ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

High Value Goods Dealers

Sector Specific AML/CFT Guidance Notes

August 2021

Contact:
AML/CFT Division
Financial Services Authority
PO Box 58
Finch Hill House
Bucks Road
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Contents

Version history

Version 2 (August 2020)	Updates made to links in relation to the updated NRA
Version 3 (August 2021)	Updates to reflect changes to the main structure of the AML/CFT Handbook Updates to footnotes to include links in the main body for consistency purposes

1. Foreword

For the purposes of this sector specific guidance the term high value goods dealer ("HVGD") refers to a business conducting activity included in paragraph 2(6)(p) of Schedule 4 to the Proceeds of Crime Act 2008 ("POCA"). The activity is defined as follows:

> (p) dealing in goods or services of any description (including dealing as an auctioneer) whenever a transaction or series of linked transactions involves accepting a total cash payment (in any currency) that is equivalent to at least €15,000;

The term "total cash payment" is not defined in legislation, however the following instances should be considered to determine if the above activity has occurred:

- a single cash payment of €15,000 or more;
- several cash payments totalling €15,000 or more, including a series of payments and payments on account within a 90 day period;
- cash paid by a customer totalling €15,000 or more in any 90 day period; or
- cash payments totalling €15,000 or more which appear to have been broken down into smaller amounts to potentially come below the threshold limit.

By virtue of being included in Schedule 4 to POCA, the business of a high value goods dealer is subject to the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code"). Also, this sector is included in the Designated Businesses (Registration and Oversight) Act 2015 which came into force in October 2015. The Financial Services Authority ("the Authority") has the power to oversee this sector for Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") purposes.

Therefore, any HVGD must be registered with the Authority in advance of accepting a total cash payment of €15,000. Businesses carrying out such activity without being registered commit a criminal offence. Please see section 7 of the Designated Business (Registration and Oversight) Act 2015 for further details.

The Authority recommends that any businesses dealing in high value goods that are not registered (due to not accepting total cash payments exceeding €15,000) adopt clear company policies and procedures to ensure staff are prevented from entering into such transactions.

2. Introduction

The purpose of this document is to provide some guidance specifically for the HVGD sector in relation to AML/CFT. This document should be read in conjunction both the Code and the main body of the AML/CFT Handbook ("the Handbook").

Though the guidance in the Handbook, and this sector specific guidance, is neither legislation nor constitutes legal advice, it is persuasive in respect of contraventions of AML/CFT legislation dealt with criminally, by way of civil penalty or in respect of the Authority's considerations of a relevant person's (as such a term is defined in paragraph 3 of the Code) regulatory / registered status and the fit and proper status of its owners and key staff where appropriate.

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the sector and provides further guidance in respect of approaches to customer due diligence where it may vary across between sectors.

This document includes some risk factors that are discussed in the June 2008 FATF Risk Based Approach Guidance for Dealers in Precious Metals and Stones.

2.1 National Risk Assessment

The Island's National Risk Assessment ("NRA") was published in 2015 and was updated in 2020. HVGDs must ensure their business risk assessment (and customer risk assessments where necessary) take into account any relevant findings of the NRA.

Laundering money through the purchase and re-sale of high value goods is a well-recognised international typology. Payments by cash or similar monetary instruments create a higher risk for ML as there is no clear audit trail and therefore the origin of the funds is harder to trace. Considering the high value goods themselves, they tend to be transportable, internationally exchangeable and easy to trade anonymously. Gold is particularly attractive to money launderers because it has a high intrinsic value, is readily accepted across the world and can be melted down into many different forms.

There are some vulnerabilities, particularly in terms of car and motorcycle dealerships due to the limited amount in the IoM that are UK or European franchised dealers (which are obligated to follow group policy regarding handling cash). Nevertheless HVGD represent a very small part of the Designated Businesses sector in the IoM and the indications are that the sector presents a **Low** risk nationally for ML and for TF.

3. Risk Guidance

The high value goods industry can cover a range of businesses, the commonality across these businesses is the acceptance of cash which remains the main part of much serious criminal activity. It can be very difficult to integrate large amounts of cash in to the global financial system. Therefore, the use of cash, monetary instruments or bearer negotiable instruments ("BNIs") as a means of payment, or method to transfer funds, can pose a higher risk of ML/FT than other means, such as wire transfer, cheques or illiquid securities.

The Code mandates that a number of risk assessments are completed –

- a business risk assessment (paragraph 5);
- a customer risk assessment (paragraph 6); and
- a technology risk assessment (paragraph 7)

In order to complete these risk assessments and keep them up-to-date vigilance should govern all aspects of all dealings with its customers, including:

- establishment of the business relationship or conducting of an occasional transaction;
- any linked transactions;
- ongoing monitoring of the business relationship; and
- technology / security issues if there is an online element to the business relationship or transaction.

3.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed under chapter 2 of the Handbook, the following activities may increase the risk of the relationship. Just because an activity / scenario is listed below it does not automatically make the relationship high risk, the customer's rationale / nature / purpose of the business relationship etc. should be considered in all cases.

If a business is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which cause it concerns, it should be determined whether this is suspicious or unusual activity. Please refer to chapter 5 of the Handbook for further detail of the Island's suspicious activity reporting regime.

As stated in paragraph 13 (Ongoing monitoring) of the Code:

> **13 Ongoing monitoring**
> (2) Where a relevant person identifies any unusual activity in the course of a business relationship or occasional transaction the relevant person must –

(a) perform appropriate scrutiny of the activity;

(b) conduct EDD in accordance with paragraph 15; and

(c) consider whether to make an internal disclosure.

(3) Where a relevant person identifies any suspicious activity in the course of a business relationship or occasional transaction the relevant person must –

(a) conduct EDD in accordance with paragraph 15 of the Code, unless the relevant person believes conducting EDD will tip off the customer; and

(b) make an internal disclosure.

This list of higher risk indicators is by no means exhaustive, and relevant persons should be vigilant for any transactions where suspicion may be aroused and take appropriate measures. Also please see the list of red flags included at 3.2.

- Where a customer is reluctant to provide normal information or provides only minimal information where requested.
- Where a customer's documentation cannot be readily verified.
- The customer is reluctant to provide the business with complete information about the nature and purpose of the relationship.
- The transaction(s) does not appear in line with what would be expected of the customer. For example, the size of purchase might be out of line with the appearance / age of the customer.
- The customer over-pays and then requests their over-payment to be refunded by wire transfer or cheque instead of cash. For example a customer wishes to purchase two items, pays for both in cash and then chooses to buy only one of the items.
- Unusual enquiries regarding the businesses refund policy. For example, asking if a refund can be made by cheque, transfer or to a third party.
- It is unusual for a customer to pay for the goods in question in cash.
- The customer was paying for goods debit/credit card or cheque but suddenly offers large cash payment.
- The customer is insistent they only wish to pay in cash.
- Unusual delivery requests such as asking for an item to be shipped to a third party overseas.
- The customer is located in a higher risk jurisdiction.
- Transactions involving numerous jurisdictions.
- The customer has no discernible reason for using the businesses' services, or the businesses' location.
- The customer exhibits unusual concern with the businesses' compliance with Government reporting requirements and/or AML/CFT policies and procedures.

3.2 Red Flags

In addition to the above higher risk indicators, there are some factors that are likely to be "red flags" in relation to that particular relationship or occasional transaction and would therefore

usually be suspicious activity. If a relevant person identifies suspicious activity appropriate steps as explained in section 3.1 of this document, and the Code, must be taken. This list of red flags is by no means exhaustive and is as follows:

- where it is identified a customer provides false or misleading information;
- where it is identified a customer provides suspicious identification documents;
- the customer does not provide the business with relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated account activity;
- the customer is secretive / evasive when asked to provide more information;
- when requested, the customer refuses to identify a legitimate source of funds or source of wealth;
- the customer refuses to provide details on beneficial owners of an account or provides information which is false, misleading or substantially incorrect;
- the cash being used appears to be stained with dye (this could indicate stolen notes);
- the customer enquires about how quickly they can end a business relationship where it is not expected;
- where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for;
- the customer is known to have criminal / civil / regulatory proceedings against them for crime, corruption, misuse of public funds or is known to associate with such persons; and
- the customer is interested in paying higher charges to keep their identity secret.

3.3 Risk factors specific to the sector

The following section of the guidance covers some of the risk factors specifically related to this particular sector. Further guidance surrounding the risk assessments is outlined in chapter 2 of the Handbook.

A number of risk assessments must be carried out by sectors as set out in the Code, including:

- business risk assessments (paragraph 5);
- customer risk assessments (paragraph 6); and
- technological risk assessments (paragraph 7).

These risk assessments should be used in order to adopt a risk based approach in assessing the risks relating to its business, its customers and any technology used in the provision of the good / service.

3.3.1 Inherent Risks – Cash transactions

Where cash, monetary instruments or BNI transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, relevant persons must approach such situations with caution and make relevant further enquiries.

In relation to cash transactions, the relevant person should consider factors such as:

- the amount of cash;
- the currency(s) of the cash;
- the denominations of cash, being vigilant for larger denomination notes; and
- the condition of the notes, being vigilant for any dye marks on the notes.

Relevant persons should be especially robust when dealing with requests for frequent or unusually large amounts of cash, monetary instrument or BNI by customers, especially where the customer is resident in jurisdictions where tax evasion is a known problem. Relevant persons should be vigilant for explanations given by customers which do not stand up to scrutiny when considering their background and circumstances.

Where the relevant person has been unable to satisfy itself that the transaction is legitimate activity, and therefore considers it suspicious, an internal disclosure must be made.

3.3.2 Inherent Risks – High value goods

High value goods of any type are caught however these are likely to include businesses such as:

- art dealers;
- auctioneers;
- car dealers;
- jewellers; or
- precious metal or stone dealers.

High value goods represent a higher risk of ML/FT as they:

- can be used as a transfer of wealth;
- have a high intrinsic value;
- are relatively easy to transport;
- can be bought and sold easily or anonymously; and/or
- are regularly used in most areas of the world.

Gold is particularly attractive to money launderers because it has a high intrinsic value, is readily accepted across the world and can be melted down into many different forms.

4. Customer due diligence

Part 4 of the Code requires relevant persons to undertake customer due diligence and ongoing monitoring in relation to all business relationships. Chapter 3 of the Handbook provides guidance on how to identify and verify the identity of the customer in relation to both a natural and legal person. Also, guidance on the timing of identification and verification of identity is provided. Please also see section 3.8 of the Handbook for further details on source of funds and source of wealth. For details of particular concessions which may be applicable please see chapter 4 of the Handbook.

In all cases where the requirements of Part 4 of the Code cannot be met (Paragraphs 8(5), 9(9), 10(5), 12(11), 14(6), 15(8) and 19(11)) the procedures and controls must be provide that –

(a) the business relationship must proceed no further;
(b) the relevant person must consider terminating[1] the business relationship; and
(c) the relevant person must consider making an internal disclosure.

5. Case Studies

The case study below is a real life example of risks that have crystallised causing losses and / or sanctions (civil and criminal) against the sector.

5.1. Smuggling of gold and diamonds to Colombia

On June 5, 2003, U.S. Immigration and Customs Enforcement ("ICE") agents arrested 11 individuals at seven jewellery stores across Manhattan's diamond district on charges of participating in an international money laundering scheme. The agents had received information that Colombian drug cartels were laundering money through the purchase, smuggling and resale of diamonds and gold. The cartels were instructing their U.S. employees to buy precious stones in New York with drug proceeds and then to smuggle them to Colombia, where they were resold to refiners for "clean" pesos that the traffickers could use risk-free.

Based on this information, ICE agents launched an investigation in 1999 into several New York jewellers alleged to be involved in the money laundering. According to the charges, the jewellers were approached by undercover agents posing as drug dealers. The agents told the jewellers that they were looking to buy gold and diamonds with illicit funds so they could smuggle these precious metals and stones to Colombia and then resell them for "clean" cash. According to the charges, the jewellers willingly accepting $1million in drug funds from the

[1] In relation to a New business relationship (paragraph 8) the business relationship must be terminated.

undercover agents. The jewellers offered to smelt the gold into small objects, such as belt buckles, screws and wrenches, to facilitate smuggling the items to Colombia.

(Based on an example from the Association of Certified Anti-Money Laundering Specialist's 5th Edition Study Guide)