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

Guidance Notes for High-Value Dealers (HVDs)

Contents

Disclaimer

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

Issued: June 2017
Updated: October2017

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

1. Introduction/FAQ

1.1 What is AML/CFT?

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

1.2 What is AML/CFT all about?

Money laundering is the process of transforming and concealing the profits generated by criminal activity and corruption (such as drug trafficking, market manipulation, fraud, tax evasion) into a 'clean'/legitimate asset. The buying and selling of high value goods is recognised as a major avenue for money laundering activity. High value goods transactions that are done via electronic payment can be easily tracked by law enforcement. However, transactions that involve large sums of cash are virtually invisible, making them very attractive to criminals seeking to launder illicit funds. These activities assist the financing of terrorism and organised crime. The vulnerabilities and risks of money laundering and terrorist financing in Gibraltar are set out in the National Risk Assessment (**NRA**) published by HM Government of Gibraltar. You can find a copy of the NRA in the 'AML/CFT' section of the OFT's website (www.oft.gov.gi).

1.3 Why is the OFT issuing these guidelines?

The OFT is required to regulate compliance with the AML/CFT obligations set out in the Proceeds of Crime Act 2015 (see section 2 below) by dealers in high-value goods, otherwise known as High Value Dealers (the "**HVDs**"). As a result, it is issuing these guidelines to assist HVDs and their employees and to give an overview of their legal obligations as set out in POCA.

1.4 Who are high-value dealers?

HVDs are businesses that accept cash payments in any currency with a value which are equal to, or greater than, €15,000.00 in exchange for goods. However, the OFT will consider any transaction for goods which is equal to, or greater than, £8,000.00 as a high value transaction for the purposes of these guidelines.

1.5 Who do these guidelines apply to?

These guidelines apply to HVDs who accept cash payments. They also apply to the employees of these businesses.

1.6 Are these guidelines relevant to all cash payments?

No. Only those which are above the monetary threshold (see 1.7 below).

1.7 What is the monetary threshold?

The monetary threshold is set at the equivalent of £8,000 (eight thousand pounds), or any higher amount. This also includes any currency equivalents, based on the exchange rate at the time the transaction is made.

1.8 What if I never accept high value cash payments?

Even if a business never accepts high value cash payments, it should nevertheless still be aware of its legal responsibilities, appoint a nominated officer (see 3.2 and section 6 below) and have a policy for reporting

suspicious payments along with a AML & CFT internal policy for its employees.

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

No. Only those payments which, having applied the customer risk assessment and monitoring criteria in section 4 below, are suspected of being made in connection with money laundering or the financing of terrorism.

1.10 Is the monetary threshold passed if cash is paid over a period of time?

The monetary threshold is passed upon the occurrence of any of the following cases:

i) the business receiving a single cash payment of £8,000 or more;

ii) the business receiving several cash payments totalling £8,000 or more, including a series of payments and payments on account from the same customer;

iii) cash payments by a customer totalling £8,000 or more in any 90 day period; or

iv) cash payments totalling £8,000 or more which appear to have been broken down into smaller amounts to come below the £8,000 limit.

1.11 Does the monetary threshold apply to credit and debit card payments and transfers?

No. It is only relevant to payments in cash.

1.12 What will the OFT do if it receives evidence of money laundering?

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

1.13 Does this booklet contain all I need to know?

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

2. Proceeds of Crime Act 2015 (POCA)

2.1 What is POCA?

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

2.2 Where can I find the POCA?

This Act may be found in the 'AML/CFT' section of the OFT's Website (www.oft.gov.gi) along with a pdf copy of these guidance notes. It can also be found on the Government's Gibraltar laws website by searching for "Proceeds of Crime" (www.gibraltarlaws.gov.gi)

3. HVDs' Responsibilities

3.1 What are the responsibilities of a HVD?

HVDs need to put in place certain controls to prevent their business from being used for money laundering. These controls usually take the form of a written policy. For information on creating an AML/CFT Policy please see Schedule 1.

3.2 Appointing a nominated officer

All HVDs must appoint a nominated officer (sometimes known as a money laundering reporting officer or MLRO). Each nominated officer shall be responsible for dealing with any AML/CFT matters and carry out appropriate risk assessments (in accordance with section 4 below) before the business can accept payments in cash above the monetary threshold (see section 5 below). If you are a sole trader or the only person conducting the business, then you are automatically the nominated officer and directly responsible. (Please see our money laundering reporting officer registration form under Schedule 2).

3.3 What controls should HVDs put in place?

HVDs should develop a policy that allows them to:

i) carry out customer due diligence (see 3.4 below) and monitor customers' business activities;

ii) assess the risk of their business being used by criminals to launder money (in accordance with section 4 below);

iii) submit annual reports to the OFT and reply to audit queries (see 5 below);

iv) report suspicious activity and customers regarded as a high money laundering risk (see 6.6 below);

v) ensure employees:
   1. are aware of POCA;
   2. are aware of the HVD's AML/CFT policy;
   3. have the necessary training; and
   4. are able to report to the nominated officer (see 3.5 below);

vi) keep customer, transactional and staff training records,(see 5 below);

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

3.4 What is customer due diligence?

Customer due diligence (sometimes known as 'know your customer' or KYC) involves verifying the identity of your customers before doing business with them. HVDs must know the identity of customers from which they are receiving payment above the monetary threshold.

Each time a cash transaction above the £8000 threshold is made a copy of the customer's ID (i.e. passport, ID card, drivers licence) should be kept along with the customer's contact details (address, contact number, email, etc.). All copies of identification should be dated and signed 'original seen'.

If the customer is acting on behalf of someone else, appropriate identification of any third parties should also be requested.

Where your customer is a company, then not only must you know the person you are dealing with, but also who the beneficial

owner is (the individual who ultimately owns the company).

Due diligence is not required for banks, EU listed companies or HM Government of Gibraltar entities.

HVDs must keep copies of due diligence documents (see 5 below).

3.5 Employee awareness

Employees should be made aware of the laws concerning money laundering and terrorist financing, including POCA (see 7 below).

In particular, client facing employees should receive regular training to make sure the business complies with the relevant laws.

Employees should also be trained on how to recognise suspicious transactions and what to do if they identify them. They should understand how their employer's anti money laundering policies and procedures affect them.

Staff should also be made aware of the penalties for committing offences under POCA and related legislation.

For further information and assistance regarding employee training and AML & CFT courses please contact the Office of Fair Trading.

3.6 Record Keeping

HVDs must keep various documents and data relating to transactions above the monetary threshold (see 5.1 below).

HVDs must also keep a staff training record to demonstrate to the OFT that its staff are aware of the business's AML/CFT policies and procedures.

3.7 Annual reports

HVDs are required to submit annual reports to the OFT which shall be used for data collection purposes and to analyse compliance with POCA (see 5 below). Annual reports, and the information they contain, may be audited by the OFT.

3.8 This sounds complicated, I'll pretend I don't receive high value payments!

The OFT works closely with GFIU and other HVDs to regulate the market and uses various sources to acquire information and determine if your business is one that is likely to be receiving high value cash payments.

Businesses who have failed to fulfil their POCA responsibilities will be subject to enforcement action, including:

i) financial penalties up to EUR 1 million;

ii) the suspension or revocation of their business licence;

iii) temporary bans for persons in managerial positions; and/or

iv) a direction to the business to take/ refrain from taking action.

4. Customer Risk – Assessment and Monitoring

4.1 What is a risk assessment?

A risk assessment is the process of assessing the risk that a customer may be using a HVD to launder money.

Each HVD has the responsibility of ensuring that both their appointed nominated officer and relevant employees are able to assess and identify a suspicious activity risk within their industry and line of work. Other than the high risk behaviour which can be easily detected and distinguished the employees must also familiarise themselves with not so clear risk pointers within their line of business.

4.2 Risk assessment policies and procedures.

All HVDs must have an AML/CFT risk assessment procedures to identify and manage its money laundering and terrorist financing risks (see 4.3 below). HVDs may only accept cash payments above the monetary threshold if, having carried out a risk assessment, they are of the view that there is no risk of money laundering or terrorist financing (see 6.4 above). HVDs must be able to show that they have applied their policies and procedures to any payments above the monetary threshold.

4.3 How do you asses the risk?

This is determined on a case-by-case basis. There are various factors HVDs may take into account in determining the likelihood of a risk. These include, but are not limited to, the identity and type of customer, the customer's behaviour and the type of transaction being carried out. These factors need to be weighed up in determining the risk of the HVD being used for money laundering and/or the financing of terrorism.

4.4 Who are high risk customers?

Common features include:

i) brand new customers carrying out large one-off transactions;
ii) customers engaged in a business which involves significant amounts of cash;
iii) customers who carry out transactions that do not make commercial sense;
iv) complex business ownership structures with the potential to conceal underlying beneficiaries (owners); and/or
v) politically exposed persons or persons from high-risk jurisdictions (these will require enhanced customer due diligence).

4.5 What is high-risk behaviour?

The following are indicators of high-risk behaviour:

i) an unwillingness to produce evidence of ID or the production of unsatisfactory evidence of ID;
ii) 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;
iii) a willingness to bear very high or uncommercial penalties or charges; and/or
iv) situations where the customer's source of funds are unclear.

4.6 Monitoring patterns of business.

Risk assessment must also include the review and monitoring of the money laundering and terrorist financing risks to the business. The risk-based approach is developed by monitoring patterns of business, for example:

i) a sudden increase in business from an existing customer;
ii) uncharacteristic transactions which are not in keeping with the customer's known activities;
iii) peaks of activity at particular locations or at particular times; and/or
iv) unfamiliar or untypical types of customer or transaction.

4.7 When do I report suspicious activity?

This will depend on the risk assessment carried out and is ultimately a question for the nominated officer, having considered all information it has about the customer and the transaction. We have however provided some examples of suspicious activity below for guidance;

i) An individual looking to purchase a high value good such as an antique, a valuable watch, painting or a car. The individual wishes to pay for the transaction in cash. He is a new customer to the business and checking his identity is proving to be difficult. The individual has questioned why there is any need for him to submit proof of identification and he has requested to pay in numerous instalments of small amounts. In this particular case the combination of risk factors should be enough to arise suspicion and bring the transaction to the attention of the nominated Anti Money Laundering Officer.

ii) A known customer who frequently makes cash transactions has been increasing his number of transactions and the amount spent on purchases considerably. The size and frequency of the transactions are not consistent with the customer's normal activities. In addition, the high amounts of cash are not reasonable within the customer's line of work. The source of the cash is unknown and when the customer was asked he was reluctant to provide details. In this case there would also be a combination of risks which should raise suspicion and be bought the nominated officer immediately.

If in doubt, submit a SAR! (see 6.1 below)

4.8 Managing and mitigating the risk.

Each HVD will carry a different level of risk. It is therefore important for each business to assert their own vulnerability. The level of risk for each HVD must be based on research within their industry and a suitable AML/CFT business policy which targets and addresses all the issues and concerns that the specific business faces.

Once the business has identified and assessed the risks it faces of being used for money laundering or terrorist financing it must ensure that appropriate controls are put in place to lessen these risks and prevent the business from being used for money laundering or terrorist financing.

5. Record Keeping & Annual Reports

5.1 What records should be kept?

All HVDs must have appropriate systems in place for recording and keeping the following:

i) customer due diligence documents; (see 3.4 above);

ii) records and data of all high value cash transactions including those above the monetary threshold; and

iii) AML/CFT risk assessments of customers making payments above the monetary threshold.

The OFT encourages all HVDs to keep a High Value Cash Transaction File.

5.2 What type of data should be collected?

As much data as you can about cash transactions, even those below the monetary threshold. As a minimum you should keep at least sufficient data to allow you to complete and submit an Annual Report (see 5.4 below).

5.3 For how long should records be kept?

All records and information pertaining to high value purchases should be kept for a minimum of 5 years.

5.4 What will the businesses records be used for?

HVDs are required to submit an Annual Report to the OFT providing information and data about cash payments received by the business during that year. The Annual Report form can be found in the 'AML/CFT' section of the OFT's website (www.oft.gov.gi).

5.5 What will the OFT do with the Annual Report?

The information will allow the OFT to collect data to regulate HVDs more effectively and to in turn assist in identifying and preventing money laundering and the financing of terrorism. The data may be provided to other POCA supervisory authorities and law enforcement bodies.

The OFT may also want to examine a HVD's records to investigate any cash transactions.

The OFT may also carry audits of the Annual Reports it receives to ensure that these are being completed accurately by HVDs.

5.6 When are the Annual Reports due?

For simplicity the OFT have linked the reporting dates to tax deadlines as follows:

i) HVDs which are not companies:

Report due 30th November (tax return is due) for period from 1st December to 30th November of the preceding year;

ii) HVDs which are companies:

Report due 31st October (a month after second payment on account on 30th September) for period from 1st October to 30th September.

5.7 What if I miss the deadline?

We strongly urge that you take the appropriate steps to ensure that your business submits Annual Reports. Failure to do so may result in enforcement action by the OFT (see 5.9 below).

5.8 Is anything else required?

Annual Reports from companies must be accompanied by an independent

accountant's verification confirming that the Report gives a true and fair representation of the cash transactions reported by the company in the report.

5.9 I don't want to submit a return! How will the OFT know I'm receiving high value cash payments?

The OFT works closely with GFIU and other HVDs to regulate the market and will use various sources to acquire information to determine if your business is one that is likely to be receiving high value cash payments. If we expect an Annual Report from your business and it does not submit one we will carry out an appropriate investigation.

Businesses who have failed to fulfil their POCA responsibilities will be subject to enforcement action, including:

i) financial penalties up to EUR 1 million;

ii) the suspension or revocation of their business licence;

iii) temporary bans for persons in managerial positions; and/or

iv) a direction to the business to take/ refrain from taking action.

6. Nominated Officer Responsibilities

6.1 What is the nominated officer's role?

The role of the nominated officer is to be aware of any suspicious activities involving the HVD that might be linked to money laundering or terrorist financing. If necessary the nominated officer must report such activities or risks to the GFIU by submitting a Suspicious Activity Report (**SAR**) (see 6.6 below). SAR forms can be downloaded from the 'AML/CFT' section of the OFT's website (www.oft.gov.gi) and submitted to the GFIU by e-mail (gfiu@gcid.gov.gi) or delivered by hand to their offices at Suite 832, Europort.

6.2 Who can be appointed as a nominated officer?

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

i) can be trusted with the responsibility;

ii) is senior enough to have access to all customer files and records; and

iii) is autonomous enough to decide whether they need to report suspicious activities or transactions.

A sole trader with no employees must act as the nominated officer themselves. The role of nominated officer should not be held by an external consultant.

6.3 Nominated officer registration

HVDs must register their nominated officers with the OFT. They should do so by completing and submitting an Officer Registration Form to aml.oft@gibraltar.gov.gi. This form may be downloaded from the 'AML/CFT' section of the OFT's website (www.oft.gov.gi).

6.4 What are the nominated officer's responsibilities?

No payments above the monetary threshold (see 1.8 above) may be received by the HVD

until the nominated officer has carried out a risk assessment in accordance with section 4 above.

Nominated officers must receive reports of suspicious activity from any employee in the business. They must then evaluate the reports for any evidence of money laundering or terrorist financing and carry out an appropriate risk assessment. They must keep a record of these risk assessments (see 5.1 above)

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

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

ii) training staff in preventing money laundering and terrorist financing using the HVD.

6.5 What happens if a money laundering or terrorist financing risk is identifies?

The nominated officer should consider all of the information about a HVD's customer and the transaction which he intends to carry out. If there are reasonable grounds to suspect money laundering they must report this to GFIU at the earliest possible opportunity using a SAR.

If in doubt, submit a SAR!

6.6 How does the nominated officer make a report to the GFIU?

Reports from nominated officers to the GFIU may be made by completing a Suspicious Activity Report (SAR). SAR forms can be downloaded from the 'AML/CFT' section of the OFT's website (www.oft.gov.gi) and submitted to the GFIU by e-mail (gfiu@gcid.gov.gi) or delivered by hand to their offices at Suite 832, Europort.

6.7 Should the nominated officer prevent a suspicious transaction taking place?

The nominated officer should seek consent from GFIU before proceeding with a transaction it suspects is being carried out to launder money or finance terrorism. If it is not possible to delay the transaction to get GFIU consent however, the nominated officer should proceed to complete the transaction and, as soon as possible, inform GFIU by submitting a SAR.

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

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

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

6.9 What happens in the nominated officer's absence?

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

A nominated officer's absence should not restrict the HVD's ability to monitor risk and submit SARs to GFIU.

7. Employee Responsibilities

7.1 What responsibilities does a HVD's employees have?

Employees of HVDs should:

i) know who their nominated officer is and what they're there for;

ii) detect suspicious activity and report it to the nominated officer;

iii) be aware of the steps taken by the business to ensure it is not used for money laundering or terrorist financing;

iv) have access to and familiarise themselves with all of the business's AML/CFT policies, procedures and risk assessments; and

v) be aware of the penalties for committing offences under POCA and related legislation.

It is the responsibility of the HVD to provide adequate training to its employees (see 3.5 above).

8. Useful Contacts

8.1 Office of Fair Trading

The OFT has been appointed as a supervisory authority under POCA for High Value Dealers and Real Estate Agents. Additionally it is responsible for business licensing and for consumer protection in Gibraltar.

- Suite 975 Europort, Gibraltar
- Tel: (+350) 20071700
- e-mail: aml.oft@gibraltar.gov.gi

8.2 Gibraltar Financial Intelligence Unit

GFIU receives, analyses and disseminates financial intelligence gathered from Suspicious Activity Reports (SARs) (see 6.6 above).

- Suite 832, Europort, Gibraltar
- Tel: (+350) 20070211
- e-mail: gfiu@gcid.gov.gi

8.3 Gibraltar Financial Services Commission

The GFSC is the financial services regulator in Gibraltar and regulates auditors, banks, company managers, e-money institutions, professional trustees, payment services providers, funds and fund service providers, insurance companies, managers and intermediaries, investment firms, and insolvency practitioners. It has been appointed as a supervisory authority under POCA.

- Atlantic Suites, Suite 3, Ground Floor, Gibraltar
- Tel: (+350) 20040283
- e-mail: information@fsc.gi

8.4 Gambling Division

The Gambling Division is the regulator for all gambling related matters in Gibraltar and is also appointed as a supervisory authority under the POCA. It has been appointed as a supervisory authority under POCA.

- Suite 603, Europort, Gibraltar
- Tel: (+350) 20064142
- E-mail: gamblinglicensing@gibraltar.gov.gi