Remit Continental

White House, Wollaton Street, Nottingham, United Kingdom, NG1 5GF

Tel: 07952262997

Email: lamin.22001@gmail.com

Anti-Money Laundering Policies and Procedures Manual

Managing financial crime and money laundering risks

Our obligations as a HMRC regulated company

Version: 1.0

Senior Management Declaration

Date: 01/03/2019

I, the undersigned, being the senior manager of Remit Continental hereby endorse the policies which have been set down in this compliance policy manual.

The manual covers the following areas:

- The financial crime risk to our business
- UK Payment Services Regulations
- Financial Ombudsman Service – its role in dealing with complaints
- Conduct of Business
- Our complaints policy
- Data protection policy

These policies may be subject to amendment or addition as required for legislative and business operational reasons.

We confirm that it is the responsibility of the Money Laundering Reporting Officer to monitor compliance with all of the policy issues mentioned above.

As and when required, the MLRO will make a report to senior management about any operational or strategic issues for the company which arise as a result of the policies set down in this manual.

We also confirm that it is our company policy that all members of staff (and agents, if applicable) must read and confirm in writing their understanding of the policies set down here – and their personal responsibilities arising from them.

In the event of staff failing to comply with the policies in this manual, this will be regarded as a material breach in contractual obligations and may lead to disciplinary proceedings.

Signed by:

Lamin Suwareh

…….

Contents

Revision History

Ver No.	Date	Author	Description
1.00	March 2019	Consultant	Initial version

Section 1 - Our Company

Company Details

Company Registered Name	SHIPPERSWORLD LIMITED
Company Trading Name	Remit Continental
Registered Business Address	White House, Wollaton Street, Nottingham, United Kingdom, NG1 5GF
Company Registration Number	**10835376**
Head Office Address	White House, Wollaton Street, Nottingham, United Kingdom, NG1 5GF
Main Office Telephone	07852262997
Main Office Facsimile	
Company Owners	Lamin Suwareh
Company Directors	Lamin Suwareh
Nominated Officer	
Contact Number	07852262997
Email Address	
HMRC Registration Details	
Date Of First Registration	
Date of Renewal	
Registration Number	
Financial Conduct Authority Registration Number	

The Company is a registered member of the UK Money Transmitters Association and recommends that UK based organisations with which we have a relationship should join.

Payment services include:

Retail money remittance services: A money transfer service offered to a sending customer whereby a remittance payment is made to a named receiving customer, often in another country, and where the transaction size is less than £5,000

Wholesale payment services: A money transfer service where the Money Transfer Principle is acting as an Intermediary Payment Service Provider (IPSP) and/or foreign currency provider for an originating MSB or Payments Institution

High value money transfer services: A money transfer service offered to a sending customer whereby a payment is made to a named receiving customer, often in another country, and where the transaction size is £5,000 or more.

Foreign Exchange plus onward transfer: Provision of currency exchange for a corporate or private client plus onward transmission of funds for a payment purpose (e.g. purchase of property/settlement of an invoice)

Our Services

Retail money remittance services	✓
High value money transfer services	✓

Section 2 – Tackling the Financial Crime risk

What the UK law requires – and penalties for non compliance

Within the broader financial crime agenda, we have identified money laundering, terrorist financing, sanctions list compliance, asset freeze issues and fraud prevention as the particular issues for our business, but we recognise that financial crime is an ever-evolving challenge and that new kinds of financial crime threat are always arising, and will need to be addressed.

What is money laundering?

Money Laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for 'clean' money or other assets with no obvious link to their criminal origins. Money Laundering can take many forms including:

- Handling the proceeds of crimes (e.g. cash) generated by such activities as theft, drug smuggling, fraud and tax evasion
- Being knowingly involved in any way with criminal property
- Entering into arrangements to facilitate laundering criminal property
- Investing the proceeds of crime (e.g. cash) in another financial product (e.g. a money transfer)
- Investing the proceeds of crime into the acquisition of property/assets

What are the criminal offences?

The Proceeds of Crime Act 2002 (POCA) as amended by the Serious Crime Act 2015

POCA Part 7 sets out the primary offences relating to money laundering. There are three principal money laundering offences covering criminal activity and four related money-laundering offences. These are shown in the table below:

No	An offence is committed under POCA when a person
1	conceals, disguises, converts, transfers or removes from the jurisdiction property which is, or represents, the proceeds of crime which the person knows or suspects represents the proceeds of crime (POCA section 327) But an offence has not been committed under this section if - * he makes an authorised disclosure under section 338 and has the appropriate consent or he intended to make such a disclosure but had a reasonable excuse for not doing so or the act he has done is done in carrying out a function he has done relating to the enforcement of any provision of this Act or of any other enactment relating to

	criminal conduct or benefitting from criminal conduct.
2	enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person (POCA section 328) But an offence has not been committed under this section if - (*same as above)
3	acquires, uses or has possession of property which he knows or suspects represents the proceeds of crime (POCA section 329) But an offence has not been committed under this section if - (*same as above) ** with the addition of that he acquired or used or had possession of the property for adequate consideration;
4	fails to disclose to the MLRO (in the regulated sector), knowing or suspecting or having reasonable grounds for knowing or suspecting that another person is engaged in money laundering – this applies to any individual at whatever level (employee, manager, director) (POCA section 330) But an offence has not been committed under this section if – he has a reasonable excuse for not disclosing the information or other matter or he is a professional legal adviser and the information or other matter came to him in privileged circumstances or that he does not know or suspect that another person is engaged in money laundering or he has not been provided by his employer with such training as is specified by the Secretary of State by order for the purposes of this section.
5	fails to disclose to NCA (in the regulated sector), knowing or suspecting or having reasonable grounds for knowing or suspecting that another person is engaged in money laundering or terrorist funding – this applies to the MLRO or sole proprietor of a business (POCA section 330 But an offence has not been committed under this section if he has a reasonable excuse for not disclosing the information or other matter.
6	A person commits an offence if – he knows or suspects that another person is engaged in money laundering or that the information or other matter on which his knowledge or suspicion is based came to him in consequence of a disclosure made under section 337 or 338 of the Act, or that he does not make the required disclosure as soon as is practicable after the information or other matter comes to him. But an offence has not been committed under this section if he has a reasonable excuse for not disclosing the information or other matter
7	A person commits an offence if – He knows or suspects that a disclosure falling within section 337 or 338 of the Act has been made, and he makes a disclosure which is likely to prejudice any investigation which might be conducted following the disclosure.

	But an offence has not been committed under this section if – he did not know or suspect that the disclosure was likely to be prejudicial or the disclosure is made in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct or that he is a professional legal adviser and the disclosure made was to a client of the professional legal adviser in connection with the giving by the adviser of legal advice to the client or to any person in connection with legal proceedings or contemplated legal proceedings.

Penalties: A person found guilty of an offence under sections 327, 328 or 329 is liable to on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or on conviction on indictment, to imprisonment for a term not exceeding 14 years or to a fine or to both.

A person found guilty of an offence under sections 330, 331, 332 or 333 is liable to on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Regulator: National Crime Agency

The Terrorism Acts (2000) as amended by the Anti-Terrorism, Crime and Security Act 2001

These acts set out the primary offences relating to the funding of terrorism. The Acts deal with suspicion of terrorist financing and requires firms in the regulated sectors to report where there are grounds to know or suspect offences relating to terrorist financing. These offences include:

- fundraising for the purpose of terrorism (section 15)
- using or possessing money for the purposes of terrorism (section 16)
- involvement in funding arrangements (section 17); and
- money laundering (facilitating the retention or control of money which is destined for, or is the proceeds of, terrorism) (section 18)

This obligation is significantly different from that under POCA – as it does not just cover "proceeds" of crime, but all funds, regardless of their origin.

Penalties: Conviction for any of the above offences can incur up to 14 years imprisonment and/or an unlimited fine. Failure to disclose the belief or suspicion that someone has committed any of the offences above can incur up to five years imprisonment and/fines. It is likewise an offence to 'tip off' a suspect that a disclosure has been made of suspicion of terrorist funding or of a subsequent investigation. This offence carries a penalty of up to two years in prison and/or unlimited fines.

Regulator: Responsibility for dealing with criminal breaches of the Terrorism Act lies with the police but businesses which follow guidance issued by HMRC are likely to have protection in a court of law.

Counter Terrorism Act 2008 Schedule 7

This schedule provides new powers for the Treasury to apply financial restrictions in respect of non-EEA countries because of the risk posed by money laundering or terrorist financing, either:

- in accordance with a recommendation of the Financial Action Task Force (see www.fatf-gafi.org)
- or on its own initiative
- if such activity poses a significant risk to the UK's national interests

The provisions of the act allow HM Treasury to impose on firms:

- stricter requirements for Customer Due Diligence – identifying clients, beneficial owners and the nature of business relationships
- stricter requirements for ongoing monitoring of transactions
- a requirement to undertake systematic reporting of all transactions with designated entities
- a requirement to limit or stop business with designated entities

Companies which wish to be notified about Orders issued under the CTA 2008 should sign up at the following address- http://www.hm-treasury.gov.uk/fin_crime_mailinglist.htm

Penalties: There are civil and criminal sanctions for failure to comply with the Counter Terrorism Act 2008 Schedule 7. These include unlimited fines and imprisonment for up to two years.

Regulator: HM Revenue and Customs

Financial Sanctions

These are normally used by the international community for one or more of the following reasons:

- To encourage a change in the behaviour of a target country or regime
- To apply pressure on a target country or regime to comply with set objectives
- As an enforcement tool when international peace and security has been threatened and diplomatic efforts have failed
- To prevent and suppress the financing of terrorists and terrorist acts

In the UK, HM Treasury is responsible for publishing the list of individuals/groups to which financial sanctions apply and for monitoring compliance. The following sanctions regimes are

presently in place: Al Qaida and Taliban, Afghanistan, Belarus, Burma/Myanmar, Democratic Republic of the Congo , Egypt , Eritrea, Federal Republic of Yugoslavia & Serbia, Iran, Iraq, Ivory Coast, Lebanon, Liberia, Libya, North Korea, Republic of Guinea, Somalia, Sudan, Syria, Terrorism and terrorist financing, Tunisia and Zimbabwe.

The HM Treasury consolidated Sanctions List is available from: http://www.hm-treasury.gov.uk/fin_crime_mailinglist.htm

Penalties: It is a criminal offence to make funds available to individuals/groups on the HMT Financial Sanctions list. This includes dealing directly with them or through intermediaries (such as lawyers or accountants). The maximum term of imprisonment for criminal contravention of the Financial Sanctions regime is currently seven years.

Regulator: Asset Freezing Unit, HM Treasury

Money Laundering Regulations

The secondary legislation is specific to money laundering activity. They make it a separate offence for relevant businesses not to have systems and procedures in place to combat money laundering.

The **2007 Money Laundering Regulations** place a range of obligations on MSB's:

- Requirement to be registered as an MSB with the designated regulator (HMRC)
- Requirement for those who run money transfer companies to satisfy a 'fit and proper' test – (those not judged satisfactory will be prohibited from running money service businesses)
- Customer 'due diligence' requirements – obligation to identify the customer and, above certain thresholds, verify the customer from an independent data source
- Simplified due diligence is allowed in situations where the customer is another financial institution (e.g. MSB to MSB transfers) – however, there are ongoing monitoring obligations for the intermediary MSB
- Special due diligence obligations in three specific situations:
    i) for non face to face customers,
    ii) customers who may be 'politically exposed' or
    iii) customers who may present a higher risk of money laundering
- Beneficial ownership – obligations to understand who are the underlying individuals who make financial gains from business relationships or transactions
- When a business relationship has been established, requirements to establish customer source of funds/purpose of transaction, also on going monitoring obligations
- To keep business records for 5 years
- To have internal reporting mechanisms to allow reporting of suspicious activity
- To appoint a Nominated Officer (sometimes known as the Money Laundering Reporting Officer)
- To train staff on the law and training in how to recognise suspicious activity
- To take a 'risk based approach' to all aspects of the AML policies for the business

Penalties: Criminal conviction under the MLR's can incur up to 2 years imprisonment. HMRC has powers to impose civil penalties (fines) on business that fail to comply with the MLR's in respect of:

- notification and registration requirements
- customer due diligence measures
- record-keeping
- policies and procedures to forestall and prevent money laundering and terrorist financing
- disclosures under Part 7 of the Proceeds of Crime Act
- training of employees

Regulator: HM Revenue and Customs. Fines will be for an amount that is considered by the supervisory authority appropriate for the purposes of being 'effective, proportionate and dissuasive'.

EU Payments Regulation

Implemented into UK law as the Transfer of Funds (information on the payer) Regulations 2007) requires Money Transfer Businesses to obtain customer's information when undertaking the transfer of customer's funds into and out of the UK. This means:

Step 1 – Collect and record customer information

The MSB must collect and record the sending customer's name and address. Each transaction must be given a unique transaction number if the customer does not have an account. The information collected is known as Complete Information on the Payer (CIP). As an alternative to requesting the customer's address, MSB can request date and place of birth or a national identity number (e.g. passport or National Insurance number).

Step 2 – Verify the customer information provided

If the transfer of funds is for an amount of €1,000 or more (approx. £800), the company must verify the customer's information from a reliable independent source (e.g. passport or a driving licence). The company must verify the customer information for transactions below €1,000 if money laundering is suspected.

Verification of the information provided is also required where there are 'linked' transactions which exceed €1,000 (that is when a customer appears to be keeping a series of transactions deliberately below the €1,000 threshold to avoid the requirement to provide ID). Transactions would also be linked if several customers were sending to the same receiving customer or the same receiving address.

Step 3 – Send the information which has been gathered to the payout service provider in the payout country

If the transfer of funds is to a destination outside the EU, complete payer information (full CIP) must accompany the transfer.

Full CIP may be defined as one of the following combinations of information:

- Customer name plus address plus transaction number
- Customer name plus date and place of birth plus transaction number
- Customer name plus customer ID number plus transaction number
- Customer name plus customer number

The key requirement is that enough information should be sent to the PSP of the payee so that the transaction is traceable back to the originating customer.

In the event that a UK based MSB is receiving transactions sent from abroad (from countries outside the EU), then the MSB must ensure that they are receiving full CIP for each transaction - if they do not receive this information from the sending payment service provider, then they should cancel the business relationship and consider a report to the National Crime Agency.

Penalties: Companies which are failing to comply with the Payments Regulation may be liable to the same penalties as for non compliance with the Money Laundering regulations (i.e. fines and/or criminal prosecution). HMRC have indicated that businesses which are consistently not complying now with the Payments Regulation may be at risk of failing the 'fit and proper' test.

Regulator: HM Revenue and Customs. Fines will be for an amount that is considered by the supervisory authority appropriate for the purposes of being 'effective, proportionate and dissuasive'.

What is Fraud?

No precise legal definition of fraud exists; many of the offences referred to as fraud are covered by the Theft Acts in England and Wales, and under Common Law in Scotland. The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. Other offences are created by more sector-specific laws such as those that prohibit corruption or create offences related to companies or financial services, for example.

For practical purposes fraud may be defined as the use of deception with the intention of obtaining an advantage, avoiding an obligation, or causing loss to another party. This most often occurs in the context of a relationship with a customer, client, or colleague on an individual or organisational

basis.

There are four basic ingredients which are necessary for a fraud to occur:

- People to carry out the fraud
- Assets to acquire
- Intent to commit the fraud
- Opportunity

While some people would never contemplate perpetrating a fraud, others might do so if they think they can get away with it. Fraudsters are usually alert, plausible and calculating. You can deter a fraudster who might want to take advantage of you personally, or your business, by being alert to the possibilities. Alertness and effective controls will increase the chances of being caught and will thus act as a deterrent.

In business some frauds arise because of a system weakness, such as a lack of proper control over placing of purchase orders. Other frauds are the result of failures to follow proper control procedures. It may be carelessness in carrying out a check. It may be that too much trust has been placed in one individual with no effective separation of duties. Frauds which result from collusion may be more difficult to prevent. A computer can be instrumental in the perpetration of the fraud because of the absence of human review of transactions. The lack of human involvement may allow transactions to be processed which would have been queried in a manual system.

An organisation can therefore be exposed to the risk of fraud in a number of different ways. For the purpose of this guide we can divide fraud into three categories:

Internal fraud: This is fraud perpetrated by individuals inside the organisation and is most often carried out by staff who have access to liquid or moveable assets, such as cash or stocks. It is likely that the risk of fraud and its scale will increase if the member of staff is able to conceal the irregularities by also having access to accounting records. It may be opportunistic, though it may also be planned and committed over a long period.

External fraud: This is fraud which is perpetrated by individuals outside the organisation and covers activities such as theft, deception and computer hacking. It is very often committed as a result of inadequate safeguards.

Collusion: This type of fraud involves two or more parties, either both internal, or internal and external, working together. This type of fraud can be difficult to detect as controls may at first appear to be working satisfactorily.

The pages that follow illustrate real cases and identify topical scams. Advice, based on this experience suggests ways of preventing fraud happening to you.

Types of Fraud

Frauds can be categorised by the type of victim involved. The most common groups of victims encountered by investigators include:

- Investors
- Creditors
- Businesses
- Banks or other financial institutions
- Central or local government
- Fraud by manipulating financial markets

Frauds can also be categorised by the technique or activity used by the fraudster. These include:

- Advance fee frauds
- Bogus invoices
- Computer hacking of information or property
- Corruption and bribery
- Counterfeiting, forgery, or copyright abuse
- Credit Card fraud
- False Accounting - manipulation of accounts and accounting records
- Fraudulent bankruptcy - exploitation of cross-border corporate structures
- Insurance fraud
- Internet online scams - auctions, credit card purchases, investment scams
- Investment fraud
- Long Firm fraud
- Misappropriation of assets
- Money laundering
- Mortgage Fraud
- Payroll fraud
- Principal agents - failure of systems to restrict key individuals
- Pyramid schemes
- Unsolicited letter frauds

For update information on issues related to fraud, reference should be made to the Fraud Reduction website published by the National Working Group on Fraud on behalf of the UK Association of Chief Police Officers (ACPO). This is available at: www.fraud-stoppers.info.

Regulatory Guidance

Firms which follow 'relevant guidance' issued by the appropriate regulator will have a defence against any accusation of non-compliance with the law. For the purposes of money transfer businesses, companies which comply with guidance issue by HM Revenue and Customs will have protection in relation to 2007 Money Laundering Regulations, EU Payments Regulation, Terrorism Act 2000, Counter Terrorism Act 2007, Section 7 and the Proceeds of Crime Act 2002.

HMRC has issued guidance (MLR8) which was formalised with effect from 12/09/2008. MLR8 is available on the HMRC website: http://www.hmrc.gov.uk/mlr/mlr_msb.pdf

Companies should also review guidance issued by the Joint Money Laundering Steering Group to firms regulated by the FCA for AML. This is available at: www.jmlsg.org.uk.

What does UK Financial Crime legislation mean for us?

The combined objective of all legislation and regulation is to make it difficult for criminals and terrorists to operate through the international financial system.

The combined impact of these laws for our company is to make it an offence for any employee, agent or agent employee to provide assistance to another person to obtain, conceal, retain or invest proceeds of crime if the employee, agent or agent employee knows or suspects or, in some cases, (i.e. terrorist funding or the offences of concealing or transferring), should have known or suspected, that the other person has been engaged in, or has benefited from, criminal conduct or, alternatively, is involved in assisting terrorist activity.

Risk Assessment of our Payments Business

The 2007 Money Laundering Regulations require that each MSB must adopt a new 'risk based approach' to its customers, products and business practices.

Risk may be established both on the basis of objective criteria and subjective criteria. A 'risk rating' is given to each criterion.

Grading	Risk Ranking
1	Low Risk
2	Low - Medium risk
3	Medium Risk
4	Medium – High Risk
5	High Risk

Below are summarised some of the operational risks that have been assessed and identified within our business.

Country Risk - Areas of Operation

We use information from Transparency International's Corruption Perception Index (CPI) 2015, the HM Treasury Consolidated List of Sanctioned Countries and the FATF public statement of High-risk and non-cooperative jurisdictions of February 2015 to assess the risk of countries we either operate or likely to operate in as listed below.

The risk scores determined using this information indicates the levels at which Enhanced Due Diligence is followed outside normal operational factors. The table below shows the mapping of these risk factors to risk scores

Country	Risk Factors	Risk Factor Score (Rank)	Risk Score	Services provided To or From
United Kingdom	· Transparency International Corruption ranking out of 180 countries	11	2	Yes
	· FATF identified country with weak AML/CFT regimes	No		
	· Country on HMT consolidated list of Sanctions targets	No		
Gambia	· Transparency International Corruption ranking out of 180 countries	93	3	Yes
	· FATF identified country with weak AML/CFT regimes	No		
Senegal	· Transparency International Corruption ranking out of 180 countries · FATF identified country with weak AML/CFT regimes	67 No	2	Yes
Nigeria	.Transparency International Corruption ranking out of 180 Countries .FATF identified country with weak AML/CFT regimes	144 No	3	yes

It is company policy to consider and take note of any reports produced by the Financial Action Task Force (FATF) on ML/TF risks in relation to particular countries where available. These reports are available at: www.fatf-gafi.org.

The FATF assessments are used as an indicator – they enable us to determine when we should place closer scrutiny on the destination for payment transactions. This does not mean that customers who send to these locations are transacting illegally or are suspected of illegal activity.

Products

Our company licences enable the business to offer all related services subject to regulatory terms and conditions being met. Our business may add in the future service listed below unless indicated by a value then the activity is not carried out.

Product	% of total business	Risk Ranking
Retail money remittance services	99.71%	1
High value money transfer services	0.29%	1

Transactions

How are they processed	% of total business	Risk Ranking
'Face to Face'	14%	1
'Non Face to Face'	86%	4
Size of Transaction	% of total business	Risk Ranking
Less than or equal to £1,000	88.85%	1
Between £1001 to £5,000	10.86%	3
Above £5,000	0.29%	5
How are they funded?	% of total business	Risk Ranking
Online Payment	92.70%	1
Deposit-to-Bank	0%	1
Cash transaction	7.30%	3

Customers

Retail Customers	% of total business	Risk Ranking
Business relationship customers	99.92%	1

Occasional customers	0.07%	2
One off customers	0.01%	4
Corporate Customers	% of total business	Risk Ranking
Business relationship customers	0%	1
Occasional customers	0%	n/a
One off customers	0%	n/a

ID Provided (retail customers/directors/owners of Payment Institutions)

Type of ID Provided	% of Customers	Risk Ranking
EU/UK Passport/driving licence (photo card) plus proof of address	94%	1
Non EU Passport plus leave to remain in UK plus proof of address	6%	3
Any other form of other ID ('unusual ID')	0%	5

Other characteristics

	% of Customers	Risk ranking
Customer is a PEP	N/A	5
Customer is non face to face (first transaction)	N/A	5
Customer is sanctions list match	N/A	5
Customer is sending more money than would be justified by given employment status	N/A	5

Customer is sending money on behalf of a group of other people	N/A	5
Customer is otherwise behaving in an unusual way which may be suspicious (see below)	N/A	5

Unusual Activity which may be suspicious

- One off transactions above £5,000 – the customer is processing a large transaction
- Split transactions – the customer is attempting to split a large transaction into several smaller transactions to avoid obligations to provide proof of source of funds
- New customers carrying out large transactions (as opposed to regular customers)
- Regular customer is processing transactions which do match the profile of previous transactions
- Customers processing transactions who do not appear to be legitimate owners of the funds (i.e. students processing large transactions)
- Customers involved in transactions which appear to be linked to transactions processed by other customers
- Customers who cannot provide ID when requested or who provide false ID
- Customers who cannot justify source of funds when requested
- Customer is not local to the business, (but not a tourist)
- Customer is paying in used notes or in small denominations
- Transactions where customer is accompanied by another person who tells him what to do
- Transactions which involve large numbers of 500 Euro notes
- The customer operates in a high-risk area dealing in lots of cash: restaurants, pubs, casinos, tax firms, beauty salons and amusement arcades
- Customers who are not native to the country they are sending money to (i.e. English people)
- Customer is processing large volume transactions in cash, (rather than sending funds from his personal bank account)

Risk Matrix – high, medium and low risk customers

It is the responsibility of the Money Laundering Reporting Officer (MLRO) to oversee all transactions which are processed. They will focus attention on high risk transactions (transactions with risk rating of 5).

Please note, the list below is not exhaustive:

Risk Ranking	Summary of red flags	Action of MLRO
5	Sanctions list match	Freeze transaction and consider a report to NCA/HM Treasury
5	Customer previously reported to NCA and NCA withheld consent	Freeze transaction and report to NCA
5	Customer provides fake ID	Freeze transaction and report to NCA
5	Customer previously reported to NCA and consent given	Freeze transaction pending enhanced due diligence check
5	Single transaction above £5,000 where no source of funds established	EDD required
5	Retail customer has sent cash transactions above £12, 000 (approx. €15,000) within 12 month period (and no source of funds established)	EDD required
5	Customer is a PEP	EDD required
5	Customer uses unusual ID to identify himself	EDD required
5	Customer is processing level of transactions incompatible with work status	EDD required
5	Customer is demonstrating unusual behaviour (which may be suspicious)	EDD required
5	Customer is an MSB who is transacting outside anticipated parameters set at start of business relationship	EDD required
5	Customer is an MSB and ownership is not clear/MSB not able to verify ownership	EDD required
4 or less		No action required

What is Enhanced Due Diligence (EDD)?

The business needs to establish more information about the customer and/or transaction. This means that the customer should be asked to provide:

- more ID information (i.e. further proofs of ID/proof of address)
- more information about the source of funds for the transaction (including possibly a written proof of source of funds) – See Appendix 1 for the Customer Risk Assessment Form
- more information on the purpose of the transaction

In the event that the customer cannot provide more information, or provides information which gives rise to suspicion, then the MLRO will freeze the transaction and will make a report to the National Crime Agency.

Policies for dealing with the financial crime risk to our business

Part A - Company approach, Internal Systems and Controls

i) Statement of company principles in relation to dealing with financial crime

'The management of Remit Continental have agreed this statement of high level principles at their meeting on 1st march 2020.

Senior management of the company recognises that a commitment to the highest standards in relation to issues of anti-financial crime procedures is fundamental to the successful operation of the business.

We further recognise that it is our responsibility to create the framework in which the successful implementation of anti-financial crime policies within the business can take place.

We recognise and endorse the need for a strong and rigorous system of controls to manage the possible threats to our business associated with financial crime.

We further recognise our obligation to monitor all the transactions which pass through our business to be on the lookout for suspicious activity which may indicate criminal behaviour.

We hereby affirm:

- *the re-confirmation of Lamin Suwareh to the position of MLRO – he is the person to who all internal suspicious activity reports should be directed*
- *the obligation of the MLRO to make a report when required to senior management on financial crimes issues and the business*
- *the company's commitment to train all staff in anti-financial crime procedures*
- *the obligation on all staff to remain aware of the potential for financial crime to occur within the business, and (if they have suspicions), their personal obligation to report their suspicions to the MLRO without delay*

The company recognises and endorses the risk based analysis of the financial products, customers and geographic areas of operation which is included in this manual.

The company endorses the operational policies to be followed by staff to address the threat of Financial Crime to our business. This includes information on the customer due diligence, transaction processing, transaction monitoring plus other important issues.

Senior managers confirm that they will keep issues of compliance under ongoing review, but commit, as a minimum, to review the company's policies manual within 12 months' time at the latest.

Signed by:

…….. .
Lamin Suwareh

ii) Nominated Officer (Money Laundering Reporting Officer)

The Money Laundering Reporting Officer (also known as the nominated officer) contact information is:Lamin Suwareh Tel: 07852262997 email: lamin.22001@gmail.com

The MLRO is the focal point within the company for the oversight of all activity related to anti-financial crime issues. Their responsibilities include:

- reviewing all new laws and deciding how they impact on the operational process of the company
- preparing a written procedures manual and making it available to all staff and other stakeholders
- making sure appropriate due diligence is carried out on customers and business partners
- receiving internal Suspicious Activity Reports (SARs) from staff
- deciding which internal SAR's need to be reported on to NCA
- recording all decisions relating to SARs appropriately
- ensuring staff receive anti-financial crime training when they join and that the receive regular refresher training
- monitoring business relationships and recording reviews and decisions taken about continuing or terminating trading activity with particular customers
- making sure that all business records are kept for at least five years from the date of the last customer transaction

iii) Staff Training

Training is given to all staff members upon commencement of money transfer service and on regular occasions afterwards (at least once a year). Training covers the following issues:

- The law relating to financial crime (MLR's/MLR8, etc)
- Risks associated with the financial crime threat to the company
- Identity and responsibilities of the MLRO
- Internal policies and procedures put in place
- Customer Due Diligence/Enhanced due diligence monitoring measures
- Suspicious activity – what to look out for
- How to submit an internal Suspicious Activity Report to the MLRO
- Record-keeping requirements

The MLRO will keep a log of all training which is provided to staff members – a sample of the training log is attached in the appendix.
All staff will be required to sign the training log where required to confirm that they have received training.

The MLRO will circulate to all staff other material to heighten awareness of anti-financial crime issues. This must be placed on the company notice board which should be available in all branch/agent locations.

Where possible, all staff should ensure that they attend seminars offered by the UKMTA on key issues relating to AML procedures. Information on UKMTA seminars is provided at www.ukmta.org. All staff will be required to view the AML training module provided by the MTA (or similar) and to take the test.

iv) Record keeping

As according to the law, the company will keep full detailed records of all transactions with copies of identifications and proof of address provided by the customer. All customer records will be retained at least for a period of five years from the date of the customer's last transaction.

The company will also retain all bank statements, internal and external SAR's as well as all records of training and compliance monitoring. All these records will likewise be kept for five years.

v) Business Monitoring

It is the responsibility of the MLRO to monitor all the activity of the business with particular reference to the potential financial crime risk. The MLRO will keep a close eye on the following criteria and provide a report to senior management when required.

The report is likely to include commentary on the following issues (in the case that there is no information to report, then a 'nil return' should be indicated):

- Confirmation that adequate CDD information is being collected and that ongoing monitoring is taking place
- Summary data relating to complex or unusual transactions
- Number of internal consents/SARs received from staff members
- Number of SARs made to National Crime Agency
- Information on status of staff training within the company
- Confirmation that all business records have been stored
- Changes in the law/operating environment which are or will impact the business
- Changes in risk matrix effecting the business
- Contacts with the regulator

Reports should normally be written.

The MLRO should indicate where there is action of the regulator, law enforcement or other agency which raises any potential issues for the business.

The MLRO will, as a matter of policy, submit an annual report to the board of directors.

The following ongoing business monitoring shall be undertaken by the MLRO:

1. On a quarterly basis, all the transactions for that quarter are downloaded into Excel and aggregated for each customer. Customers with high volumes of transactions are reviewed for additional due diligence documentation.
2. Transactions during the quarter are also analysed for unusual patterns, such as large transfers or a series of transactions totalling more than £5,000 during the quarter.
3. If the information, explanations or documents provided by the customer does not corroborate the transactions, a report to NCA is considered.

Part B - Customer due diligence and transaction processing

i) Customer due diligence – private client

Customer applying for business in person at a branch

It is company policy that all customers should provide their name and address or name and date and place of birth or name and national ID number, such as passport number before they process the first transaction.

All customers are required to provide a Photo Id irrespective of the transaction amount and whether a business relationship is deemed to have been established or not.

At the point that a customer transacts £2,000 or more either as a one off or series of linked transactions their address will be verified (if not already done).

At the point that a customer transacts £4,000 or more either as a one off or series of linked transactions their address will be verified (if not already done) and they will also be asked to indicate source of funds (their profession) and purpose of transaction.

Customer applying for business over the telephone or over the internet

Non-face to face transactions are considered to be higher risk than transactions carried out with the customer present.

Further checks will be made on the information provided and these will include at least one of the following:

- Request sight and take copies of their identification documents.
- Verification of customer details against an independent online database.
- Telephone contact with the customer at a home (land line) telephone number or business address which has already been verified, using call to verify additional aspects of personal identity information already provided during application process
- Sending a letter to the customer at his home address and then calling him to verify details included in the letter
- Requiring that funds should be sent from a bank account in the customer's name

Please note, the easiest way to get certified customer ID is to use the 'Identity Checking service' at the UK post office (the fee for this service is £6.95.) For more details see:

http://www.postoffice.co.uk/portal/po/content1?catId=63400715&mediaId=105000818

Changes and modifications to clients' details

All customers should be made aware that information is held for 5 years – random checks may be made on information supplied and if any details are incorrect, customers will be suspended from the system until the customer supplies the updated personal information. Staff should particularly take care to make sure that customer ID information previously supplied is still valid (and that ID documents have not expired).

Offering services to migrant workers

Details of document required by migrant workers are available at http://www.direct.gov.uk/en/Employment/Understandingyourworkstatus/Migrantworkers/index.htm and Home Office website: www.homeoffice.gov.uk. Firms are not required to establish whether an applicant is legally entitled to work in the UK but if, in the course of checking identity, it came to light that the applicant was not entitled to do so, the deposit of earnings from employment could constitute an arrangement under the Proceeds of Crime Act.

ii) Customer due diligence – companies

Before carrying out any business with our company, the following information and documentation must be obtained from each company client (see appendix for example form):

- Full name, registered number and registered address
- Business address
- Business activity
- Names of all directors
- Names all beneficial owners (anyone who owns or controls, directly or indirectly, more than 25% of the company)
- Turnover of the business, its size and number of employees
- Length of establishment

The above information must be supported by:

- Extract from appropriate company register or a Certificate of Incorporation
- Letter from the directors confirming which named individuals have authority to act on behalf of the company (if applicable)
- Copy of ID and proof of address for all those who are authorised to trade.

iii) Customer due diligence – MSB's

The company will request the following information from each MSB client ('originating MSB') before processing the first transaction (see appendix for example form):

- Full name, registered number and registered address
- Business address
- Business activity
- Names of all directors
- Names all directors and beneficial owners (anyone who owns or controls, directly or indirectly, more than 25% of the company)
- Confirmation of the MLRO's name
- Turnover of the business, its size and number of employees
- Length of establishment

The above information must be supported by:

- Extract from appropriate company register or Certificate of Incorporation
- Letter from the directors confirming which named individuals have authority to act on behalf of the company (if applicable)
- Copy of ID and proof of address for all those who are authorised to trade

Additionally, each MSB should provide the following information:

- Copy of their MSB registration certificate or an extract from HMRC MSB register or FCA Financial Services register.
- Copy of all MLR101 fit and proper tests submitted to HMRC to verify that the management are 'fit and proper' people (i.e. have no criminal/money laundering convictions, etc)
- A written confirmation from the director(s) or those authorised to trade, that the MSB will send the Complete Information on the Payer (CIP) for all transfers made through our company, directly to the paying out agent as required by the EU Payments Regulation 2007.

The company will meet with the director and/or owner of the MSB before starting business.

In any event, the company will verify the MSB certificate with HMRC and will record when the MSB certificate expires. The company will periodically verify again with HMRC that the MSB is still entitled to trade (and that the certificate has not been withdrawn for some reason). All information on originating MSB partners will be recorded (see appendix for example form) along with baseline information on the volume of transactions expected.

v) Customer due diligence – correspondents

We recognise the risk involve in dealing with third party paying out agents. Therefore, it is company policy to deal directly with only banks as our paying out agents. This is to ensure we further minimise the risk involved with third party paying out agents, as the banks, being regulated institutions carry out their own anti-money laundering measures on the beneficiaries.

vi) What is a business relationship?

A business relationship exists where the company sets up a process with the customer which makes it easier for them to make regular transactions. It is our company policy that a business relationship exists if a customer has done more than one transaction and one of the following situations apply:

- a unique customer number is allocated, and a customer registration form is completed
- a loyalty card is issued
- customers are able to deposit cash into the company bank account
- customers can make transactions by telephone or over the internet
- customers are offered credit facilities

In situations where a business relationship exists, there is an obligation to obtain a proof of ID, plus confirmation of purpose of transaction and source of funds. There is an obligation on the company to monitor all transactions carried out in the business relationship (see transaction monitoring).

vii) Linked Transactions

It is company policy that transactions are 'linked' when the following criteria apply:

i) The same sending customer has sent to the same receiving customer in a number of individual transactions £4,000 or more within one month.
ii) Three sending customers or more are sending to the same receiving customer (or receiving address or receiving telephone number) AND the receiving customer or bank account has received more than £10, 000 in last 3 three months or £4,000 within one month.
iii) A sending customer is sending funds on behalf of one or several people (see under CDD – private client)

In the event that 'linked' transactions are identified, they should be notified to the MLRO who will determine whether or not there are any suspicious circumstances which mean the transaction should be reported to NCA.

viii) Beneficial ownership

Corporate clients

All corporate clients will be required to indicate when they register with the company who is the beneficial owner(s) of that company (those holding 25% share of the company).

Foreign correspondents/invoice payments

In cases where the company is requested to make payments to third parties at the request of foreign correspondents, the MLRO will take steps to understand and record:

- Who is the owner of the invoice?
- Who is the payee of the invoice?

Both the invoice owner and invoice payee will be subject to a sanctions list check.

ix) Source of funds – when to verify

Any sending customer will be requested to provide written proof of source of funds for any one off cash transaction of £2,500 or more. Acceptable proofs will include:

- Source of funds declaration on the Customer Risk Assessment Form (see appendix 1)
- Mini statement
- Bank statement less than three months old
- Letter of secured or unsecured loan
- ATM receipt
- Wage slip
- Or other acceptable document (depending on the circumstances)

In the event that the customer is unable to provide any of this information, the transaction must be refused.

Alternatively, the transaction can proceed if the customer provides a banker's draft, a bank counter cheque or if funds come from a bank account in the name of the sending customer.

If any customer does cumulative transactions which total more than £10,000 (approx. €12,000) in any 3 month period, then his/her address will be verified on the CreditSafe online database (if not already done), plus documentation of source of funds (see Appendix 1) and if the CreditSafe online verification fails, then he will be asked to provide written proof of address. A failure to do so will be regarded as suspicious and a report should be made to NCA

x) Transaction processing

All money transfer transactions can be in cash, by banker's draft, by bank counter cheque or from the customer's bank account to the Company bank account.

Non face to face transactions over the telephone are permissible, but customer will be required to quote their customer ID and should also be asked to answer security questions.

When a retail customer makes an approach in person to the company with a request to transfer funds, we will complete a send form in our money transfer system which requires certain information (see the 'Send Form' in the appendix) about the sending customer and the beneficiary.

Each customer is assigned a customer ID number when they process the first transaction and each transaction is given a unique transaction number. Each sending customer is also given the unique transaction number verbally. He/She will need to pass this number to the beneficiary to allow them to pick up the funds in the receiving country.

Upon completion of the transaction, the customer is offered a receipt which records all the details of the transaction.
The company will keep complete records for each transaction showing the following:

- Unique transaction number
- Sending customer ID number (generated by the company)
- Sending customer name
- Sending customer address (including full postcode)
- Sending customer telephone number
- Transaction amount
- Exchange rate
- Fee charged
- Pay out bank account
- Pay out location (if cash transaction)
- Receiving customer name (if available)
- Receiving customer address (if available)
- Receiving customer telephone (if available)

All customers will need to be made aware that they should make a complaint to the business in the first instance if they are not happy with any aspect of the way the transaction has been processed. Any complaint must be processed in line with the complaints handling process established by the business (see complaints handling policy).

xi) When to accept or decline a transaction

It is company policy that a transaction must be declined in the following circumstances:

- customer provides insufficient CDD information when required
- customer is unable to provide ID and proof of address when required
- customer is unable to provide proof of source of funds when requested

xii) Sanctions List check

The company has developed a policy to check all transactions to confirm that no transaction involves any individual or company on the UK Sanctions list. (HM Treasury Consolidated List).

In the situation that there is any target match, the transaction would be automatically frozen and a report will be made to HM Treasury (Asset Freezing Unit) by the MLRO. The details of the Asset Freezing Unit are as follows:

Asset Freezing Unit
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ
E-mail: assetfreezingunit@hm-treasury.gov.uk
Fax: 020 7270 5430
Telephone: 020 7270 5664 or 020 7270 5454

The transaction will also be reported to National Crime Agency (NCA).

If and when the company processes USD$ to settle payments, it is company policy that all beneficiaries of transactions processed in USD$ are verified against the Office of Foreign Asset Control (OFAC) list. In any case where a target match is found, the transaction will not be allowed to proceed.

xiii) Politically Exposed Persons (PEPs) check

The definition of a 'PEP' is set out below:

- is or has, at any time in the preceding year, been entrusted with prominent public functions
- is an immediate family member of such a person
- is a known associate of such a person
- is resident outside the UK
- is or has, at any time in the preceding year, been entrusted with a prominent public function by –
    a) a state other than the UK;
    b) the European Community; or
    c) an international body; or
- is an immediate family member or a known close associate of a person referred to in the paragraph immediately above.

It is a matter of company policy that all customers will be required to indicate whether they or any member of their family has previously worked in a non EU country at any time in the preceding 12 months. In case the answer is yes, the cashier must make enquiries to establish whether the customer may meet the criteria for being 'politically exposed'.
In cases where a PEP is identified:

- Senior management approval should always be sought before establishing a business relationship with a PEP
- The source of funds should be established
- The business relationship should be subject to enhanced monitoring

xiv) Transaction monitoring

The number and volume of transactions going through the company will be monitored, together with scrutiny of transactions, according to risks parameters relating to: customers, products, delivery channels and geographical area of operation.

The MLRO will keep under review all the transactions which are being processed by each customer. This means the MLRO will:

- review on a regular basis whether the volume of transactions which is being processed by the customer is consistent with what was anticipated when the customer was registered
- keep a watch out for a sudden increase in business from an existing customer
- look out for uncharacteristic transactions which are not in keeping with the customer's known level of activity
- look out for peaks of activity at particular locations or at particular times
- look out for unfamiliar or untypical types of customer or transaction
- look out for transactions related to potential sanctions list matches or PEP's

To assist with transaction monitoring, the company has defined a transaction monitoring protocol (see Business Monitoring section in part A).

Part C- Suspicious activity reporting – our obligations

i) What is suspicious activity (which must be reported)?

The law requires staff working in financial sector businesses to be on the lookout not only for suspicious transactions, but also for any activity which takes places around a potential transaction.

Suspicion is personal and subjective and falls far short of proof based on firm evidence.

Two examples are given below from a recent court case (K Limited v National Westminster Bank) in which the judge gave some helpful guidance on what suspicion is:

'the essential element in the word 'suspect'…is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feel of unease would not suffice. But the statute does not require that suspicion to be 'clear' or 'firmly grounded and targeted on specific facts', or based upon 'reasonable grounds'

'There is no legal requirement that there should be reasonable grounds for suspicion. The relevant bank employee either suspects or he does not. If he does suspect, he must (either himself or through the Bank's nominated officer) inform the authorities'

A person who considers a transaction to be suspicious would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime.

At the same time, the employee should take extra care with transactions done by new customers that do not make any sense or one that seem abnormal. (e.g. a known unemployed person sending a large amount of money)

A fuller list of suspicious indicators is included in Section 3 (Risk Assessment).

ii) Suspicious activity reports – internal company process

In the situation that an employee, agent or agent employee (for this purpose, collectively, staff members) has suspicions about a customer and/or transaction, he must ensure that the company MLRO is notified about his suspicions as soon as possible.

Staff should use the internal 'Suspicious Activity Report Form' (see appendix for example).

The SAR should contain as a minimum the following information:

- Date/time of transaction
- Amount
- Customer name/customer ID information (e.g. passport number, etc)
- Transaction number
- Reason for suspicion of transaction

If in doubt, the staff member should call the MLRO to discuss the reasons for their suspicion – however, they should be careful not to do this whilst the customer is standing in front of them (they may 'tip off' the customer otherwise, see below).

In the situation where the staff member works for an agent, the report should be made in the first instance to the Agent MLRO, who must then report on to the company MLRO.

The timing for submitting the internal SAR is important. The law states that an individual working in the regulated sector (i.e. a money transfer company) should make a report as soon as he or she becomes suspicious. This may mean either before the transaction takes place or immediately afterwards.

Where a staff member becomes aware that a customer wants to carry out a transaction which is suspicious and the timing for the transaction allows it, the staff member must ensure that 'consent' is given before processing the transaction. 'Consent' means that the company has sought and obtained approval from the Financial Intelligence Unit at the National Crime Agency (NCA) to process the transaction. Further information on 'seeking consent' is provided below.

However, staff may decide that there would be a danger that if they were to seek consent for a particular transaction (i.e. in advance of the transaction taking place) that there might be a danger that the customer would be 'tipped off'. See below for more information on 'tipping off'.

All staff members will have fully discharged their duties, and will have the full protection of the law, once a report of their suspicions has been made to the company MLRO.

Once the MLRO receives the internal SAR from the staff member, the MLRO has two options:

- Report the SAR on to National Crime Agency (see procedure below)
- File an internal note indicating why, on the basis of review of the circumstances around the transaction, it is judged not necessary to make a report to NCA

The MLRO should complete the MLRO SAR Resolution form (see appendix for sample) in the event he decides not to make a report to NCA

iii) Dealing with the National Crime Agency

The disclosure regime for money laundering and terrorist financing is run by the financial intelligence unit within the National Crime Agency (NCA). NCA was created on 3 April 2006 by the Serious Organised Crime and Police Act 2005. It is a law enforcement body devoted to dealing with organised crime within the UK and networking with other law enforcement agencies to combat global organised crime. For full details on NCA and their activities view their website at: http://www.nationalcrimeagency.gov.uk/

Making a Suspicious Activity Report to NCA

A suspicious activity report (SAR) is the name given to the making of a disclosure to NCA under either Proceeds of Crime Act or the Terrorism Act. NCA has issued a preferred form to be completed when making a SAR, which may become mandatory in the future. NCA encourages firm to start using the preferred form now.

Preferably, firms should use SARs Online (http://www.nationalcrimeagency.gov.uk/) where you have computer access. This securely encrypted system provided by NCA allows firms to:

- register the firm and relevant contact persons
- submit a SAR at any time of day
- receive e-mail confirmations of each SAR submitted

SARs can still be submitted in hard copy, although they should be typed and on the preferred form. Firms will not receive acknowledgement of any SARs sent this way.

Hard copy SARs should be sent by post to: UK FIU, 1-7 Old Queen Street, London, SW1H 9HP.

The Financial Intelligence Helpdesk can be contacted on 020 7238 8282. Firms can contact NCA on this number for:

- help in submitting a SAR or with the SARs online system

- help on consent issues
- assessing the risk of tipping off so you know whether disclosing information about a particular SAR would prejudice an investigation

NCA is required to treat any SARs confidentially. Where information from a SAR is disclosed for the purposes of law enforcement, care is taken to ensure that the identity of the reporter and their firm is not disclosed to other persons.

It is our company policy that only the MLRO and any senior manager nominated by him on the NCA online system can submit a SAR to NCA.

It is expressly forbidden for employees to make a SAR direct to NCA.

Seeking 'Consent'

Staff may encounter situations when processing a transaction where a request needs to be made to NCA 'seeking consent' to undertake acts which would be prohibited as a principal money laundering offence. The idea behind consent is that the company is seeking a permission to proceed with the transaction before the transaction is finally processed.

NCA has up to 7 days to confirm whether or not the transaction for which consent has been requested can proceed – until NCA give consent, the transaction cannot proceed – it is frozen. In these circumstances, the staff member must be very careful that they do not 'tip off' the customer about the reason for the delay in processing the transaction.

Where NCA gives notice that consent to a transaction is refused, a further 31 day period (the "moratorium") commences on the day that notice is given. The 31 days include Saturdays, Sundays and public holidays. It is an offence to undertake the act during this period as the participant would not have the appropriate consent. The moratorium period enables NCA to further their investigation into the reported matter using the powers within Proceeds of Crime Act (POCA) in relation to the criminal property (e.g. imposing a restraint order). If the moratorium period expires and no such action has been taken, the reporter is free to proceed with the act(s) detailed in the initial disclosure.

It is company policy that all requests for consent must be processed through the company MLRO – it is expressly forbidden for employees to make a 'consent' request direct to NCA.

'Tipping Off'

Any staff member needs to make a judgement as to whether any delay to the transaction ('consent request') would have the effect of 'tipping off' the customer.

It is a criminal offence under POCA Part 7 for anyone, following a disclosure to the MLRO or to NCA, to do or say anything that might either 'tip off' another person that a disclosure has been made or in any way prejudice an investigation. The Terrorism Acts contain similar offences. This means that businesses must not tell a customer:

- that a transaction was/is being delayed because consent from NCA has been requested;
- that details of their transactions or activities will be/have been reported to NCA;
- that they are being investigated by law enforcement.

The punishment on conviction for 'tipping off' is a maximum of 5 years imprisonment or a fine or both.

In situations where delaying a transaction may inadvertently lead to 'tipping off', it will make sense to process the transaction and then ensure that a SAR is submitted to the MLRO as soon as possible after. The staff member will have the protection of the law as soon as a SAR has been submitted to the MLRO.

If in doubt about whether to proceed with a transaction, the staff member should call the MLRO for advice.

Processing subsequent transactions for a customer where a SAR has been filed to National Crime Agency

These are situations where 'enhanced due diligence' is called for. Where a SAR has been made to NCA, the company will await to see if any response is received from NCA to the SAR which has been filed.

In the event that no response has been received from NCA on the previously reported transaction, then the MLRO will have to decide how to deal with the customer if he returns to process a subsequent transaction.

The MLRO may decide either:

- to refuse the transaction
- to process the transaction (but only having asked for written proof of source of funds to be provided)

The MLRO has put in place a system to monitor customers where a report has been made to NCA. The MLRO will be able to identify and freeze transactions processed by customers who have previously been reported to NCA.

Part D – Management of Agents

i) Money Laundering Controls to be used by agents

Our Anti-money laundering controls are policies and procedures that we put in place within our business in order to prevent activities related to money laundering and terrorist financing. Our agents must use the same money laundering controls, which are described in full in this Anti-money Laundering Manual, including:

1. Assessing the risks of our business being used by criminals to launder money;
2. Verifying customers' identity;
3. Monitoring customers' transactions and reporting suspicious activity to the MLRO;
4. Keeping the right records; and
5. Ensuring appropriate internal management controls of the agent.

ii) Other conditions

1. Agents must upload KYC documentation on our money transfer system for verification.

2. Agents must book all money transfer transactions on our money transfer system and not use any other systems for transactions conducted in our business name.

3. Agent shall not release customer transactions for payment in the destination country. All transactions will be released by us after verifying the necessary customer due diligence.

Section 3 UK Payment Services Regulations

Payment Services Directive (PSD) (which has been implemented in the UK as the Payment Services Regulations 2009 – referred to as the PSR) will affect any business provided payment services to their customer. These firms include:

- banks;
- building societies;
- e-money issuers;
- money remitters;
- non-bank credit card issuers; and
- non-bank merchant acquirers.

The FCA's role under the Payment Services Regulations 2009 explains how it is being implemented is available in the FCA Approach Document a copy can be downloaded from their website. www.fca.org.uk/your-fca/**documents/-psd-approach-document**

What is the Payment Services Directive (PSD)?

The PSD creates a consistent legal framework for payment services across the European Economic Area (EEA) – European Union (EU) plus Iceland, Liechtenstein and Norway. It has been agreed at the European level and the plan now is to move this into the national law book by every EEA State. This means that the PSD became an integral part of national law across the EEA since 1st November 2009.

Origins of the PSD

The origins of the PSD go back to 2001 with the introduction of a piece of regulation (2560/2001) which set out to ensure that prices for cross border credit transfers within the euro-zone were no more than those charged for local transfers. This started Europe on the path to create a Euro payment system in co-operation with the European Central Bank - the Single Euro Payments Area (SEPA). The PSD is the first time that Europe has created a set of rules for domestic and international payments and is part of an effort to create a single market for payments in Europe so that we can mirror that which exists in the US.

The concept of SEPA requires a great deal of harmonisation between the legal framework governing Payment Service Providers (PSPs) in different Member States if it is to succeed, with the result that the European Commission (EC) has supported the implementation of a consistent legal framework.

Inevitably the EC extended the original remit and, at the end of 2003, issued a draft "Legal Framework for Payments" that sought to modernise and simplify the regulatory framework applying to retail payment services throughout the EU. After a good deal of discussion what has now become the PSD was published in December 2005.

After another fifteen months of vigorous debate, the contents of the PSD was finally agreed by the European Parliament and published in December 2007. Local governments across the EU and EEA (not just the euro-zone countries) now have until 1st November 2009 to finish transposing the Directive into national law.

Aims

The principle objectives of the PSD are to:

- Establish a single payment market across the whole EU (not just the euro-zone).
- Provide the necessary regulatory framework for a single payments market.
- Create a level playing field and enhance competition within the domestic and cross border payments market.
- Ensure consistent consumer protection and improve transparency.
- Create the potential for more efficient EU payment systems.

The PSD is a "maximum harmonisation Directive", which means that national legislation must not differ from its provisions unless expressly permitted by the Directive. However, there are parts of the Directive that allow Member States' discretion, which will result in some variation. These variations are likely to limit the ability for the EU to achieve some of the objectives outlined above.

Key Institutions

While HM Treasury has taken the lead in the initial EC negotiation and consultation, the FCA will be the main regulatory authority for most aspects of the PSD in the UK. This will mean that it will be responsible for authorisation, registration and supervision, as well as managing the PSD on an ongoing basis.

There are also a number of other bodies who will be involved on an ongoing basis:

- **HM Revenue and Customs** (HMRC) will retain its current responsibility for anti-money laundering (AML) supervision for money transmitters.
- **The Financial Ombudsman Scheme** (FOS) will provide the out of court redress mechanism. This will be the first time that an official complaint channel will be available to users of money transfer services.

- **The Office of Fair Trading** (OFT) will be responsible for ensuring free and fair access to payment systems, with the Competition Appeal Tribunal (CAT) as the appeal mechanism

Scope of Impact

The PSD regulations will affect services provided by the following types of institution: credit institutions (i.e. banks and building societies); electronic money institutions (e-money issuers such as those offering prepaid cards); and the new Payment Institutions (PIs).

PIs are a new type of financial institution introduced under the PSD that have less onerous regulatory requirements than full blown credit institutions (usually banks and deposit takers.

From November 2009 it will become illegal for anyone to provide payment services in the EU unless they are one of these regulated (or registered) institutions. There are transitional arrangements that allow you to delay registration/authorisation if you were providing payment services before the 25th December 2007.

The PSD covers a wide range of payment services and included among them are money transfer services. The following provides some examples of payment services covered and excluded from the PSD:

- **In Scope Transactions:**
  - Domestic and international credit transfers within the EEA of all transaction sizes and currencies.
  - Direct Debits.
  - Card payments (credit, debit, prepaid) where these products can be used in multiple retailers.
  - Consumer and corporate payments.
- **Out of Scope Transactions:**
  - Cash to cash payments (of any type).
  - Transactions that flow outside the EU, or come in from outside the EU.
  - Foreign currency transactions where there is no account held on behalf of the consumer (even if they are funded by a card payment).

It should be noted that if you provide a payment service as defined by the PSD it will be necessary for you to become a regulated (or registered) institution whether or not the transactions you provide are in or out of scope.

In terms of competitive impact there are a number of likely impacts:

- Potential for increased numbers of players in the money transfer space, who may choose to provide/be capable of providing additional payment services.
- Pressure on pricing for current providers of services, as new players enter the market.
- The opportunity for money transfer companies to offer new payment services on the back of their new PI license.
- The opportunity to "passport" services into markets that have traditionally been closed to non-bank money transfer providers.

The PSD and Existing Regulation

There is a wide range of legislation that currently impacts the UK money transfer business, such as the Unfair Commercial Practices Directive and the Consumer Rights Directive. However the main impact of the PSD on current legislation will be on the Anti-Money Laundering Directive and linked national legislation, which has been given additional weight by direct references in the PSD.

A piece of self regulation closely linked to the PSD is the Remittances Customer Charter developed by DFID and supported by UKMTA. This commits participating firms to giving clear, transparent information in a standard format which are similar to those required by the PSD, for example:

- Total fees to the sender and any fees payable by the receiver.
- The exchange rate that applies to the transaction.
- How much money will be received?
- How long the transfer will take, where and how the receiver can collect it.
- What to do if things go wrong.

This Charter will be updated as a consequence of the PSD but should mean that those who have already signed up will have already implemented many of the required changes.

Section 4 - Financial Ombudsmen Service – its role in dealing with customer complaints

All Payment business will be subject to the Financial Ombudsman Service (FOS) from 1st November 2009. All customers will have a right of recourse to FOS if a payments company

(such as ours) is otherwise unable to resolve an eligible complaint which has been made against the company by one of its customers.

Employees will not normally have much direct contact with the FOS, but need to understand the official complaints- handling procedures and the role of the ombudsman service in helping to resolve disputes.

What exactly is the ombudsman service?

The Financial Ombudsman Service was set up by Parliament in 2001 as the independent expert in settling disputes between consumers and businesses that provide financial services.

By law, the FOS covers all businesses authorised by the Financial Conduct Authority (FCA) and all businesses that hold a standard consumer credit licence issued by the Office of Fair Trading (OFT).

The FOS also covers some other businesses or former businesses – for more details see the website (www.financial-ombudsman.org.uk).

The FOS is not a regulator or an industry trade body. Nor are the FOS a consumer champion or a government body. There job is to settle disputes without taking sides.

The FOS are totally impartial and consider each dispute on its own merits – making what the FOS believe is a fair and balanced decision, based on the facts and circumstances of the individual case.

The official ombudsmen are like judges. But sworn witnesses, cross-examinations and formal legal procedures are not part of their usual process for resolving complaints.

The FOS can get to the bottom of most complaints just by writing to – or phoning – the people involved. And the FOS tells consumers they do not usually need professional, legal or financial help to bring a complaint to them.

Being 'covered by the Financial Ombudsman Service' - what does it mean?

In simple terms, it means that our company must have in place – and operate – in-house complaints-handling procedures that comply with the complaints-handling rules. And any

complaint that the company is unable to settle to the consumer's satisfaction – or within the required timescales – can then be considered by the Financial Ombudsman Service.

It the company is unable to resolve a consumer's complaint, we must tell the consumer of their right to take their complaint to the Financial Ombudsman Service. All 'eligible complainants' can bring a complaint to the ombudsman service.

Financial Ombudsman Service and our customers

In accordance with the FOS rules, our company has published a summary of our in-house complaints-handling process. This means we have:

- set out how we seek to handle and resolve any relevant complaints *and*
- explained that – if the complaint is not resolved – the consumer may be entitled to refer it to the Financial Ombudsman Service.

All customers are informed of this information as part of the transactional process - also via websites and receipts as to the availability of this summary.

Telling our customers about the Financial Ombudsman Service helps to underpin our customer's confidence in our business and the payment services we provide.

Who is an 'eligible complainant'?

This is the term used in the FOS rules to describe those who can complain to the ombudsman.

Complaints can be made by, or on behalf of, customers (or potential customers) who are:

- private individuals
- certain businesses with a yearly turnover of under £1 million (some restrictions apply)
- charities with a yearly income of under £1 million
- trusts with net assets of under £1 million.

In some circumstances, the FOS can accept complaints from consumers who are neither customers nor potential customers of the business being complained about.

Examples include employees covered by a group insurance policy held in the name of their employer, or someone who has given the business a guarantee or security for a loan.

Complaints-handling rules

These rules, requiring businesses covered by the Financial Ombudsman Service to have in-house complaints-handling procedures, reflect what is widely considered to be good practice. The rules apply to businesses that *are* or *have been* authorised by the FCA or the OFT.
The rules are published as part of the Financial Conduct Authority's handbook (available online at http://www.fca.org.uk/static/documents/handbook-releases/redress136.pdf)

When a customer complains – what action to take?

The Financial Ombudsman Service won't consider a complaint until our company have first had the opportunity to deal with it ourselves. So it is our company policy that we will always investigate any complaint and decides how we want to respond to it.

The complaints-handling rules require us to try to resolve complaints at the earliest opportunity. The rules set out time limits for dealing with complaints. This means that we must send the consumer a 'final response' (or explain why we are unable to do this) within eight weeks of the date we received the complaint.

We must also send the complainant details of how to contact the ombudsman service and a copy of the FOS leaflet titled 'your complaint and the ombudsman'. **These are ordered via the FOS website or by phoning the FOS publications helpline on 020 7964 0092.**

What is a 'final response'?

A final response will include the following points as required under the rules:

- give a summary of the complaint, setting out the result of your investigation and your final view on the issues raised by the customer;
- say whether you acknowledge there has been any fault on the part of your business;
- give details of any offer you are making to settle the complaint;
- enclose the FOS leaflet and;
- tell the consumer about their right to refer the dispute to the Financial Ombudsman Service within six months, if they are unhappy with your response.

If, at the end of eight weeks, we want more time to investigate the complaint – and the customer agrees to this – the ombudsman service will not automatically get involved.

But we must still tell the customer about their right to take their complaint to the Financial Ombudsman Service. If the consumer takes their complaint to the ombudsman service after

eight weeks – and they are satisfied, from what we tell them at this stage, that the complaint has special features which mean we clearly do need more time – then the FOS may decide not to look into the complaint immediately.

We do not ask FOS for any time extension as a matter of routine.

What are the time limits for consumers bringing unresolved complaints to the ombudsman service?

The complaints-handling rules set time limits for consumers to complain to the ombudsman – after which our company can choose to object to the ombudsman looking at the complaint, on the grounds that it is 'time-barred'.

Generally these time limits are:

- six months from your business sending the consumer a final response;
- six years from the event the consumer is complaining about (or, if later, three years from when the consumer could reasonably have known they had cause to complain).

While some businesses are happy for the ombudsman to consider all complaints made against them, even if the consumer has missed the formal time limits. We reserve the right to object to the ombudsman considering a complaint we have received – where we believe that any of these time limits has already expired – then we will let the FOS know as soon as practically possible.
Depending on how clear-cut the issue is, the FOS will:

- dismiss the complaint straight away, telling the consumer that they are too late to complain; or
- investigate further, to check dates and the full circumstances – including asking the consumer why they didn't complain earlier.

However, in 'exceptional circumstances' the FOS does have the discretion to look at complaints that fall outside these time limits. An example might be if the consumer was incapacitated during the period when they could have complained.

We must comply with an ombudsman's decision

If the consumer accepts the ombudsman's decision, it is binding on us. The rules require us to comply promptly with any money award or direction that the ombudsman makes.

If we do not do this, the consumer can go to court to enforce the award or direction, if necessary. And the relevant regulator may take into account any failure to comply with an ombudsman's decision.

We must also comply promptly with any settlement we may have agreed to make at an earlier stage of the FOS process – for example, during conciliation or following an adjudicator's view.

Section 5 Conduct of Business

Introduction to Conduct of Business

The principal sources of our regulatory obligations (the "**obligations**") may be found in the PSRs (which derive from the EU Directive 2007/64/EC on payment services in the internal market). FCA guidance on our obligations may be found in their "approach document", which can be found on the FCA's website at www.fca.gov.uk. The FCA have also published "perimeter guidance" to help firms consider whether their activities fall within the scope of the PSRs (see FCA doc 2009/19).

Our principal compliance obligations include:

i. providing relevant service and charges information to our customers,
ii. incorporating mandatory terms in our contracts with customers,
iii. executing our customers' orders within certain time-frames,
iv. granting our customers refunds if certain conditions are met, and
v. dealing with complaints in a fair manner.

This Policy is supplementary to our other published policies, including our tackling financial crime, complaints and data protection policies.

Transactions under Framework Contracts

Where we have an ongoing relationship with a customer, employees that have identified that a relationship exists under the PSRs must ensure that a "**Framework Contract**" is in place that governs all future executions of transactions. We will comply with the terms and condition of the Framework Contract in addition to the guidelines set out in this Policy.

Providing customers with a Framework Contract and changes to such contract

A Framework Contract (which includes all the information specified in Schedule 4 to the PSRs) will be provided to a customer prior to an ongoing relationship being established and before the customer will be bound by its terms and conditions.

Customers may request a copy of the original contract or copy of the most current contract as a replacement for lost or damaged earlier issued contracts. Any changes to a Framework Contract in place with a customer will be advised at least two months before they are due to take effect.

However, there is an exception with respect to changes to exchange rates that may be applied immediately and without notice on the basis of the following reasons:

i. this has been agreed in the Framework Contract and the changes are based on the "reference exchange rates" information already provided in the Framework Contract to the customer or
ii. the changes are more favourable to our customer.

The addition of new payment services to an existing Framework Contract, which does not change or affect a change in the terms and conditions relating to the existing payment services, will not be treated as a change and so do not require the provision of two months' notice.

Any rate changes such as interest rate or exchange rate are implemented and calculated in a neutral manner that does not discriminate against our customers. Customers will not be unfairly or unduly disadvantaged.

Termination of a Framework Contract

A customer can terminate the Framework Contract at any time, unless a period of 30 days notice had been agreed at the beginning of the contract. Any charges that we make on the early termination will be reasonable and relate to actual costs.

For framework contracts that have been running for or exceed 12 months or alternatively, those which are set to end after a fixed period of 12 months or more, there will be no charge for terminating the contract.

Recurring charges for services specific to the running of the payment services offered or advance payments in respect of such service charges will be returned upon termination of a Framework Contract.

We will give at least two months' notice if we wish to terminate a Framework Contract that is not for a defined term.

Information to be provided at the request of a customer prior to execution of a transaction

At the customer's request, prior to execution we will inform the customer of:

i. the maximum execution time for the transaction concerned; and
ii. any charges payable (including a breakdown of those charges where applicable).

Information to be provided to a payer on individual payment transactions

We will provide the payer with the information in respect of individual payment transactions, including:

i. a reference enabling the customer to identify the payment transaction and, where appropriate, information on the payee;
ii. the amount of the transaction in the currency of the payment order, along with details of any exchange rate used and the amount of the payment transaction after it was applied;
iii. the amount and breakdown of any transaction charges, so that the customer knows the total charge he is required to pay; and
iv. the date of receipt of the payment order.

Information to be provided to a payee on individual payment transactions

We will provide the payee with the information set out in the Framework Contract in respect of individual payment transactions, namely:

i. a reference enabling the customer to identify the payment transaction and, where appropriate, information on the payer and any information transferred with the payment transaction;
ii. the amount of the payment transaction in the currency in which the funds are at the customer's disposal;
iii. any exchange rate used by us and the amount of the payment transaction before it was applied; and
iv. the amount and breakdown of any transaction charges.

How Framework Contract information must be presented

The pre-contractual information required to be provided to Framework Contract customers must be provided to the customer in a way which enables our customer to store and reproduce the information unchanged.

If a customer so requests, we will provide post transaction information to Framework Contract customers. We also provide such information as soon as reasonably practicable after each individual transaction. Post transaction information can be provided or made available at least once a month.

Low Value Payment Instruments

Low value payment instruments are those that under a Framework Contract can only be used for individual transactions of 30 Euros (or equivalent) or less, or for transactions executed wholly within the UK of 60 Euros (or equivalent) or less.

In cases of low value payment instructions, we only have to provide the following, less detailed, information to customers regarding the main characteristics of our payment service:

i. the way in which the instrument can be used;
ii. the payer's liability for unauthorised payment transactions;
iii. details of any charges applicable;
iv. any other material information that the customer might need to make an informed decision; and
v. details of where the customer can easily access the full information in Schedule 4 of the PSRs that must normally be disclosed prior to being bound by a Framework Contract.

We can agree with the customer that there is no need to communicate contractual changes in respect of low value payment instructions.

Fluctuations in exchange rates between euro and sterling may cause difficulties over time in determining whether a particular payment instrument is a low value payment instrument. Recording rates on a transactional basis ensuring that the valuations are monitored and taking a reasonable and consistent approach to dealing with such fluctuations in rate will enable future determination on the payment instrument being a low value payment instrument.

Single Payment Transactions

When we should use a Single Use Contract

Where there is no ongoing relationship with a particular customer, or in cases where there is such a relationship but our Framework Contract does not cover the particular payment service requested, we will ensure that a "**Single Use Contract**" is provided to the customer or made easily. The Single Use Contract will relate to one-off transactions.

By complying with its terms and conditions as well as this Policy we will comply with our regulatory obligations.

Information to be provided to a payer after receipt of a payment order

We will provide, or make available to, our payer the information set out in the Single Use Contract immediately after receipt of the payment order, including:

i. a reference to enable the customer to identify the transaction (and if appropriate the information relating to the payee, for example, in a money remittance what the payee will need to do to collect the funds);
ii. the amount of the payment transaction in the currency used in the payment order;
iii. details of any charges payable by the payer (including, where applicable, a breakdown of those charges);
iv. where the transaction involves a currency exchange and the rate used differs from the rate provided before the transaction, the actual exchange rate used (or a reference to it) and the amount of the payment in the other currency after exchange; and
v. the date the payment order was received.

Information to be provided to a payee after execution of a payment order

We will provide, or make available to, a payee customer, immediately after execution of the payment transaction, the following information:

i. a reference to enable the customer to identify the transaction and where appropriate, relevant information transferred with it (for example, name of the payer and invoice number);
ii. the amount of the transaction in the currency in which the funds are being put at the payee's disposal;
iii. details of any charges payable by the payee (including a breakdown of those charges); and
iv. the exchange rate used (if relevant) and the amount of the payment before it was applied.

How Single Use Contract information must be provided

Unless a customer so requests, no information to be provided or made available to Single Use Contract customers needs to be provided on paper or another durable medium. We may give such information orally over the counter or make it otherwise easily accessible, for example by a link to a secure website.

General Obligations

Communication of Information

Ensure that any information provided or made available in accordance with this Policy or under the terms of the relevant contract with our customer is provided or made available:

i. in an easily accessible manner;
ii. on paper or on another durable medium (eg email/text etc) if our customer so requests;
iii. in easily understandable language and in a clear and comprehensible form; and
iv. in English or in another language agreed between us and the customer.

Charges for Information

Any information specified in this Policy or under the terms of the relevant contract with our customer is provided free of charge. However charges for additional or more frequent provision of information may apply, or where another means of transmission from that agreed in the relevant contract is requested, but such charges will be reasonable and correspond to the actual cost to us of providing the information. We will therefore be able to justify the level of any such charges.

Information on additional charges or reductions

The levy of any additional charge or offer a reduction in cost for using a particular means of payment, advice on the levy or offer will be made to the customer before starting the payment process for the transaction.

Each party to a payment transaction to pay own charges

The payee must pay any charges levied by its payment service provider on the receiving of the transaction in such cases that a local charge which is out of our control and the payer must pay any charges levied by us. Unless the payment transaction involves a currency conversion, arrangements are made where the payer pays both charges, or the payee pays both his and the payer's charges.

Currency and currency conversion

Where we offer a currency conversion service before a payment transaction, we must disclose to the customer the exchange rate to be used and all charges before the transaction are agreed. The jent transaction will then be executed in the agreed currency.

Execution of payment transactions

When we provide a payment services to a payer we will ensure that the amount of the payment transaction is credited to the payee by the end of the third business day following the time of receipt of the payment order.

"Business day" in this context means a day on which we are open for business (other than a Saturday, Sunday or public holiday).

For the purposes of the above, the time of receipt of a payment order is the time at which the payment order is received by us. If we receive the order on a day which is not a business day for us, or if we receive an order outside UK bank hours, we will consider this as being received on the following business day.

Where a customer agrees with us that execution of a payment order is to take place either:

i. on a specific day,
ii. on the last day of a certain period, or
iii. on the day on which they put funds at our disposal, the time of receipt is deemed to be the day so agreed. If such day agreed is not a business day for us, the payment order should be considered as having been received on the first business day thereafter.

Where we provide payment services to a payee customer, we must ensure the relevant funds are available to the payee customer immediately after the funds have been credited to our account.

Where all the conditions set out in our Framework Contract with a customer have been satisfied, we should not refuse to execute an authorised payment order, unless such execution is otherwise unlawful.

Where we do refuse to execute a payment order, we must notify the customer at the earliest opportunity of the refusal, and if possible, the reasons for such refusal together with the procedure for rectifying any factual errors that may have led to the refusal.

The notification must be provided or made available in the way agreed in the relevant contract with the customer. However, we should not make such a notification where it would be otherwise unlawful.

Furthermore, we do not need to provide a notification in respect of low value payment instructions if the non execution is apparent from as such from a declined payment from a payment card service provider at point of payment.

A customer may only revoke a payment order after we have received such order if we consent. However, if a customer has agreed with us that execution of a payment order is to take place either

a. on a specific day,
b. on the last day of a certain period, or
c. on the day on which he has put funds at our disposal, such customer may revoke a payment order up to the end of the business day preceding the agreed day.

We will ensure that the full amount of any payment transaction is transferred and that no charges are deducted from the amount transferred.

We may agree with payee customers to deduct charges from the amount transferred to us before passing on such amount, provided that the full amount of the payment transaction and the amount of the charges are clearly stated in the information we provide to such payees.

Refunds and redress

Where we incorrectly execute a payment transaction or execute a payment transaction which was not authorised by a customer and we have been notified of such error by the customer within 13 months after the transaction date, we must immediately refund the amount of the unauthorised payment transaction to the customer.

However, it will be reasonable for us to investigate such a claim before making a refund if there is evidence to suggest that either fraud or deliberate, or grossly negligent, behaviour on the part of the customer may have occurred.

Where such an investigation is justified, we will carry it out as quickly as possible in light of the circumstances.

Complaints

Please refer to our Complaints Policy for the procedures to be employed when dealing with customer complaints.

We will ensure customers have access to our Complaints Policy upon request, and will include a copy of such policy in any written acknowledgement of a customer complaint.

It is important that we send a written "final response" to complainants within 8 weeks after receipt of a complaint. The final response should either

a. accept the complaint and, where appropriate, offers redress or remedial action,
b. offer redress or remedial action without accepting the complaint, or
c. reject the complaint and gives reasons for doing so.

The final response will also include a copy of the Financial Ombudsman Service's ("**FOS**") standard explanatory leaflet and inform the complainant that if he remains dissatisfied with our response, they may now refer their complaint to the FOS and must do so within six months.

If we are unable to provide such a final response within 8 weeks, we will send the complainant a written response which explains why we are not in a position to make a final response and indicate when we expect to be able to provide one.

This response will also inform the complainant that they may now refer the complaint to the FOS and will enclose a copy of the FOS standard explanatory leaflet.

In handling complaints, we will identify and remedy any recurring or systemic problems, such as

a. analysing the causes of individual complaints so as to identify root causes common to types of complaint,
b. considering whether such root causes may also affect other processes or products, including those not directly complained of, and
c. correcting, where reasonable to do so, such root causes.

We will retain records of complaints received and the measures taken for three years from the date the complaint was received. This record may be used to help the FOS if necessary.

Contracts to which the distance marketing regulations apply

The Financial Services (Distance Marketing) Regulations 2004 (the "**DMRs**") apply to "distance contracts" made on or after 31 October 2004.

A "**Distance Contract**" is one which has been concluded with a "consumer" (defined in the DMRs as any individual who is acting for purposes which are outside any business he may carry on), either by ourselves or by an intermediary acting on our behalf, in respect of which we (or the intermediary) have made exclusive use of one or more means of distance communication up to and including the time at which the contract was concluded. Accordingly, if we negotiate and conclude a contract with a customer solely by telephone, post or via our internet site (or by other means without both parties being physically present at the same time), and such customer is an individual who is acting for purposes which are outside any business he may carry on, such contract will be a Distance Contract.

Customers who have concluded a Distance Contract with us have the right to cancel their contract within 14 days, from the day after the Distance Contract was concluded. If we provide the information referred to below after the date on which the Distance Contract is concluded with a customer, the cancellation period ends on the expiry of 14 calendar days from the day after the date on which the customer received that information.

In addition to the terms and information we are obliged to provide under the PSRs, we will provide the information set out in paragraphs 8 to 13, 16, 17 and 21 of Schedule 1 to the DMRs to our Distance Contract customers.

We will provide this information which is available and accessible to our Distance Contract customers prior to the conclusion of the Distance Contract. Informational requirements exceeding those under the PSRs in respect of Framework Contracts include informing our Distance Contract customers of any specific additional cost we charge for using the relevant means of distance communication. If we charge more for a customer to make a payment through our internet page or via the telephone then we will inform our customer of this fact prior to concluding the contract.

Note that if we enter into Single Use Contracts which are also Distance Contracts, the informational requirements in Schedule 1 to the DMRs go significantly further than those in the PSRs.

Section 6 - Our complaints policy

Our company is committed to delivering an efficient and professional service. We aim to provide prompt, courteous, helpful, open and informative advice in response to every approach made by a member of public. We are always keen to hear the views of our customers, particularly the general public, about our performance generally – what we do right and what we do wrong.

From time to time things may go wrong, and we may fail to provide the Standards of Service that we have set ourselves. Such instances reported to us by customers provide us with an opportunity to put things right and to learn from our mistakes.

Types of complaint handled

Handling complaints quickly, fairly and helpfully is a key part of our approach to service delivery. Examples of complaints about a service provided might include:

- dissatisfaction with the way in which we respond to an enquiry, or the time that we took to respond;
- a perceived injustice because of alleged maladministration on our part;
- a denial of a request for information made under the Freedom of Information Act;
- dissatisfaction with the way in which our assets are maintained; or
- dissatisfaction with the response to a request for our services to be provided in a different format.

Should things go wrong and we fail to provide the quality of service expected by our customers. We will endeavour to:

- ensure that making a complaint is as easy as possible;
- treat a complaint seriously whether it is made in writing by letter, via fax, email
- or by telephone;
- deal with it promptly, politely and where appropriate, informally (for example, by
- telephone);
- include in our response an apology where we have got things wrong, an
- explanation of the position, or information on any actions taken; and
- learn from complaints; use them to improve our service.

Making a complaint

Customers can make a complaint in writing by letter, via fax, email or by telephone. We require customers emailing complaints to provide either a request for an email response or provide a telephone number or full postal address.

Complaints will normally be directed to the member of staff with whom they have been dealing in some cases the nominated office (MLRO) will decide that the complaint is serious enough in nature to process the complaint themselves.

Where the person the customer has dealt with is responding to the complaint we expect them to use this as an opportunity to explain what actions have been taken and to try to sort things out with the customer.

The customer may prefer to speak to the line manager of the member of staff this information is to be provided without exception and refusal of an employee to give this information will result in disciplinary action.

All complaints are recorded and we will provide a summary of all complaints to the Financial Conduct Authority. These statistics are also used internally to improve our products and services.

Complaints Handling Procedures

We shall make every effort to operate in accordance with the Financial Conduct Authority (FCA) and the Financial Ombudsman Service (FOS) complaint management procedures.

We recognise that we have an obligation to Customers who are dissatisfied with our service to resolve any complaint within 8 weeks from the point of notification.

If this is not possible for any reason then we will state our reasons for not being able to do so and propose an alternate completion date to the Customer.

If we are unable to resolve the complaint within this timescale, or to the Customers satisfaction, or the Customer does not accept a deferred date, then such complaints may be eligible for consideration by the FCA or the FOS.

We will provide details of our complaints procedures to assist the Customer as part of our first response process.

Acknowledgement

When we receive a complaint, we will provide written acknowledgement within 5 business days starting from the day after the complaint was received (business days are Mon-Fri excluding bank holidays). The letter will contain details of our Complaints Procedure and of the customer's right to refer the complaint to the Financial Ombudsman if they are dissatisfied with our assessment and ruling.

It will also state who is dealing with the complaint and how to make contact with them (this will normally be the Complaints Officer).

Initial Response

We will send the complainant a letter no later than 15 days after the complaint was made, containing a full account of the investigation activities planned, any findings thus far and, if appropriate, any offer of redress. This letter will again advise the Customer of their rights, who is dealing with the complaint and how to make contact with that person.

Further Acknowledgement

In the situation whereby, the complainant responds to the Initial Response then again will acknowledge receipt of their response with 5 business days starting from the day after the complaint was received.

Holding Response

If, for whatever reason, we have been unable to conclude our investigation and provide a Final Response (see below) to the complaint then we will issue what is called a Holding Response.

The purpose of this Holding Response is to inform the complainant of the reasons why we have been unable to and presently cannot provide a Final Response and to provide a further indication of what is happening with the complaint and to provide an indication of when the complainant can expect to hear from us again.

If the complainant receives a Holding Response, we will invite the complainant to discuss the matter personally with the Managing Director. The purpose of this step is to ensure that the complaint (and the complainant) receives the highest priority in those situations where the complaint cannot be fully resolved through normal investigatory processes.

Final Response

Once we have completed our investigation we will write to the complainant and offer a summary outcome. Where appropriate, it may also include a final offer of redress. Such letters will be marked clearly as the final response and will include details on how to contact the FOS if the complaint has not been resolved to the complainant's satisfaction or, if the offer of redress is considered insufficient or inappropriate.

Our target time to send the Final Response is within 8 weeks of the initial complaint or 4 weeks after receipt of rejection of offer of redress (where applicable) we strive to ensure that we achieve our target time. We accept that this may not always be possible as on occasions complexity of the complaint may require more time to investigate fully.

We will always abide by regulatory guidelines in relation to a complaint and as such, we will always ensure that complainants are kept informed about their complaint and our activities in response to their complaint.

Monitoring of Complaints

We may be required to provide information on the complaints we have handled to the FCA. It is our policy to keep detailed documentation on individual complaints - any private information will not be shared with any third parties and we comply with the Data Protection Act 1998.

These details will usually include as a minimum;

- The nature, date and method of communication of the complaint
- The complainant's details
- How the Complain was dealt with (outcomes)
- Whether the complaint was upheld or refuted
- Whether the complaint was closed (addressed to complainant's satisfaction) or whether it remains open and outstanding
- What financial redress or other significant outcome resulted from the complaint

Ultimate Redress

It is our policy that after contacting all parties should the complainant remains dissatisfied with the outcome of the complaint then they may seek redress through the FOS and ultimately the courts if they so wish.

In each instance, we will mark the on the complaint file what advice was provided. We will then reclassify the complaint as 'Investigated but not resolved'. Claims have been deemed to be investigated and reported to the FCA on this basis.

Financial Ombudsman Service (FOS)

The FOS is an independent and government-backed service designed to help retail consumers and small commercial businesses (annual turnover of less than £1million) who find themselves in a dispute with a financial organisation such as us.

It is a free service and it can be contacted at any point in a dispute providing the complainant has first contacted the financial organisation with whom the dispute relates to. Most cases are resolved within a 6-month period however some inevitably take longer.

Consumers do not have to accept any decision made by the Financial Ombudsman and at all times the consumer has the right to seek redress in a court should they so wish. However if the Ombudsman decision is accepted by the complainant then it is binding both the firm and the complainant.

To contact the FOS, consumers are advised to write or telephone or email their situation to:
Financial Ombudsman Service
South Quay Plaza
183 Marsh Wall
London
E14 9SR
Telephone No.: 0845 0801800
Email address: Complaint.info@financial-ombudsman.org.uk

More information on the FOS can be obtained by visiting www.financial-ombudsman.org.uk or by downloading the booklet entitled “Your complaint and the ombudsman” from this website.

Section 7 Data Protection Policy

Introduction

The DPA regulates the '**processing**' of '**personal data**'. Its definition of '**personal data**' covers all information relating to identifiable living individuals which is held on computer, in another 'automatically-processable' format or in a manual filing system which is structured so as to facilitate access to information relating to particular individuals. (Information relating to companies and other 'legal' persons is not caught). Its definition of '**processing**' covers any conceivable activity in relation to personal data, including collection, analysis, processing in the ordinary sense of the word, storage, disclosure, international transfer and deletion.

On a day to day basis we have to process personal data in various circumstances and in relation to various categories of individual. This Policy deals specifically with personal data collected in the context of the establishment and management of our customer relationships and the execution of transactions on the instructions of our customers ('**Customer and/or Transaction Management**').

It is important to remember that the DPA regulates processing of personal data relating to all **individuals**, not just relating to **customers**. Information relating to individual representatives of corporate customers, or to individuals (or individual representatives of corporate entity) elsewhere in a payment chain – for example, an ultimate payee or an individual representative of a payment institutions - is also protected by the DPA.

The individuals that the personal data relates to, whether customers or otherwise, these are referred to as '**data subjects**'.

The UK Information Commissioner (the '**Commissioner**') is responsible for enforcement of the DPA and has published a range of guidance on data protection issues, all of which is available on the Commissioner's website at www.ico.gov.uk.

Our principal obligations under the DPA include:

i. processing personal data fairly, legitimately, lawfully and proportionately;
ii. informing individuals regarding our processing of their personal data;
iii. abiding by restrictions on the international transfer of personal data;
iv. keeping personal data secure, taking steps to ensure that they are accurate and up-to-date and deleting them when they are no longer needed;
v. maintaining an appropriate registration with the Commissioner's office; and
vi. responding appropriately when data subjects seek to exercise their statutory rights of access, correction and objection.

A copy of our Policy will be supplied to each employee.

The requirements set out in this Policy are mandatory unless otherwise stated and must be followed by all our employees. It is the responsibility of each such person to acquaint themselves with the requirements of this Policy. **Failure to comply with this Policy may constitute a serious disciplinary offence and could result in dismissal.**

Data Protection Officer

The company Nominated Officer (MLRO) is charged as the designated data protection officer (the '**Data Protection Officer**').

Employees with any questions about our Data Protection Policy or application in particular circumstances you should consult the Data Protection Officer.

Fair and Proportionate Processing

The DPA requires that all of our processing of personal data should be fair and lawful and should meet one of various specified conditions. In designing and implementing each procedure for Customer and/or Transaction Management involving the processing of personal data, we will take these requirements into account and ensure that they are met.

We expect that our routine processing of personal data for Customer and/or Transaction Management procedure will generally meet the most general of the available conditions, which is known as the '**legitimate interests**' condition. The 'legitimate interests' condition will apply, and allow us to process personal data, if **both**:

A: the processing is necessary for the purposes of legitimate interests that we, or a person to whom we disclose the data, pursue (these may be business, compliance or other purposes); **and**

B: the processing is not 'unwarranted' because it prejudices the rights, freedoms or legitimate interests of the data subjects.

Each processing operation will, therefore, be assessed to ensure that part A of this condition is met meaning that we have a legitimate business, compliance or other purpose for carrying out the processing. If part A is met, employees should then consider whether the processing will prejudice the data subjects in any way our expectation is that, provided the other rules in this Policy are followed, our ordinary processing for Customer and/or Transaction Management purposes will not prejudice data subjects' rights, freedoms or legitimate interests. If an employee considers that there is a potential for prejudice to be

caused in a particular case, the prejudice should be balanced against our interests and a view taken on whether our interests outweigh the prejudice to the data subjects.

If employees are in any doubt as to whether the 'legitimate interests' condition is met, employees should consider whether the processing can be justified on the basis that it meets any of the other statutory conditions available in the DPA.

The other conditions most likely to apply are as follows:

i. Processing is justified if it is necessary to fulfil a UK legal obligation. This will include, for example, processing in order to carry out legally-required anti-money-laundering checks; or in response to a UK court order. Foreign legal requirements are not automatically sufficient to justify disclosure or other processing of personal data.
ii. Processing is justified if it is necessary for the performance of a contract with the data subject or to take steps at the data subject's request with a view to entering into such a contract. This will justify some processing of personal data relating to individual customers.
iii. Processing can be justified on the basis of data subject consent. Our customer contracts should, therefore, include consents to the processing of individual customer data that will be necessary as part of our Customer and/or Transaction Management procedures.
iv. The requirement that personal data should be processed lawfully can be breached in a number of circumstances, not covered by this Policy because in themselves they fall outside the scope of the DPA – for example, processing for fraudulent purposes would be unlawful and would therefore breach the DPA.

The DPA also prohibits the processing of **excessive**, **irrelevant** or **inadequate** personal data. Our systems and procedures have been designed so as not to collect personal data which are excessive or irrelevant (in particular: personal data should not be collected on a 'just-in-case' basis) and, of course, employees should ensure that the data collected is adequate for the relevant purposes.

Personal data collected for any given purpose should not then be used for a purpose which is **incompatible** with that purpose – we do not expect this to be an issue in the ordinary course of Customer and/or Transaction Management, however.

We expect the general requirement that processing of personal data should be **fair** to be met if all the other requirements are met.

Transparency / Information-Provision

We are required under the DPA to ensure that data subjects have various information readily available to them this requirement is subject to exceptions, however, and these exceptions are of relatively wide application in the context of Customer and/or Transaction Management. In particular,

a) information only needs to be made available where it is practicable to do so;
b) in the case of personal data which are not collected directly from the data subject (for example, payee data collected from a payer customer), we are not obliged to provide information if to do so would involve disproportionate effort; and
c) we take the view that we can assume that data subjects have, and need not therefore make available, information which should reasonably be obvious to them.

The information to be made available is

a) our identity;
b) the purposes for which we expect to process the data; and
c) any further information that needs to be provided to ensure that our processing of the data is fair.

We must ensure that our customer contracts inform our individual customers of the following:

a) our identity;
b) the purposes for which we process their information (including know-your-client and related compliance purposes as well as the execution of transactions and customer management generally); and
c) the following further information, which, we consider, needs to be provided to ensure that our processing of customer data is fair:
d) the categories of person to whom we may disclose customer data (including, for example, non-customer payers and payees; aggregators; any persons with whom we might share data for fraud prevention purposes; and regulatory and prosecuting authorities);
e) the fact that, if payments are made to persons outside the European Economic Area, this may involve transfers of the customer's personal data to jurisdictions which do not have data protection laws as strict as those in the UK; and
f) information as to the customer's rights of access and correction under the DPA, and contact details so that they can contact the Data Protection Officer if they want to exercise those rights

Our customer contracts also require customers to pass this information on to any individuals whose personal data they provide to us.

We take the view that we do not need to provide information to data subjects other than individual customers to justify our processing of their personal data for routine Customer and/or Transaction Management purposes. In particular:

a) We take the view that the effort involved in contacting an individual non-customer payer or payee, whose personal data are given to us by a customer, in order to provide him or her with information about our processing of his or her personal data, would be disproportionate given that we process his or her information only in order to facilitate a transaction of which he or she will in any case be aware.
b) We take the same view in relation to individual representatives of our customers – having required our customers to pass the required information on to their representatives we take the view that the effort involved in contacting the representatives directly would be disproportionate.

International Transfer

The DPA restricts transfers of personal data to most countries and other territories outside the European Economic Area (the European Union plus Iceland, Liechtenstein and Norway).

Transfers can be made as necessary to facilitate a transaction, on the basis that they are necessary to perform a contract with the data subject (where the data relate to a customer) or entered into in the interests of the data subject (where they relate to an overseas payee).

Except for transfers necessary to facilitate a transaction, personal data should not be transferred to countries or territories outside the European Economic Area unless the Data Protection Officer has considered the proposed transfer and concluded, on the basis of legal advice if necessary, that it can be made without breach of the DPA.

Security, Accuracy and Data Deletion

We have in place appropriate technical and organisational security measures to protect the personal data that we process for Customer and/or Transaction Management purposes against unauthorised or unlawful processing and accidental loss, destruction or damage.

We identify the particular security measures that are 'appropriate' in the context of our business. They must deliver a level of security which is appropriate to the nature of the data and the risks associated with unauthorised or unlawful processing and accidental loss, destruction or damage. We will, in particular, take reasonable steps to ensure the reliability of our employees who have access to the data.

If any aspect of our processing of personal data for Customer and/or Transaction Management purposes is outsourced to a third party service provider now or in the future, including the outsourcing of any wider function which includes the processing of personal data, we must:

a) satisfy ourselves that the service provider will have appropriate technical and organisational security measures in place;
b) ensure that the arrangement is governed by a written agreement which requires the service provider to process the data only on our instructions and imposes on the service provider obligations equivalent to our obligations; and
c) while the arrangement is in place, take reasonable steps from time to time to ensure that the service provider is meeting its security obligations in practice.

We will take reasonable steps to ensure that the personal data that we process is accurate and, where relevant, up to date.

Deleting of personal data will only take place when we no longer have need of it, given the purposes for which they were processed. This does not, for example, prevent us from keeping records containing personal data which may be relevant if there is a future dispute with a customer or another person, but it does require us to delete those records when a dispute is no longer a real possibility unless we have another legitimate purpose for continuing to keep the personal data.

Sensitive Personal Data

Whilst we do not seek to collect or process personal data identified by the DPA as ‘sensitive’ for Customer and/or Transaction Management purposes. Employees should not collect or process sensitive personal data for these purposes and should delete them if employees become aware that we have collected them, except with the approval of the Data Protection Officer given on the basis of an assessment of the requirements of the DPA.

The DPA's definition of ‘sensitive personal data’ covers personal data consisting of information as to: racial or ethnic origin; political opinions; religious or other similar beliefs; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission of any offence; or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Automated Decision-Taking

Whilst we do not use so-called ‘automated decision-taking’ techniques for Customer and/or Transaction Management processes. Employees should not use such techniques except with

the approval of the Data Protection Officer given on the basis of an assessment of the requirements of the DPA.

The DPA's restrictions on the use of 'automated decision-taking' cover systems which make decisions which significantly affect individuals **solely** on the basis of the automated processing of their personal data, without any human intervention

Registration

We maintain a registration with the Commissioner's office which covers our processing of personal data for Customer and/or Transaction Management (and other) purposes.

Employees should keep the Data Protection Officer aware of material changes to the purposes for which we process personal data or, within any given purpose, the categories of personal data that we process, the categories of data subject to whom the data relate, the categories of person to whom we disclose the data or the countries or territories outside the European Economic Area to which we transfer the data, so that they can ensure that the registration is amended accordingly.

Rights of Access, Correction and Objection

Data subjects have statutory rights of access to and correction of the personal data that we hold about them. They also have a statutory right to object to our processing of their personal data, including their request to stop processing their data, although only in very limited circumstances.

If a data subject attempts to exercise any of these statutory rights employees are required to immediately pass on this information by formal communication to the Data Protection Officer so that they can ensure that we respond appropriately and within the timescale laid down under the DPA.

In recording and processing personal data for Customer and/or Transaction Management purposes employees should bear in mind data subjects' rights of access. Employees should not record personal data that employees would not want the data subject to see.

Declaration by Appropriate Person

'I, the undersigned, hereby confirm that I have read and understood the policies which have been set down in the compliance policy manual.

I understand that it is my personal responsibility to ensure that the policies are implemented, both by me personally and also any other members for whom I am personally responsible.

In the event that I fail to implement these policies, I understand that I may be in material breach of my contractual obligations and this may lead to disciplinary proceedings.

This document is prepared in the English language and not withstanding its translation into any other language, the English version shall be the definitive version, which shall be referred to for all legal purposes.

Signed for and on behalf of Remit Continental

Signed……. Date……

Lamin Suwareh

Appropriate Person Declaration

Name _____ Appropriate Person

Signed……. Date……

Appendix List

Appendix 1 – Operational Forms

The forms in this section are templates that have been modified or used as shown for the purpose of ensuring that

a) Acceptable ID Documents
b) Corporate/Business Customer Registration Form -
c) Customer Risk Assessment /MLRO Resolution Form
d) MSB/Payment Institution Application
e) Internal Suspicious Activity Form
f) Transaction Monitoring
g) Training Log Report

a) Acceptable ID Documents

Proof of Identity

At least one of the following ORIGINAL documents:

- Current signed passport
- EEA national ID card
- National ID card (non EEA)
- Current UK issued travel document
- Home Office Immigration and Nationality Directorate application card
- Full UK driving licence
- UK provisional driving licence
- Firearms certificate

Please note: if the customer does not present a document bearing a photograph, he/she needs to provide a passport size photograph

Proof of address

At least one of the following ORIGINAL documents issued within the last 3 months showing the customer's name and current address:

- Bank, building society or credit card statement
- Driving licence (if not used as proof of ID)
- Council Tax bill/mortgage statement
- Benefits/pension book showing current address
- Inland Revenue correspondence
- An official letter from a third party (e.g. employer, solicitor) confirming address

Alternatively, a letter sent to the customer's address and signed and returned by them may be considered. Other forms of ID/proof of address may be acceptable, but require sign off by MLRO.

Identification – what checks should be made on customer ID evidence provided?

- check the ID has not expired
- check any photographs for true likeness
- check the date of birth compared to the customer's apparent age
- compare spelling of names and addresses on different identification documents
- compare the customer's signature with signatures included in the identification evidence
- check for the authenticity of the ID provided as there are lots of counterfeit passports, driving licences and asylum seeker documents in circulation

b) Corporate/Business Customer Registration Form

1	Company Name		2	Company Registration	Companies House Number:
	Address				Date of registration:
	Town			VAT/Company Tax Number	Number:
	Postcode				Date of last return:
	Date of birth			Trade Licences (if any held)	Number:
	Place of birth				Date of expiry:
3	What is the purpose of the **Money Transfer** transactions you will carry out with our Company?	Invoice Settlement	4	Have the owners or any member of their close family worked outside the UK at any stage in the last 12 months?	No
		Overseas Employees			If Yes – they job they did was as follows:
		Land Acquisition			
		Property purchase			
		Other			
	What is the source of funds for **Money Transfer** transactions?	Company Funds		Please give names and addresses of individuals or companies to whom you expect to send transactions to	i)
		Director Funds			ii)
		Employee Funds			iii)
		Business Loan/Gift			iv)
		Other			v)
	If Source is (Director/Employee Funds) please provide the following Information.				
	Employee's name				
	Employee's address				
	What is their annual income? (approximately)				
	How often will they be sending money through our Company?	Weekly	5	If Paying by Bank Transfer please provide your 'personal' bank account details from which transactions will be funded.	
		Every month		Bank Name / Sort Code	
		Other		Name as appears on account / Account Number	
	Amount expected to be sent in the next 12 months?	£			
	Declaration	'I will be sending my Company money only'		'I confirm that the information provided is accurate to the best of my ability. I undertake to inform you within	

		Sign		30 days if there is any change in the information provided above.'
		Date		

c) Customer Risk Assessment / MLRO Resolution Form

Sender Details

1		
	Customer Name	
	Address	
	Town	
	Postcode	
	Date of birth	
	Place of birth	
	Passport	Passport Number:
		Date of expiry:
	UK Driving licence	Number:
		Date of expiry:
	Other ID	Number:
		Date of expiry:

Receivers Details

2			
	Customer Name		
	Address		
	Town		
	Postcode		
	Transfer Method	Cash	
		Bank Transfer	
	Bank Details For Bank Transfer		
	Account Name		
	Bank Name		
	Branch Code		
	Swift/ABA/IBAN Number		
	Account Number		

Transfer Purpose and Source Of Funds Declaration

3		
	What is the purpose of the **Money Transfer** transaction you will carry out with our Company?	Family support
		Health costs
		Education costs
		Property purchase
		Other
	What is the source of funds for **Money Transfer** transaction?	My Salary/ My Work
		My Savings
		My Benefits
		Personal Loan/Gift
		Other
	Are you sending money on behalf of another person	Yes / No
	Reviewing Officer's Signature	Sign
		Date

Financial Details Of Order

4		
	Amount Being Sent	
	Initial Amount	
	Exchange Rate	
	Payout Amount	
	Transaction Fees	
	Review Comments:	

d) MSB/Payment Institution Application

Business Name			Turnover of the business per annum (or for new businesses, forecast turnover)	
Registered number (Companies House)			Number of Employees	
MSB number (If Applicable)			How long has business been operational?	
FCA Licence Number (If Applicable)				
(Date of initial registration)			What is the estimated volume of transactions (in £ sterling)?	Monthly
Registered Office Address (If applicable)				Annual
			What is the average number of transactions?	Monthly
				Annual
Business Address			What is the nature of main business activities?	
Which countries would you be sending money to?			What is the prime source of most funds?	

Number of Directors (Please complete directors details on page 3)		What is the typical purpose of most transactions?	
		Name of MLRO (If Applicable)	
Have any of the directors, owners with more the 25% share, controllers or their relatives or close associates worked in a Non-UK government post in the past 12months.		Did your MSB/Payment Service process any transactions which are out of the ordinary or otherwise different from the typical transaction profile?	
		Sign	
Number of business owners owning more than 25% of shares or voting rights or otherwise excise control over the management of the business (Please complete beneficial owners details on page 3)		Date	
		Name	
		Contact Telephone	
Name of individuals authorised to represent the company		Contact Mobile	
		Email Address	
Sending CIP with transfers	By signing this application form, an MSB hereby confirms that it will send the complete information on the payer (CIP) with the transfers as required by EU Payment Regulations		
Is there anything else that is or may be relevant to this application that you would like to bring to our notice in the space below. (If in doubt please state and we will assess the relevance)			

No	Full Name of Beneficial	Date of Birth	Residential Address	Passport or UK Drivers Licence No.	Director or Beneficial Owner or Both

	Owner				
1					
2					
3					
4					
5					

Please provide one of the following to verify the identity of your company/business:

- Extract from appropriate company register
- Certificate of Incorporation (or similar registration document)
- Copy of a current Money Services Business (MSB) registration certificate
- An FCA Payment Institutions registration confirmation (or similar confirmation from non-UK regulators)
- Confirmation of listing on a regulated market (if you are a listed public company)
- A business tax return or audited accounts plus Accountants letter confirming nature of the business (unincorporated businesses only)

Please provide one of the following to verify the identity of the directors, authorised representatives and beneficial owners

- Certified copy of passport

- Copy of a UK drivers Licence
- EEA national ID card

Please provide one of the following to verify the addresses of the directors, authorised representatives and beneficial owners

- Copy of a Gas, Electric or water bill within the last 3 months
- Copy of a bank statement within the last 3 months
- Copy of current year council tax bill

Other documents to provide

- Letter on company letterhead confirming who is authorised to represent the company (must be signed by at least two directors)
- Copy of all MLR101 fit and proper test submitted to HMRC to verify this has been done.

e) Internal Suspicious Activity Report (for internal company use only)

Private and Confidential

SUSPICIOUS ACTIVITY REPORT (SAR)

To: Money Laundering Reporting Officer

From: ……(name of employee)

Date:

This SAR is (circle which applies) is:

1. A request for consent for a transaction which is not yet completed
2. A report on a transaction which has taken place which I consider suspicious
3. Report on other business related activity which I consider suspicious

I consider the following transaction suspicious and report to you under the internal reporting procedure:

1) Date of transaction: _____
2) Amount: _____
3) Customer name/ID: _____
4) Transaction number: _____
5) Reason for suspicion: _____

Signature of reporting staff _____

f) Transaction Monitoring

The company monitor for each customer and their transactions against the following criteria, customers and/or transactions which fall outside of these criteria will be flagged for further scrutiny:

Criteria	Description
1	Customer information (sending) - required information is: • Customer name (as on ID document) and • Address or • Date of birth and place of birth or • National ID number (e.g. Passport number)
2	Customer information (receiving) - required information is: • Customer Name (as on ID document) • Full bank account details Plus (if available): • Address • Date of birth
3	Customer sending more than £800 (approx. €1,000) in a single transaction (a copy of valid customer ID needs to be available)
4	Customer is sending a second or subsequent transaction (any amount) (a copy of valid customer ID needs to be available and identification of the source of funds/purpose of transaction information)
5	Sending customer and/or receiving customer is a UK or US sanctions list match
6	Sending and/or receiving customer is on any other government sanctions or criminal alert list
7	Sending and/or receiving customer is a politically exposed person (PEP)
9	Sending customer has sent a single cash transaction of £5,000 or more (a copy of proof of address should be provided plus necessary proof of funds should be available)
10	Sending customer has sent a series of transactions in last 12 months which cumulatively total £10,000 (approx. €12,000) or more (a copy of proof of address should be provided plus necessary proof of funds should be available)
11	Three sending customers or more are sending to the same receiving customer (or receiving address or receiving telephone number) <u>AND</u> Receiving customer or bank account has received more than £10,000 (approx. €12,000) in last 3 three months. (a copy of necessary proof of funds should be available)

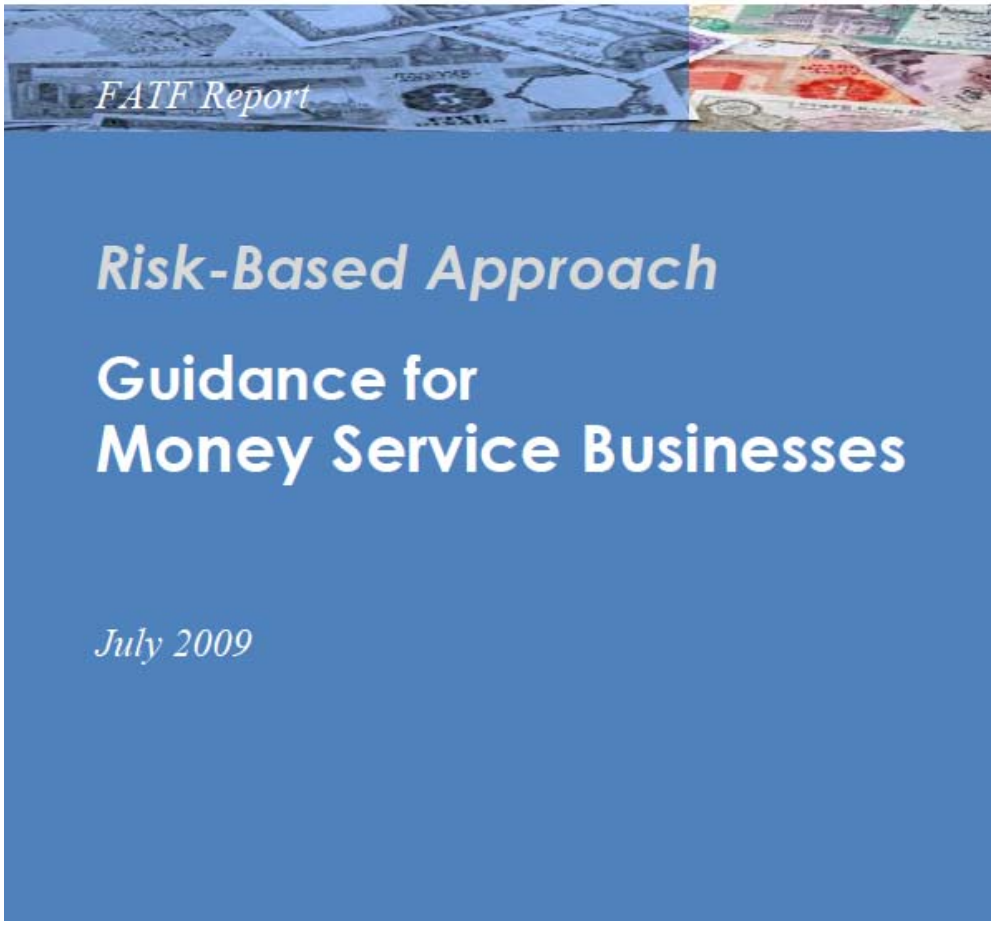
g) Training log

Date of Training	Who took part	What was discussed

Appendix 2 – FATF Report 'Risk Based Approach Guidance for Money Service Businesses'

This guidance can be found at the FATF website: http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Guidance%20for%20Money%20Service%20Businesses.pdf

FATF • GAFI
Financial Action Task Force — Groupe d'action financière



Appendix 3 – FATF Report 'Commercial Websites and Internet Payment Systems'

This guidance can be found at the FATF website: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf

Financial Action Task Force

Groupe d'action financière

MONEY LAUNDERING & TERRORIST FINANCING VULNERABILITIES OF COMMERCIAL WEBSITES AND INTERNET PAYMENT SYSTEMS

18 June 2008