HAFIZ BROS TRAVEL & MONEY TRANSFER LIMITED

144 Calder Street, Glasgow, G42 7QP.

Policy Statement and Risk Assessment

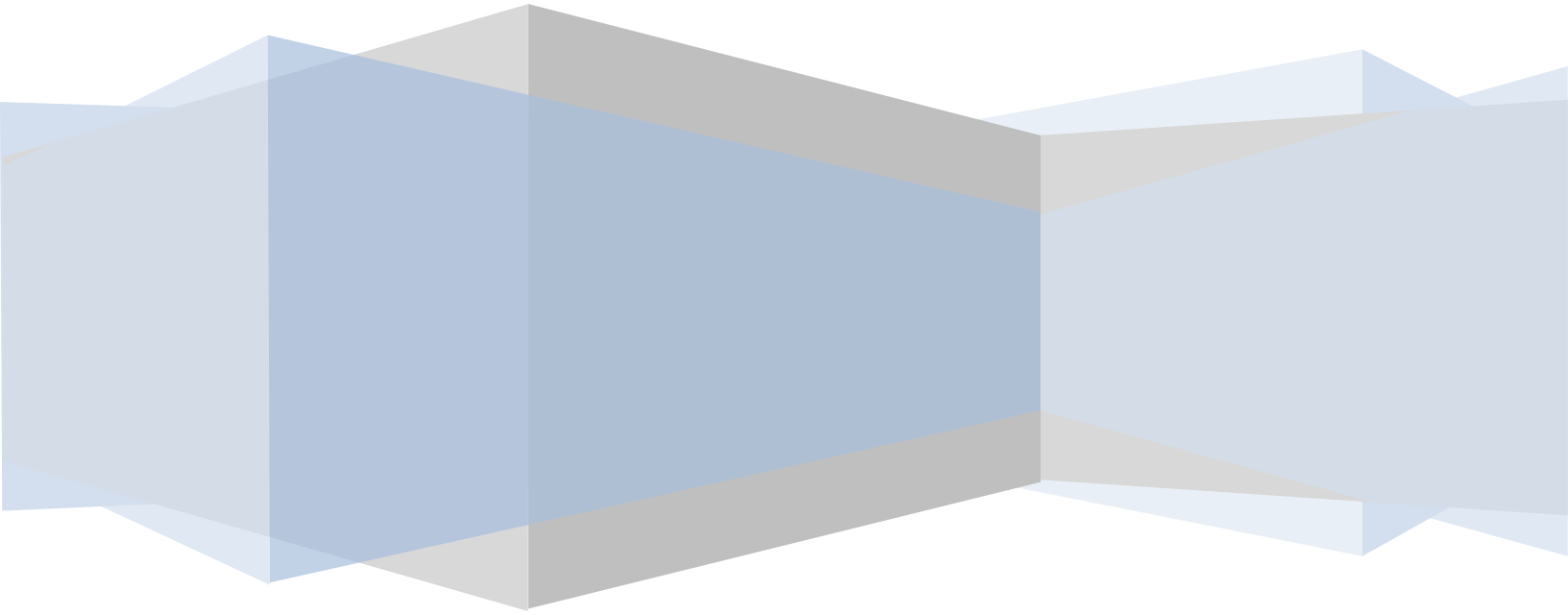

Table of Contents

Policy Statement

Hafiz Bros Ltd, herein referred to as; the Company; recognizes their legal obligations to have procedures and controls in place to deter, disrupt and detect money laundering and terrorist financing.

What is money laundering?

Money laundering is any transaction or series of transactions undertaken to conceal or disguise the nature and source of funds that have been obtained from illegal activity. The main objective of the money launderer is to transform 'dirty' money into seemingly clean money or other assets in a way to leave as little trace as possible of the transformation. Examples of illegal activities that often involve money laundering are drug trafficking, terrorism, fraud, bribery, robbery, embezzlement and illegal gambling.

Commitment to anti-money laundering (AML) legislation

The company totally supports the government's anti-money laundering and combating terrorist financing measures. The company and its staff adopt a zero tolerance approach to money laundering and terrorist financing and are committed 100 % to ensuring that the business is not used by money launderers and terrorists, and that any such attempts or suspicious activity are promptly reported to the relevant authorities.

Employee training

The company is committed to ensuring all relevant staff are made aware of the law and their obligations under it and are regularly trained in how to recognize suspicious activity. All new staff will undergo training before dealing with the public and all existing staff will undergo continuous training. Staff will undergo follow-up training every 6 months.

Prompt reporting of suspicious activity

The company recognizes the importance of staff promptly reporting suspicious activity. Any suspicious activity must be reported immediately to the nominated officer, Mr. Amir Shahzad, who will make a decision as to whether a disclosure be made to the Organized Crime Agency.

Summary of company's approach to assessing and managing its money laundering and terrorist financing risk

The company has adopted a risk-based approach toward the threat of money laundering and terrorist financing. This requires a number of steps which are to:

- Identify the money laundering and terrorist financing risks that are relevant to the business.
- Assess the risks presented by

  The types and behavior of customers

  Products and services offered

  Delivery channels, e.g. cash over the counter, e.g. location of business premises, source or destination of customers' funds

- Design and implement controls to manage and mitigate these assessed risks, e.g. customer ID and verification, and customer due diligence
- Monitor and improve the effective operation of these controls and
- Record appropriately what has been done, and why.

Summary of company's procedures for carrying out ID and verification of that ID

For money transfer

There are stringent procedures in place for sending and receiving money by money transfer, which are detailed in Appendix 1.

For Individuals

ID
When checking ID of individuals the business must obtain their name, address and date of birth.

Verification
Obtain verification of ID from identity documents, e.g. passport or driving license plus secondary identification which shows individuals name and current address, e.g. utility bill or bank statements.

For limited companies

ID
The company should obtain the full name, registered number and registered office in country of incorporation of corporate customer. The names of all directors and names of any beneficial owners holding over 25% of the limited company should be obtained.

Verification
The company should verify the identity of the corporate entity from either a search of the relevant company registry or a copy of the company's certificate of incorporation.

Company's customer due diligence measures

Customers due diligence measures must ascertain the intended nature and purpose of the business relationship and also to collect information on the customer, their business and risk profile to allow ongoing monitoring of the business relationship to ensure that transactions undertaken are consistent with the knowledge.

Due diligence measures must be applied:

- When establishing a business relationship
- When carrying out an occasional large transaction (i.e. involving £2,000 or euro/foreign currency equivalent or more)

- Where there is a suspicion of money laundering or terrorist financing
- Where there are doubts about previously obtained customer identification information
- At appropriate times to existing customers on a risk-sensitive basis

Ongoing monitoring of business relationships

It is essential that there is ongoing monitoring of business relationships which means

- Ongoing scrutiny of transactions (including the source of funds) to ensure that the transaction are consistent with the company's knowledge of the customer, their business and risk profile

- Ensuring that the documents, data or information held evidencing the customer's identity are kept up to date.

Monitoring and managing compliance

Mr. Amir Shahzad is responsible for ensuring that appropriate monitoring processes and procedures are established and maintained.
Regular audits and exercises that test the procedures will be carried out on a regular and ongoing basis.

Risk Assessment

Risk assessment carried out 03 January 2013.

Customer profile

	Percentage of customers
In a business relationship	30%
Regular customers doing one-off transactions	40%
Passing trade	30%
How are customers introduced to the business?	
Through recommendation/word of mouth	70%
Through advertising	20%
Off the street passing trade	5%
Other sources	5%
Are there any non face-to-face customers?	No
Are there any potential Politically Exposed Persons?	No
General description of usual types of customer and Purpose of transactions	Mainly individuals send money to families in Pakistan
Any significant customers outside normal Customers profile?	No
What is percentage of cash transactions?	90%

Risk identification

Money Transmission Business

Money transmission business are faced with a high risk that they will be used to launder the proceeds of crime of transfer monies that finance terrorism. The risk can vary according to customers, delivery channels and geographical destination of funds.

Factors that increase the risk of money laundering or terrorist financing are

- High value remittance
- Cash funding and cash payouts
- The country to which money is being transmitted may have a higher crime rate or likelihood of money laundering or terrorist financing
- Dependence on an agent for customer contact
- Non face to face transactions
- New customer with no previous relationship with money transmission business looking to undertake larger transactions
- Lack of knowledge regarding the origin or destination of funds
- Lack of a meaningful purpose for the transaction

Factors that decrease the risk of money laundering or terrorist financing are

- Low value remittances
- Funding from and payment into bank accounts
- The using of accounts to keep track of customer transactions
- The ability to track linked transactions and identity transaction patterns
- The ability to freeze transactions after they have been initiated
- The countries in which the product operates are regarded as having a lower risk of crime, money laundering or terrorist financing

- Knowledge of the recipient as well as the sender of funds
- Face to face contact with the customer
- An ongoing relationship with the customer
- Knowledge of the origin of funds
- A stated purpose for the transaction

The ID requirements for sending and receiving cash for money transfer quite stringent, which helps to mitigate the risk. However, there is millions of money transfer transactions conducted each month and the likelihood of a particular transaction actually involving the proceeds of crime is very low.

The risk is in failing to identify customers or situations where the level of foreign exchange activity is higher than one would expect from that segment of the business or unusual or inconsistent in some other way. In such circumstances there is justification for looking more closely at whether the customer may be laundering money or financing terrorism.

Factors that increase the risk of money laundering or terrorist financing are

- **Cash transaction:** cash is the mainstay of much organized criminal activity. The objection of the first stage of money laundering is to move the criminal cash into the financial system. They will often seek to exchange cash in one currency for foreign currency or vice versa.
- **Speed and size of the transaction:** Money launders normally want to move funds quickly in order to avoid detection. This is easily done in large one-off transactions.
- **Split transaction:** Money launderers may look to split a large transaction into several smaller one with the intention of avoiding anti money laundering controls. Such known as ‘smurfing’ can occur within one location.
- **Customer operates within a high risk sector:** some money launderers will be proprietors of cash-based businesses such as restaurants, pubs, casinos, taxi firms, beauty salons and amusement arcades. The aim here is to mix ‘dirty’ money with ‘clean’ and so muddy the trail.
- Customer operates a Money Service Business.

- Customer undertakes transactions that make no commercial sense or do not match profile of customer. This will also include significant and unusual changes to a customer's established pattern of behavior.

- The customer is not the beneficial owner of the funds and carries out transaction on behalf of third party or parties.

Factors that decrease the risk of money laundering or terrorist financing are

- The transaction is funded by a cheque, debit/credit card or CHAPS payment.

- Transactions are conducted for a customer on a regular basis and the client is known to the organization.

The company's risk-based approach has been designed to ensure that it places an emphasis within its strategy on deterring and disclosing in the areas of greatest perceived vulnerability.

The provision of currency and the ability to convert currencies is a particular area of risk. Most customers both personal and business will have a legitimate need to convert currency. However, the risk is in failing to identify customers or situations where the level of foreign exchange activity is higher than one would expect from that particular segment of the business or unusual or inconsistent in some other way. In such circumstances there is justification for looking more closely at whether the customer may be laundering money or financing terrorism.

Cheque Encashment

Cheque cashers are not normally exposed to large scale money laundering because the flow of cash in a cheque cashing transaction is in the opposite direction to that required by most money launders. Also is in the very nature that a cheque is traceable, gives us reason to believe that large scale money laundering is unlikely. Outside customers with whom the bureau has a business relationship, only cheques for small sums are cashed, and ID documents with address verification are kept on file. Whilst the risk money laundering is minimal, the possibility is not totally ignored.

Risk factors and response

The risk factors that are relevant to the business and action that will be taken to mitigate these risks are listed below

Risk factor	**Explain why and how the factor does or does not apply**	**What procedures are in place to mange and mitigate the risks**
Customer types and behavior		
Customers with businesses that handle large amounts of cash	Does not apply	If applied ID documents on account file with verification. Ongoing monitoring of transaction to ensure there is no inconsistency with our knowledge of business
Complex business structures	Not applicable at present	Ongoing monitoring
Potentially Politically Exposed Persons	Does not apply	If applies ID documents on account file with verification and ongoing monitoring of every transaction. If anything strange report to SOCA
High risk jurisdictions	Applies small number of money transfer transaction	ID documents on account file with verification. Ongoing monitoring of transaction to ensure there is no inconsistency with our knowledge of business
Customers who are not local to the business	It does apply	Any non local customers who exceed the € 1,000 limit must produce verifiable ID and account for why they are cashing money so far from home

Risk factor	Explain why and how the factor does or does not apply	What procedures are in place to mange and mitigate the risks
New customers carrying out large transaction	Applies rarely	Must produce verifiable ID and account for the source of their money
Customers carrying out regular large transactions	Applies rarely	Must produce verifiable ID and account for the source of their money
Number of transactions below the amount requiring ID checks carried out by same customer within a short space of time	Applies rarely	Must produce verifiable ID and account for the source of their money
A number of customers sending payments to the same individual	Applies occasionally	Must find out reason why, and produce verifiable ID and account for source of their money
Non face-to-face customers	Does not apply	Must produce verifiable ID which has been certified and account for the source of their money
Situations where the source of funds not established		Reports to Amir Shahzad and if necessary to SOCA
Product/transaction types		
Complex or unusually large transaction	Not yet occurred	Must produce verifiable ID and account for the source of their money and there must be a good reason for complexity
Unusual patterns of transaction which have no apparent economic or visible lawful purpose		Report to Nominated Office and if necessary to SOCA

Risk factor	Explain why and how the factor does or does not apply	What procedures are in place to mange and mitigate the risks
Uncharacteristic transaction which are not in keeping with the customer's activities	Can occur	Report to Amir Shahzad to decide what steps to take
Sudden increase in business from existing customer.	Applies occasionally	Question why If answer does not stack up report to Amir Shahzad for further action
A high level of transaction for amounts just below the amount requiring ID checks	Can happen but easily spotted.	Lower limits for ID checks and report to Amir Shahzad for further action
Delivery channels		
Large cash transaction		Must produce verifiable ID and account for the source of their money
Occasional or one-off transaction as opposed to business relationships		Must produce verifiable ID and account for the source of their money
Business organization / geographical area of operation		
Large numbers of branches	2 branches	No extra risk
Large number of agents	Occasionally transfer funds for other MSBs	No extra risk
Geographical location of operation	Albert Drive is in Glasgow with a fluctuating and migrant population with attendant risks	Stringent ID checks in place and high awareness of suspicious activity factors
Number of employees	7 employees	Any employees will be well trained to recognize suspicious activity

Risk factor	Explain why and how the factor does or does not apply	What procedures are in place to mange and mitigate the risks
Money sent to or received from areas known to have high levels of criminality or terrorist activity	Applies to small number of money transfer transaction	ID documents on account file with verification. Ongoing monitoring of transaction to ensure there is no inconsistency with our knowledge of customer

Customer due diligence: policy on acceptable ID and satisfactory verification

Arrangements for Dealing with Money Transfer Transactions

All money transfer customers must register with company by providing passport or any other photo ID and a United Kingdom proof of address, and if customer does not have proof of address in own name, then they must fill in a third party proof of address form.

Procedure for customers conducting transaction in excess of € 1,000 and for all money transfers

1. Obtain name, address and date of birth of customer
2. Obtain two primary forms of ID or one primary plus one secondary form of ID

Primary forms of ID

a) Passport
b) Driving license
c) National ID card
d) Firearms certificate or shotgun license
e) ID card issued by the electoral office Northern Ireland

Secondary forms of ID include the following

a) Current bank statement
b) Current utility bill

Checks on ID evidence

- Check any photographs for likeness
- Check the date of birth compared to customer's apparent age
- Compare spelling of names and addresses on different identification documents
- Compare customer's signature with signature included in identification evidence
- Photocopy and check all ID evidences and record in account file

Arrangements for dealing with limited companies

Where the customer is a limited company you should identify the individuals you deal with and obtain details of the company's:-

- Registered number, corporate name and any trading names used;
- Registered address and any separate principal trading address; and
- Business activity

The details should be checked by either a search of the relevant company registry or by a copy of the company's certificate of incorporation. Record them in the account file.

Arrangement for dealing with cheque cashers

All cheque cashers should produce one primary form of ID plus one secondary form of ID

Primary forms of ID

a. Passport
b. Driving license
c. National ID card
d. Firearms certificate or shotgun license
e. ID card issued by the electoral office for Northern Ireland

Secondary forms of ID include the following

a. Current bank statement
b. Current utility bill

However there may be times when the company decides that a customer cannot reasonably meet the standard identification requirement and the provisions above cannot be met. The company may then accept as ID evidence, a letter or statement from an appropriate person who knows the individual that indicates that the person is who they say. An appropriate person is an independent professional person who is not a relative or friend of the individual, for example:-

- Family GP
- Accountant
- Solicitor
- Civil servant
- Teacher
- Notary
- Post office branch employee
- Employer

Customer due diligence: business relationships

A business relationship is an arrangement between the company and a customer that anticipates an ongoing relationship between the two parties. This can be a formal or an informal arrangement.

When a business relationship is identified then the company must obtain the following information to understand the purpose and intended nature of the relationship

- Details of the customer's business or employment
- Record of changes of address
- The expected source and origin of the funds to be used in the relationship
- Initial and ongoing source(s) of wealth or income
- The relationship between signatories and underlying beneficial owners
- The anticipated level and nature of the activity that is to be undertaken through the relationship.

ID and verification procedures are as above for transaction over €1,000 and money transfers.

Before commencing business, the company must decide if all the information of the customer and his/her sources of income make sense.

Ongoing monitoring of business relationships

Business relationships need to be monitored constantly by front line staff at each transaction and monthly by Amir Shahzad. Trigger events for possible money laundering and terrorist financing risks include

- A sudden increase in business from an existing customer
- Uncharacteristic transactions which are not in keeping with the customer's known activities

- Size and frequency of transaction is not consistent with the normal activities of this business
- The pattern of transactions has changed since the business relationship was established
- Peaks of activity at particular times
- Unfamiliar or untypical types of customer or transaction

Should any of the above trigger events occur then front line staff should query the customer if they feel it is appropriate, or if not, pass the information onto the Mr. Amir Shahzad, who should make appropriate enquiries as to what is happening.
Every month front line staff must review all client information to ensure that records are up to date.

From any customers that are considered high risk, Mr. Amir Shahzad should be informed of all transaction, in order that the company can act swiftly, if necessary.

Due Diligence measures when customer is another MSB

Where our customer is a money transmitter or currency exchange office, Hafiz Bros will apply an enhanced due diligence (EDD) due to higher risk of money laundering or terrorist financing.

Although the extent of EDD measures we will be applying will be based on the risk and circumstances of each individual case.

Because this kind of transaction or bulk transfer will consist of numbers of underlying transactions placed via MSB, we will monitor by;

- Asking MSB for number of underlying transactions of each bulk transfer made to you. This information will allow us to monitor that the number and average value of transaction is consistent with the level of business we anticipated when we began our business relationship with the same MSB. It will also give us an indication of risk, particularly where either the number of underlying transactions or the average transaction value is significantly above then what we expected. In such cases we will establish and record why it is different. Where we consider there is a risk we will make checks to ensure that customer (MSB) is carrying out customer due diligence. (And if a money transmitter obtaining complete information on the payer on your customers.). This will include checking the relevant records for specific transactions.
- By checking that they (MSBs) are registered and authorised with the FSA. This is because businesses carrying out money transmission that are not registered with or authorised by the FSA cannot lawfully provide payment services in the UK. If MSB is not properly registered we will decline the transaction.

EDD checks on transmissions to high risk countries-financial corridors:

Some remittances to high risk regions may be sent through other adjacent countries. These are sometimes referred to as financial corridors, where the beneficiary of a money transmission is in a high risk country and the money is being sent to an MSB outside that

country you should consider carrying out EDD checks on your customer. As these are high risk transactions you should also check that the beneficiary exists and confirm their identity. There is no definitive list of high risk and non cooperative jurisdictions may help you decide what you consider as high risk. You can find this information on the FATF website: www.fatf-gafi.org

Third party payments-

Third party payments are money transmissions, normally from the UK to another country, where the liability of the UK transmitter is offset or partly offset by the settlement of a liability of another person. This type of remittance and settlement involves two separate transactions, each of which requires the appropriate CDD or EDD.
Where the beneficiary is based in one country but the transfer of funds is made to another. It is sometimes described as third party pooling or cover payment. The arrangement may come about from the overseas MSB seeking to offset the money it is owed against settlement through payment of an invoice.

Under the MLRs the settlement of a debt by means of an offset payment to a different country from beneficiary is a separate transaction. In case of our customer is the overseas MSB who requests payment to be made to the third party, we will make sure our risk assessment includes indicators of risk and apply EDD on the overseas MSB. We will ask for and verifying additional documents, data or information to satisfy ourself that the identity of the overseas MSB is established. We will keep a full record for settlement accounts.
Where the payment is to be made against an invoice we will check that the document is genuine. Checks will include some or all of the following; depending of the level of risk identified:

- Is the name and address of the purchasing business correct
- Does the supplier exist
- Is the description of the goods credible
- Is the value of the goods realistic

Where we have any level of doubt about the invoice we will seek further evidence to check that it is genuine by getting supporting documentation such as movement certificates, shipping orders, packing lists and or bills of lading.

Money transmission from overseas into the UK- Inward remittances

These occur when a customer outside the UK wishes to carry out a transfer of funds to a beneficiary in the UK.
The location of the customer does not affect the MSBs need to perform CDD. We will apply CDD and where appropriate ongoing monitoring if an overseas customer deals directly with us in the UK.

Where the transfer of funds is sent to us from an overseas MSB we will treat them as our customer. Where we are receiving a bulk transfer (where the transfer represents a collection of underlying transactions) the situation is high risk. We will carry out EDD and obtain the number of underlying transactions of each bulk transfer made to us. This information will allow us to monitor that the number and average value of transactions is consistent with the anticipated level of activity when we began our business relationship. It will give us an indication of risk, particularly where the number of transactions or the average transactions value is significantly above what we expected. Where we are not satisfied with the reasons provided by our customer we will make a note of their explanation why the average transaction value has increased and check that our customer has carried out appropriate CDD. If it is necessary to make any further check before we decide whether to accept the transaction.

Where the transfer of funds is included in any sort of offset arrangement (where we pay the beneficiary from our own funds and debt owed to us by the overseas MSB is satisfied by a payment from them to third party at our instruction) this is a separate, potentially high risk transaction. We will perform CDD and if appropriate EDD checks on the person who has requested the third party payment. Based on our assessment of the risk this will include checking some specific transactions where we have instructed the overseas MSB to make a payment to a third party.

Monitoring the risk

What analysis is carried out in respect of:	
Number and size of transaction	all transaction analyzed daily
Customer profiles	Analyzed every 6 months
Patterns and fluctuation in trade	Analyzed monthly for all business Relationships and per transaction for High risk customers
Suspicious activity	all transaction analyzed for suspicious Activity intuitively by front line staff

Internal controls and communication

All public facing staff report directly to the Mr. Amir Shahzad. Public facing staff can make decision based upon experience, but if any doubt they must act through the Mr. Amir Shahzad.

As new information comes to light or new legislation is enacted, all staff will be briefed as soon as possible. Staff will be trained upon commencement of duties before dealing with the public and will have follow on training every 12 months.

Mr. Amir Shahzad will review and update risks and control every 6 months so that policies and procedures continue to effectively manage the risks.

All relevant information regarding policies or procedures will be communicated to relevant staff immediately.

Monitoring and Managing compliance

Mr. Amir Shahzad will ensure that appropriate monitoring processes and procedures are established and maintained. He will conduct regular audits and exercises that test that procedures are adhered to throughout the business.

Suspicious activity reporting

All suspicious activity should be reported to the Mr. Amir Shahzad.

It is essential to recognize the importance of front line staff awareness. Such factor as intuition, direct exposure to a customer face to face or on the telephone,
And the ability, through practical experience, to recognize transaction that does not seem to make sense for that customer, cannot be automated.

If staff is unsure whether consent for a transaction should be authorized, they should refer the matter to Mr. Amir Shahzad. If he is not obtainable, then staff must refuse transaction. A list of suspicious activity is listed below.

Mr. Amir Shahzad must decide if there are reasonable grounds to suspect money laundering. Before deciding to make a report to SOCA, Amir Shahzad will need to access all the business's relevant records with regards to the customer. He will need to consider the level of identity information held on the customer and any information held on his personal circumstances, and review transaction patterns and volume through the accounts.

If the Amir Shahzad decides not to make a report to SOCA, the reason for not doing so should be clearly documented and retained on file.

The following lists are not exhaustive but set out some of the main indications that a transaction is suspicious.

New customers and occasional or 'one-off' transaction:

- Checking identity is proving difficult
- The customer is reluctant to provide details of their identity
- There is no genuine reason for the customer using the services of an MSB
- A cash transaction is unusually large
- The customer is happy with a poor rate
- The customer is buying currency that does not fit with what is known about customer's destination
- The cash is in used notes and/or small denominations and the customer request currency in large denomination notes
- The customer will not disclose the source of cash
- The explanation for the business and/or the amounts involved are not credible
- A series of transaction are structured just below the regulatory threshold for due diligence identity checks
- The customer has made an unusual request for collection or delivery
- Transaction having no apparent purpose or which make no obvious financial sense, or which seem to involve unnecessary complexity
- Unnecessary routing of funds through third parties.

Regular and established customers

- The transaction is different from the normal business of the customer
- The size or frequency of the transaction is not consistent with the normal activities of the customer
- The pattern of transaction has changed since the business relationship was established

- Money transfer to high-risk jurisdiction without reasonable explanation which are not consistent with the customer's usual foreign business dealings
- Sudden increase in the frequency/value of transaction of a particular customer without reasonable explanation.

Example where customer identification issues have potential to indicate suspicious activity

- The customer refuses or appear reluctant to provide information requested
- There appears to be inconsistencies in the information provided by the customer
- The customer's area of residence is inconsistent with other profile details such as employment
- An address appears vague or unusual
- The supporting documentation does not add validity to the other information provided by the customer
- The customer is in a hurry to rush a transaction through, with promises to provide the information later.

Example of activity that might suggest to staff that there could be potential terrorist activity

- The customer is unable to satisfactory explain the source of income
- Frequent address changes
- Media reports on suspected or arrested terrorists or groups.

Cheque encashment

- look out for low and consective cheque number as fictious companies may be set up for the purpose of cheque fraud
- A number of different people cashing cheques all of which are drawn on the same company, with an unfamiliar name
- There will be an indication of benefit fraud where people try to cash their benefit cheques and produce wages slips as ID or vice-versa where they are cashing their wages cheque and produce paperwork regarding job seekers allowance as ID
- In some circumstances there may be an indication of fraudulently obtained cheques where a person has a number of cheques drawn on different individuals, rather than company cheques, claiming to have done work for these people
- A sudden increase in cheque values
- A customer wants to cash a cheque which was made payable to them weeks
- It appear that there has been something added to the cheque after the time of issue, e.g. different handwriting is evident, value digits appear squeezed in

Record -keeping

An account file must be set up for each customer with whom we have a business relationship, and for each large occasional transaction.

Copies of ID and verification must be kept on file and details of all transactions with that customer recorded.
All information used to set up a business relationship must be recorded and kept on the file.

Details of any suspicious activity, reports to Amir Shahzad and disclosures to SOCA must be kept on file.

Evidence of customer's identity record must be kept for five years beginning on the date on which the occasional transaction is completed or the business relationship ends.

Records of transaction (weather undertaken as occasional transactions or part of a business relationship) must be kept for five years beginning on the date on which the transaction is completed.

All other records must be kept for five years beginning on the date on which the business relationship ends.

Training

Training of all relevant employees within the company plays a critical role in the successful implementation of any risk based approach to managing potential money laundering risks. All relevant employees must be aware of and understand the legal and regulatory environment in which they operate.

All employees are to be trained before commencing face to face dealings with the public, and thereafter to receive follow-on training every month.

Training to enable employees to recognize and deal with suspicious transactions should include:-

- The identity and responsibilities of Mr. Amir Shahzad (or MLRO)
- The potential effect on the firm, its employees personally and its clients of any breach of the law

- The risks of money laundering and terrorist financing that the business faces
- The vulnerabilities of the business's products and services
- The policies and procedures that have put in place to reduce and manage the risks
- Customer due diligence measures, and, where relevant, procedures for monitoring customers' transactions
- How to recognize potential suspicious activity
- The procedures for making a report to Mr. Amir Shahzad.
- The circumstances when consent is to be sought and the procedure to follow
- Reference to industry guidance and other sources of information, e.g. Serious Organized Crime Agency, Financial Action Task Force.

All staff should be made aware that HMRC have the power to impose civil penalties on businesses that fail to comply with the requirement of the Regulations in respect of:

- Notification and registration requirements
- Customer due diligence measures
- Ongoing monitoring of a business relationship
- Enhanced customer due diligence and ongoing monitoring
- Record keeping
- Policies and procedures to prevent money laundering and terrorist financing
- Appointing a Amir Shahzad and internal reporting procedures
- Training of employees

There is no upper limit in regulation 42 on the amount of penalties. Penalties will be for an amount that is considered appropriate for the purposes of being effective, Proportionate and dissuasive.

Businesses can ask HMRC to review the decision to impose a penalty, or of the amount of the penalty, and the decisions to refuse or cancel registration. Penalty and the registration decisions can also be appealed to the VAT and Duties Tribunal.

MLR 2007 regulation 45 sets out the offence of failing to comply with the MLR 2007 obligations. **Conviction under the MLR 2007 can incur up to 20 years' imprisonment and/ or an unlimited fine**.

Appendix 1: ID Requirements For Send and Receive Money Transfers

Customers must present ID on all receive transactions and when sending transactions over 1000 Euro.

1.1- Receive Transaction 0-599.99

The following documents **on their own** can be accepted as proof of the customer's name and date and place of birth

- Passport and one evidence of proof of address.
- National Identity Card
- Current UK photo-card driving license
- Resident permit issued to EU nationals by Home Office
- Home Office IND Application Registration card and one evidence of proof of address.
- Immigration Forms SAL 1 and SAL 2 (issued before January 2002) and one evidence of proof of address.
- Certificate of Registration issued by the police or customs and one evidence of proof of address.

If customer does not have any of above documents, then they must provide 2 documents; 1 proving their name and 1 proving their address.
They must provide 1 document from List A and 1 document from List B

LIST A **Documents to prove NAME**	**LIST B** **Documents to prove address**
• Current full UK old style paper driving licence • Birth certificate • Building industry sub-contractors certificate issued by inland revenue • Inland revenue tax notification (P45 and P60 is not acceptable) • Firearms certificate • Police warrant card • UK forces ID card	• Utilities bill (no more than 3 months old) • Local authority tax bill (for current year) • Current full UK old style paper driving licence (if not used from List A) • Bank, building society or credit union statement or passbook (no more than 3 months old) containing current address • Most recent original mortgage statement from a recognized lender • Solicitor's letter confirming recent house purchase • Local council rent card or tenancy agreement

1.2- Send and Receive Transaction €1,000 - £1999.99

The following documents **on their own** can be accepted as proof of the customer's name and date and place of birth

- Passport
- National identity card
- Current Uk photo-card driving license
- Residence permit issued to EU nationals by home Office
- Home Office IND Application Registration card
- Immigration forms SAL1 and SAL2 (issued before January 2002)
- Certificate of Registration issued by the police or customs

If customer does not have any of the above documents, then they must provide 2 documents; 1 proving their name and 1 proving their address.

They must provide 1 document from list A and 1 document from List B

LIST A **Documents to prove NAME**	**LIST B** **Documents to prove address**
• Current full UK old style paper driving licence • Birth certificate • Building industry sub-contractors certificate issued by inland revenue • Inland revenue tax notification (P45 and P60 is not acceptable) • Firearms certificate • Police warrant card • UK forces ID card	• Utilities bill (no more than 3 months old) • Local authority tax bill (for current year) • Current full UK old style paper driving licence (if not used from List A) • Bank, building society or credit union statement or passbook (no more than 3 months old) containing current address • Most recent original mortgage statement from a recognized lender • Solicitor's letter confirming recent house purchase • Local council rent card or tenancy agreement • Letter from a hostel manager confirming temporary residence • Letter from the matron of a nursing home or residential home

1.3- Send and Receive Transaction £2,000 - £4,999.99

For transaction over £2,000 customers must verify their full name, country, date of birth and address.

The must provide 1 document from List A and 1 document from List B

LIST A **Documents to prove NAME**	**LIST B** **Documents to prove address**
• Passport • National identity card • Current UK Photo-card Driving licence (full or provisional) • Residence permit issued to EU nationals by Home Office • Home office IND card • Immigration forms SAL1 and SAL2 (issued before January 2002) • Certificate of registration issued by the police or customs • Current full UK old style paper driving licence • Birth certificate • Building industry sub-contractors certificate issued by inland revenue • Inland revenue tax notification (P45 and P60 is not acceptable) • Firearms certificate • Police warrant card • UK forces ID card	• Utilities bill (no more than 3 months old) • Local authority tax bill (for current year) • Current full UK old style paper driving licence (if not used from List A) • Bank, building society or credit union statement or passbook (no more than 3 months old) containing current address • Most recent original mortgage statement from a recognized lender • Solicitor's letter confirming recent house purchase • Local council rent card or tenancy agreement • Letter from a hostel manager confirming temporary residence Letter from the matron of a nursing home or residential home

1.4- Send and Receive Transaction £5,000 - €14,999.99

For transaction over £5,000 customers must verify their full name, country, date of birth and address.

On payments below €15,000 you should seek evidence on the source of funds when

- The customer has presented cash in payment for the transaction, five times the size of an average transaction for your business.
- The customer has paid for the transaction by cheque or debit card, ten times the size of an average transaction.

Where a person is sending money for someone else and information such as wage slip or bank statement is not available you should consider obtaining and keeping a signed certificate/ declaration by the customer about the source of funds-checked against a proof of ID documents, such as a passport.

Where you have to accept a declaration it is sensible to include details of something that can itself be checked this could be contact details for each person named in the declaration. Every case will be different.

Where funds have come from a bank account, you can take some re-assurance that the customer's ID and personal details have been checked by another regulated business in the UK or another country which is prepared to provide the customer with account facilities. However, you should not be satisfied just because the money has come from the customer's bank account that the source of funds is lawful. You should establish how the money got into the bank and where the money came from, is it wages, a cheque form a family member, payment for sale of personal items etc

The must provide 1 document from List A and 1 document from List B

LIST A **Documents to prove NAME**	**LIST B** **Documents to prove address**
• Passport • National identity card • Current UK Photo-card Driving licence (full or provisional) • Residence permit issued to EU nationals by Home Office • Home office IND card • Immigration forms SAL1 and SAL2 (issued before January 2002) • Certificate of registration issued by the police or customs	• Utilities bill (no more than 3 months old) • Local authority tax bill (for current year) • Current full UK old style paper driving licence (if not used from List A) • Bank, building society or credit union statement or passbook (no more than 3 months old) containing current address

• Current full UK old style paper driving licence • Birth certificate • Building industry sub-contractors certificate issued by inland revenue • Inland revenue tax notification (P45 and P60 is not acceptable) • Firearms certificate • Police warrant card • UK forces ID card	• Most recent original mortgage statement from a recognized lender • Solicitor's letter confirming recent house purchase • Local council rent card or tenancy agreement • Letter from a hostel manager confirming temporary residence • Letter from the matron of a nursing home or residential home

When to check source of funds in one off transactions below €15000

The way customers present themselves and the source of their funds are key indicators of potential risk. Through our risk based approach (RBA), we will be able to show that we have taken all reasonable steps to satisfy that the transaction is not suspicious, including, where appropriate, identifying the source of funds.

This is best done through independent documents or data provided by the customer, for example, a payslip or bank statement. The documents required and the level of checks will depend on the risks to our business.

Where a person is sending money for someone else and information such as wage slip or bank statement is not available you should consider obtaining and keeping a signed certificate/ declaration by the customer about the source of funds-checked against a proof of ID documents, such as a passport.

Example 1- if a customer claims he is transmitting money on behalf of a group of friends will consider writing down details of the names and addresses of the friends and the amounts to be transmitted.
Where we have to accept a declaration it is sensible to include details of something that can itself be checked this could be contact details for each person named in the declaration. Every case will be different.
Example 2- the customer claims the cash is from the sale of car. We will include details of the car, its registration number and the date of sale.

On payments below €15,000, we will seek evidence on the source of funds when

- The customer has presented cash in payment for the transaction, five times the size of an average transaction for your business.

- The customer has paid for the transaction by cheque or debit card, ten times the size of an average (monthly) transaction.

Where the number of such transactions exceeds 5%, we may limit the source of funds checks to the top 5% of transactions by value.

Where funds have come from a bank account, we can take some re-assurance that the customer's ID and personal details have been checked by another regulated business in the UK or another country which is prepared to provide the customer with account facilities. However, we will not be satisfied just because the money has come from the customer's bank account that the source of funds is lawful and we will establish how the money got into the bank and where the money came from, is it wages, a cheque form a family member, payment for sale of personal items etc.

Where we have any suspicion that the transaction relates to money laundering and or terrorist financing we will send a suspicious activity repost (SAR) to the serious organised crime agency (SOCA) and get consent from them to continue with the transaction. If our suspicion is raised after the transaction is completed we will send a SAR at the earliest opportunity.