into consideration the risk profile of the existing customer but also the impact that that customer's business may have on the HVGD as a whole. For example, a customer may be considered low risk but their business represents a substantial part of the HVGD's turnover. A trigger event that would not be material for smaller customers may be material for a HVGD's large customers, triggering the need apply CDD measures once again.

Applying a risk based approach, HVGDs should take into consideration the evolving risk profile of existing customers when assessing their ML/TF/PF risks. While customers with a consistent risk profile are not exempt from ongoing CDD measures, resources should be focussed on those which are more recent, or those with changes in the pattern of spending or the types of goods they are interested in.

8. Targeted Financial Sanctions

8.1 What are targeted financial sanctions?

Targeted financial sanctions (**TFS**) are legal restrictions imposed by the United Nations, European Union, United Kingdom or Gibraltar against states, people, businesses, organisations and financial institutions (the "**designated persons or entities"**) to achieve specific international policy or security objectives.

TFSs includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons or entities.

TFSs can be issued in relation to:

1. Terrorist Financing (see 1.11) to prevent supply of funds or other assets which are linked to terrorists, terrorist organisations and those who finance terrorism; or
2. Proliferation Financing (see 1.12) to introduce preventative measures to stop the flow of funds or other assets to proliferators and those financing proliferation of weapons of mass destruction.

8.2 Why do I need to know about sanctions?

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

If you undertake an act that is prohibited by financial sanctions and, at the time you did so, you knew or had reasonable cause to suspect that the act was prohibited, you have breached financial sanctions and may face criminal prosecution or a financial penalty. HVGDs must therefore stay up-to-date with the sanctions regimes in force, to:

1. consider the likely exposure of their business to sanctions; and
2. take appropriate steps to mitigate those risks, taking into account the specific nature of their business activities.

8.3 What are my sanctions obligations?

Pursuant to s.8(3) of the Sanctions Act 2019, HVGDs must have policies, controls and procedures in place which ensure that:

1. they are aware of the lists of persons and entities to whom international sanctions apply; and
2. they undertake appropriate checks of the lists when undertaking business in relation to both new and existing customers.

The OFT recommends that HVGDs subscribe to the consolidated lists of UN, UK and EU sanctions so that they screen their new and existing customers against the lists. The list can be found in the 'Sanctions' section of the GFIU's website (www.gfiu.gov.gi/sanctions). Here you will also have access to the GFIU's Financial Sanctions Guidance Notes to assist you further.

8.4 Who needs to be screened?

HVGDs must TFS screen:

1. every person or entity in relation to which a HVGD is required to carry out CDD measures (see section 6);

2. all entities in the control and ownership structure of their customer; and
3. any other person or entity that is involved in a transaction and that they determine should be screened.

8.5 When do I carry out screening?

Unlike CDD, the carrying out of TFS obligations is not a risk-based and therefore applies to all customers.

HVGDs must carry out TFS screening:

1. when they have a new customer or business relationship; and
2. on existing customers or business relationships as and when the TFS lists are updated. HVGDs must therefore have systems to be notified when this happens. The OFT recommends that HVGDs subscribe to the integrated sanctions notification email provided through GFIU's Themis online system that will provide all users with the latest updates of the relevant financial sanctions. For more information and to sign up to the system visit https://www.gfiu.gov.gi/reporting.

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

If you carry out a search on a new or existing customer and you get a positive sanctions match this will need to be investigated further and may require the HVGD to obtain further information in order to assess whether the information reveals that sanctions apply to that person or entity.

You should consider whether you have a false positive, i.e. a match to a designated persons or entity, either due to the common nature of the name or due to ambiguous identifying data, which, on examination, proves not to be a positive sanctions match. You should use all the information at your disposal to determine this on a risk-based approach. If in doubt treat it as a positive sanctions match.

If you have a positive sanctions match you must:

1. immediately freeze any identified assets or funds held or controlled by that person or entity without delay;
2. not deal with the assets or make them available to the designated person or entity; and
3. make a disclosure to the GFIU. When reporting you must include:
    i. the information or other matter on which the knowledge or suspicion is based;
    ii. any information you hold about the designated person or entity by which they can be identified; and
    iii. details of any funds and economic resources that you have frozen.

8.7 Is TFS screening all I need to do?

It should be noted that HVGDs should not rely exclusively on screening TFS lists to meet their TFS obligations. While sanctions screening is a primary control, it has its limitations and should be deployed alongside a broader set of non-screening controls to effectively implement sanctions regimes. HVGDs should therefore also consider information from the UN Security Council to identify red flags for high risk scenarios based on risk factors, including (but not limited to) the nature of their business, their customer base and geographical risks.

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

No! This guidance only set out an overview of the applicability of the Sanctions Act 2019 to the HVGD sector. There are other obligations in the Act that are not referred to in this document. You should not therefore regard this document as an exhaustive authority. The full body of the Act may be found in the 'Documents' section of the 'AML/CFT/CPF' page of the OFT's Website (www.oft.gov.gi).

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

9. Record Keeping, Data & Annual Returns

9.1 What records must be kept?

HVGDs are required to keep records pursuant to s.25 POCA. These records are:

1. copies of the documents and information obtained when carrying out CDD measures (see section 6) in relation to cash transactions in an amount of 10,000 euro or more and business relationships (see 9.2 and 9.3); and
2. the supporting evidence and records of all transactions, both domestic and international, including account files and business correspondence, and results of any analysis undertaken, as well as any other information that may reasonably be necessary to identify such transactions.

The OFT strongly recommends that REAs also keep records of staff training (see 10.3).

The records and data must be readily available for inspection by the OFT on request (Regulation 12 of the Supervisory Bodies (Powers etc.) Regulations 2017).

9.2 Transactions in an amount of 10,000 euro or more and business relationships.

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

1. a copy of the documents and information collected while applying CDD measures (see section 6);
2. the supporting evidence and records of all cash transactions (or set of series of linked cash transactions (see 1.6)) in an amount of 10,000 euro or more (see 9.3);
3. the written risk assessment of every cash transaction (or set of related cash transactions) in an amount of 10,000 euro or more and every business relationship (see 6.17); and
4. the action taken in respect of any suspicious activity detected (see sections 5.5 to 5.7).

In addition, HVGDs must also keep the records of any difficulties encountered during the CDD process (s.10(l) POCA).

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

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

The OFT recommends that 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 HVGD'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 Return to the OFT (see 9.6).

9.4 How long must I keep the records for?

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

9.5 What will the records be used for?

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

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

Additionally, HVGDs are required to submit information annually to the OFT in advance of the renewal of the business licence and may be required to submit annual returns to the OFT providing information and data about cash transactions in an amount of 10,000 euro or more during that year (see 9.7). This information should correspond with the HVGD's records.

The annual return form can be found in the 'AML/CFT/CPF' section of the OFT's website: www.oft.gov.gi.

9.6 When are Annual Returns due?

Prior to the renewal of their business licence HVGDs will receive a business licence renewal notice which shall require them, as part of the renewal process, to declare whether or not they have received payments in cash in an amount of 10,000 euro or more during the term of their licence which is due to expire. Where they declare that that they have received payments in cash in an amount of 10,000 euro or more, the HVGD shall be required to complete and submit the HVGD Annual Return containing up to date financial and other data for the licence term which is due to expire. The due date shall be three months after the HVGD's business licence renewal date.

9.7 What if I miss the deadline?

We strongly urge that you take the appropriate steps to ensure that your business submits its annual returns on time. Failure to do so may result in the HVGD not being allowed to renew their business licence. They may also be subject to enforcement action by the OFT that may include:

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

9.8 What will the OFT do with the Annual Return?

The information will allow the OFT to:

1. collect data about the amount and type of high value transactions carried out by the HVGD and more generally in Gibraltar;
2. monitor HVGDs' compliance with their AML/CFT/CPF obligations under POCA and this guidance; and
3. identify suspicious trends and ML/TF/PF schemes.

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

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

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

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

10. Employer & Employee Responsibilities

10.1 What are my responsibilities as an employer?

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

Additionally, HVGDs have a duty to ensure that its employees are regularly given training to know what ML/TF/PF is and how to recognise and deal with transactions and other activities which may be related to ML/TF/PF (s.27(1)(b) POCA). HVGDs must take appropriate measures, having regard to the risks, the nature of the business and its size, so that its employees are made aware of the law relating to ML/TF/PF and relevant data protection requirements (s.27(1)(a) POCA).

Employees should be familiar with:

1. the requirements in POCA and this guidance;
2. the ML/TF/PF risks to which the trade sector generally is exposed;
3. the specific ML/TF/PF risk to which the HVGD is exposed (see section 3);
4. the HVGD's AML/CFT/CPF policies, controls and procedures including CDD measures (see sections 4 and 6);
5. how to manage transactions on a risk based approach and identify high risk customers and/or high risk behaviour (see section 6);
6. how to report suspicious activity to the MLRO;
7. the penalties for committing offences under POCA and related legislation; and

8. relevant data protection requirements (s.27(1)(a)(ii) POCA).

It is essential to also train employees to understand how ML/TF/PF schemes could take place through the business by providing examples of this.

10.2 How often should training take place?

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

10.3 Records

The OFT strongly recommends that HVGDs keep a staff training record to demonstrate to the OFT that its staff are aware of the business's AML/CFT/CPF policies, controls and procedures and relevant ML/TF/PF risks (see section 9).

10.4 What responsibilities do employees of HVGDs have?

Employees of HVGDs 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/PF;
4. have access to, and familiarise themselves with, all of the business's AML/CFT/CPF policies, controls and procedures; and
5. be aware of the penalties for committing offences under POCA and related legislation.

10.5 Who is responsible for offering training?

It is the responsibility of the HVGD to provide adequate training to its employees (see 10.1 and 10.2). While the OFT provides significant content on its website which may be used for training purposes (www.oft.gov.gi) and often shares opportunities for training with HVGDs, this alone may not be enough to ensure the HVGD meets its training obligations. The OFT should not solely be relied upon to provide training.

The GFIU 's e-Nexus program provides online interactive training sessions regarding AML/CFT/CPF which HVGDs may find useful.

11. Reporting Ownership & Management Changes

11.1 HVGD requirements.

Pursuant to the OFT's powers in Regulations 11(1)(c), 11(3) and 12(1)(b) of the Supervisory Bodies (Powers Etc.) Regulations 2017 the OFT requires all HVGDs to report to the OFT where there is a change to their ownership or management.

11.2 What changes must be reported?

HVGDs must notify the OFT of any change to:

1. the beneficial ownership of a HVGD, including, but not limited to, shareholders, partners and silent partners;
2. the board of directors, an executive and/or another senior manager of a HVGD;
3. a person holding (including persons appearing to the OFT to intend to hold) a management function in a HVGD; and
4. a person in accordance with whose wishes or directions any person involved in the carrying on of the business of a HVGD acts (including persons it appears to the OFT is in that position).

11.3 When do I need to report the change?

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

11.4 What will the OFT do with the information?

Upon receipt of a notification the OFT shall conduct a fit and proper assessment of that person in accordance with the OFT's legal obligations.

11.5 Failure to notify

Where a HVGD fails to notify the OFT of a change to their ownership or management as required by this section within the time limit stipulated it shall regard the failure as non-compliance by the HVGD of its AML/CFT/CPF obligations and shall consider taking appropriate and propionate enforcement action as necessary.

12. Potential High Value Goods Dealers

12.1 Who are Potential HVGDs?

Potential HVGDs are dealers in goods which have not yet received a payment in cash in an amount of 10,000 euro or more but are open to accepting such cash payments.

12.2 Why do Potential HVGDs have obligations?

Potential HVGDs 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 in cash in an amount of 10,000 euro or more it will automatically be a HVGD and this guidance will be applicable to that business in full.

12.3 What are the obligations of Potential HVGDs?

Potential HVGDs' obligations include, but are not limited to:

1. Carrying out a risk assessment of the business's attractiveness and vulnerability to ML/TF/PF (see section 3);
2. Establishing appropriate AML/CFT/CPF policies, controls and procedures commensurate to the business's ML/TF/PF risks (see section 4);
3. Appointing a MLRO who understands the business's ML/TF/PF risks, is acquainted with POCA and who shall be responsible for all AML/CFT/CPF matters (see section 5);
4. Carrying out sanctions screening on new and existing customers (see section 8); and
5. Training staff to ensure they are aware of the HVGD's ML/TF/PF risks and of the business's AML/CFT/CPF polices (see section 10).

References to HVGDs in sections 3 to 10 of this guidance should, where relevant, be read as also applying to Potential HVGDs.

12.4 Can a Potential HVGD avoid these obligations?

Yes. A dealer shall be able to avoid complying with most of Part III of POCA and this guidance if they:

1. do not accept cash payments in an amount of €10,000 or more;
2. have a written policy not to accept cash payments in an amount of €10,000 or more;
3. such policy is communicated in writing to the OFT; and
4. they maintain the cash policy and ensure it is complied with. As soon as the cash policy is not complied with, even if it is only for one transaction, the dealer will automatically be regarded as a HVGD and all of the obligations in the legislation and this guidance shall be immediately applicable.

It should be noted that the OFT may conduct enquiries to determine whether any such cash policy is being implemented. Any changes to cash policies must be communicated to the OFT.in writing.

13.Art Market Participants

13.1 What are Art Market Participants?

According to s.7(1) POCA, Art Market Participants are persons who by way of business:

1. trades in artistic works and the value of the transaction (or series of linked transactions) amounts to 10,000 euro or more; or
2. acts as an intermediary in the sale or purchase of, artistic works and the value of the transaction (or series of linked transactions) in relation to which they

are the intermediary amounts to 10,000 euro or more" ("**Art Intermediaries**").

A person involved in the sale of their own artistic work directly shall not be regarded as an Art Market Participant by the OFT.

The OFT considers that an Art Intermediary is a person that brokers, facilitates, negotiates or otherwise arranges the purchase or sale of artistic works (such as a dealer, advisor or auction house).

13.2 What are artistic works?

According to s. 7 (1) POCA, "artistic work" has the meaning given to it in s. 6 of the Intellectual Property (Copyright and Related Rights) Act 2005 and includes:

1. a graphic work, photograph, sculpture or collage, irrespective of artistic quality;
2. a work of architecture being a building or a model for a building; or
3. a work of artistic craftsmanship.

13.3 What are the obligations of an Art Market Participant?

An Art Market Participant's obligations are largely the same as those that apply to HVGDs in this guidance.

The main difference is that transactions for artistic works in an amount of €10,000 or more need not be in cash for the obligations in POCA to apply to Art Market Participants.

As a result, while references to HVGDs in this guidance should be read to apply generally to Art Market Participants, it should be noted that the obligations should, where relevant, also apply to non-cash transactions involving Art Market Participants also.

An Art Market Participants'' obligations therefore include:

1. Carrying out a risk assessment of the business's attractiveness and vulnerability to ML/TF/PF (see section 3);
2. Establishing appropriate AML/CFT/CPF policies, controls and procedures commensurate to the business's ML/TF/PF risks (see section 4);
3. Appointing a MLRO who understands the business's ML/TF/PF risks, is acquainted with POCA and who shall be responsible for all AML/CFT/CPF matters (see section 5)
4. Carrying out CDD measures and assessing customer and transactional risk (see Section 6);
5. Carrying out ongoing monitoring of its customers and business relationships (see Section 7);
6. Carrying out sanctions screening on new and existing customers (see section 8);
7. Keeping records and data and submitting annual returns (see section 9); and
8. Training staff to ensure they are aware of the HVGD's ML/TF/PF risks and of the business's AML/CFT/CPF polices (see section 10)

14. Useful Contacts

14.1 Gibraltar Financial Intelligence Unit

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

Suite 832, Europort, Gibraltar

Tel: (+350) 20070211

Fax: (+350) 20070233

gfiu@gcid.gov.gi

www.gfiu.gov.gi

14.2 HM Customs Gibraltar

HM Customs Gibraltar is the supervisory authority for the trade in tobacco in Gibraltar and for art storage freeport operators.

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 Customer ML/TF/PF Risks

1. Identifying risk factors

This schedule sets out a number of common factors that HVGDs and their employees may take into account when carrying out ML/TF/PF risk assessments of customers and transactions. For assessing a HGVD's ML/TF/PF risk please refer to section 3.

It is important to note that this schedule only provides indicators to consider when assessing risk. The identification of one of these factors need not necessarily mean that ML/TF/PF is, or will be, taking place. They will however assist the HVGD 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.

Pursuant to s.17(3) POCA, HVGDs must examine, as far as reasonably possible, the background and purpose of all transactions that fulfil at least one of the following conditions as indicators of high risk:

1. they are complex transactions;
2. they are unusually large transactions;
3. they are conducted in an unusual pattern;
4. they do not have an apparent economic or lawful purpose, and in particular, a HVGD shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

The factors listed in this schedule are not an exhaustive list and HVGDs and their employees should take into account all of the information at their disposal to determine if there is a ML/TF/PF risk. If more information is required, it should be requested before proceeding with a transaction to ensure that there is no ML/TF/PF risk.

2. Assessing low risk customers?

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

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

3. Who are high risk customers?

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

The following are indicators of high risk customers:

1. brand new customers carrying out large one-off transactions;
2. customers engaged in a business which involves the constant movement of significant amounts of cash;

3. customers who carry out transactions that:
    i. do not make commercial sense;
    ii. have an unusual pattern; and/or
    iii. are complex;
4. existing customers where:
    i. the transaction is different from the usual business of the customer;
    ii. the size and frequency of the transaction is different from the customer's usual pattern of business,

    (see 6 below).
5. complex business ownership structures with the potential to conceal underlying beneficial owners;
6. politically exposed persons (these will always require enhanced CDD, see 6.15 of the guidance notes and paragraph 4below); 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).

4. Who are politically exposed persons?

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

1. Heads of State, heads of government, ministers and deputy or assistant ministers;
2. Members of parliament or of similar legislative bodies;
3. Members of the governing bodies of political parties;
4. Members of supreme courts, of constitutional courts or of other 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 8 are not regarded as PEPs).

These individuals, who may be local or international PEPs, are usually at a higher risk of having possible connections to money laundering in particular 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 s.20A POCA).

For more information about transacting with PEPs see section 6.15 of the guidance notes. For in depth guidance on PEPs please refer to the FATF's guidance which can be found in the 'AML/CFT/CPF' section of the OFT's website (www.oft.gov.gi).

5. 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. funds available do not tally with type of customer;
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, charges or rates;
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.

6. Monitoring patterns of business.

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

1. a sudden increase in business from an existing customer;
2. uncharacteristic transactions which are not in keeping with the customer's financial situation;
3. 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 cannot give a proper explanation of where the money comes from;
5. peaks of activity at particular locations or properties; and/or
6. unfamiliar or atypical types of customer or transaction.

7. Enhanced due diligence and reporting.

The indicators above may, when assessed by the HVGD or its employees, require enhanced due diligence to ensure that the AML/CFT/CPF risk is understood appropriately and the necessary risk assessment is carried out (see sections 6.11 and 6.16 of the guidance notes).

If the HVGD's MLRO, having considered all the factors surrounding the customer and the transaction, knows or suspects that ML/TF/PF is taking place, they should submit a suspicious activity report (see sections 5.6 to 5.8 of the guidance).

Schedule 2 – Verifying Source of Funds & Wealth

1. **Purpose of establishing/verifying source of wealth and funds**

Pursuant to s.10(f) POCA, the application of CDD measures includes "taking a risk-based approach to the verification of source of funds and wealth of the customer and beneficial owners".

As defined by the Financial Action Task Force (**FATF**):

1. Source of funds – "*refers to the origin of the funds or assets which are the subject of the business relationship between the [HVGD] and its client and the transactions the [HVGD] is required to undertake on the client's behalf (e.g., the amounts being invested, deposited or remitted)*".
2. Source of wealth - refers "*to the origin of the entire body of wealth (i.e., total assets) of the client*". The purpose of obtaining a customer's source of wealth and funds is to assist the firm in developing an assessment of the economic profile of each customer. This profile should be scrutinised throughout the length of the business relationship to aid in the identification of any suspicious activity.

2. **Plausible verifiability**

The minimum CDD requirements to satisfy yourself on source of funds and wealth is to obtain documents to a level of plausible verifiability. This should be applied to low and medium risk clients.

The term "plausible verifiability" is made up of two parts:

1. Plausible - This is the documentation which evidences that the customer's economic activity is commensurate with the information obtained by the HVGD through its CDD process. It should be clear to the HVGD that the funds a customer is providing are in line with the information held on the customer.
2. Verifiability - This is documentation relating to the economic activity of a client to a level of detail that would enable the HVGD, the OFT, law enforcement agencies or other bodies to verify the source of income/wealth if the customer's risk profile increased, or ML/TF/PF was known or suspected.

3. **Independent verification**

In cases of higher risk, it is no longer considered adequate to apply standard/simplified CDD (see 6.11) and HVGDs must apply enhanced CDD measures (see 6.12). In these cases, HVGDs are required to independently verify the source of funds and wealth of their customer. The information required should be considered on a case-by-case basis in line with the risk posed by the customer.

Independent verification requires that a HVGD corroborates the information provided by the client using reliable and independent sources.

Independent verification must be applied:

1. for PEPs and family members and close associates of PEPs (see 6.15).
2. where the firm has risk profiled the customer as high risk.

In the case of high-net-worth individuals it may be difficult to assess the entirety of their income or wealth. In these cases, the extent of verification required should be in line with the risk profile of the individual and include independent verification of at least the majority of the customer's income or wealth.

Open-source information (e.g. searches on google) can be used for verification purposes, however, the information must be from a reputable and independent source.

4. Corporate clients

In the case of corporate clients, the requirement to establish or verify source of funds and wealth extends to its beneficial owners (**BOs**) (see 6.6), regardless of whether the funds or wealth of the entity are derived from the BOs or the company's own activities. This is due to the risk that the BOs are in a position to transmit illicit funds through the entity.

In the case of the activity of the corporate itself, audited financial statements are typically sufficient for verifying source of funds and wealth. Where this is not an option, other documentation should be considered on a case-by-case basis.

5. Examples of CDD to corroborate source of funds & wealth

Below is a non-exhaustive list of documents that can be used to verify source of funds and source of wealth.:

1. Employment income:
    - Name and address of employer;
    - Nature of business;
    - Annual salary and bonuses;
    - Recent payslip;
    - Latest accounts/tax declaration (if self-employed).
2. Savings
    - Bank statement and enquiry on source of wealth.
3. Property sale
    - Details of the property;
    - Copy of contract sale;
    - Title deed
4. Sale of shares or other investment
    - Copy of contract;
    - Sale value of shares sold;
    - Statement of account from agent;
    - Transaction receipt/confirmation;
    - Shareholder's certificate;
    - Date of sale.
5. Loan
    - Loan agreement;
    - Amount, date and purpose of loan;
    - Name and address of lender;
    - Details of any security.
6. Gift
    - Date received;
    - Total amount;
    - Relationship to applicant;
    - Letter from donor explaining reason for
    - the gift;
    - Certified identification documents of
    - donor;
    - Source of wealth documentation of donor.
7. Maturity/Surrender of life policy
    - Amount received;
    - Policy provider;
    - Policy number/reference;
    - Date of surrender.
8. Company sale
    - Copy of the contract of sale;
    - Internet research of Company Registry;
    - Name and address of Company;
    - Total sales price;
    - Applicants' share participation;
    - Nature of business;
    - Date of sale and receipt of funds;
    - Media coverage.
9. Company profits/dividends
    - Copy of latest audited financial statements;
    - Copy of latest management accounts;

- Board of Directors approval;
- Dividend distribution;
- Tax declaration form.

10. Inheritance

- Name of deceased;
- Date of death;
- Relationship to applicant;
- Date received;
- Total amount;
- Solicitor's details;
- Tax clearance documents.

Schedule 3 - Glossary of Terms & Abbreviations

Art intermediary	Refer to section 13.1
Art Market Participant	Refer to section 1.2 and 13.1
Artistic works	Refer to section 13.2
AML	Anti-money laundering and
BO	Beneficial owner
Cash	Money in coins or notes.
CDD	Customer due diligence
CFT	Combatting the financing of terrorism
CPF	Counter proliferation financing
FATF	Financial Action Task Force
GFIU	Gibraltar Financial Intelligence Unit
HVGD	High-value good dealer
High value good	Refer to section 1.8
ID	Personal identification document
ML	Money laundering
MLRO	Money laundering reporting officer
NRA	National Risk Assessment
OFT	Office of Fair Trading
PEP	Politically exposed person
PF	Proliferation financing
SAR	Suspicious activity report
SBPR	Supervisory Bodies (Powers Etc.) Regulations 2017
TF	Terrorist financing
TFS	Targeted financial sanctions