AML POLICY & PROCEDURES

INTER CITY MONEY LIMITED
1A PARSON STREET
FIRST FLOOR, KEIGHLEY, WEST YORKSHIRE, BD21 3EY

Contents

Version and Changes Page

Document	AML Policy & Procedure
Current Version	5.0
Date Created	12th February 2016
Created By	Arshad Mehmood
Reviewed By	Taliq Hussain
Last Reviewed Date	18 December, 2020
Next Review Date	April, 2021
Responsible Person	Taliq Hussain

Summary of Changes

Version 2.9

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

Criminal Finances Act 2017 Version
3.0
Added and Implemented Anti-Bribery, Commission, accepting/offering Gifts/Traveling/ Accommodation cost policy.

Version 4.0

Updated following regulations in Version 5.0 under section "The Money Laundering Regulations 2019 in the United Kingdom".
The present policies are based on material made available by the relevant UK regulatory bodies. In particular Money Laundering and Terrorist Financing (Amendment) Regulations 2019 transposing 5th AMLD, Anti Money Laundering Guide, Regulation (EU) 2015/847 on information accompanying transfers of funds (the Payments Regulation) and the Payment Services Regulations (2017).

Version 5.0: EDD Policy for High-Risk Country along with Link transactions description

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 responsibility to ensure that the policies are implemented, both by me personally and also any other members for whom I am personally responsible. If 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 notwithstanding its translation into any another language, the English version shall be the definitive version, which shall be referred to for all legal purposes.

INTER CITY MONEY LIMITED
FCA: 514406 Co. Reg: 04279071
1A Parson Street, Keighley
West Yorkshire BD21 3EY
Tel: 01535 685754 Fax: 01535 685

Anti-Money Laundering Policy and Procedures Policy Statement

The present policies are based on the provision of the relevant UK regulatory framework. In particular Money Laundering and Terrorist Financing (Amendment) Regulations 2019 – transposing 5th AMLD, Anti Money Laundering Guide, Regulation (EU) 2015/847 on information accompanying transfers of funds (the Payments Regulation) and the Payment Services Regulations (2017).

What is money laundering and what the UK law requires (and the penalties for not following the law

What is money laundering?

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages:

- **Placement:** Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.
- **Layering:** Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.
- **Integration:** Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

The Criminal Finances Act 2017

The Criminal Finances Act 2017 makes important amendments to the Proceeds of Crime Act, the Terrorism Act and the Anti-terrorism, Crime and Security Act. It extends the powers of law enforcement to seek further information, recover the proceeds of crime and combat the financing of terrorism. It extends the powers of law enforcement to seek further information, recover the proceeds of crime and combat the financing of terrorism.
Criminal Finances introduces corporate offences of failing to prevent tax evasion which may apply to businesses who facilitate this criminal activity.

Tax Evasion

Tax evasion is a generic term to describe criminal conduct which involves individuals or businesses paying too little tax or wrongly claiming tax repayments by acting wrongly or dishonestly. Tax based fraud or evasion is generally investigated by Her Majesty's Customs and Revenue (HMRC) or by the National Crime Agency (NCA).
The principal tax fraud offences are:

- Fraudulent evasion of income tax
- Fraudulent evasion of VAT

- Cheating the public revenue
- Providing false documents or information to HMRC, and
- Fraudulent evasion of excise duty on imported goods or smuggling goods (eg cigarettes, alcohol)

The **Money Laundering Regulations** are secondary legislation in relation to money laundering. They make it a separate offence for relevant businesses not to have systems and procedures in place to combat money laundering.

The Regulations specifically require that relevant businesses should:

- Have systems in place to identify their customers and risk factors considerably
- Keep business records
- Have internal reporting mechanisms to allow reporting of suspicious activity
- Appoint a nominated officer (sometimes known as the Money Laundering Reporting Officer)
- Train staff on the law and training in how to recognise suspicious transactions
- Be registered as an MSB with the regulator (HMRC)

New Enhanced obligations on money service businesses according to **2019 Money Laundering Regulations** include a number of:

- The obligation on 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 verify the customer from the independent data sources.
- Special due diligence obligations for non-face to face customers and for customers who may be 'politically exposed'.
- Beneficial ownership – obligations to verify the identity of the individuals who make ultimate financial gains from business relationships or transactions. Amendments to regulation 28 require firms to update their records relating to the beneficial ownership of corporate clients. Firms also need to understand the ownership and control structure of their corporate customers and record any difficulties encountered in identifying beneficial ownership. Regulation 30A is a new requirement for firms to report to Companies House discrepancies between the information the firm holds on their customers compared with the information held in the Companies House Register.
- When a business relationship has been established, new requirements to establish customer source of funds/purpose of the transaction
- Obligation to take a 'risk-based approach' to all aspects of the AML policies for the business
- Policy of the company that all members of staff shall actively participate in preventing the services of the company from being exploited by criminals and terrorists for money laundering purposes. This participation has as its objectives:
- Ensuring the company's compliance with all applicable laws, statutory instruments of

regulation, and requirements of the company's supervisory body
- Protecting the company and all its staff as individuals from the risks associated with breaches of the law, regulations and supervisory requirements
- Preserving the good name of the company against the risk of reputational damage presented
- By implication in money laundering and terrorist financing activities making a positive contribution to the fight against crime and terrorists

To achieve these objectives, it is the policy of this company that:

- Every member of staff shall meet their personal obligations as appropriate to their role and position in the company
- Commercial considerations shall never be permitted to take precedence over the company's anti-money laundering commitment

The company shall appoint a Money Laundering Reporting Officer (MLRO), and a deputy to cover in his or her absence, and they shall be afforded every assistance and cooperation by all members of staff in carrying out the duties of their appointments.

Penalties and Sanctions

If a person or business fails to comply with the ML Regulations, they may face a civil financial penalty or criminal prosecution that could result in an unlimited fine and/or a prison term of up to 2 years.

HMRC also have the power to:
- Suspend or cancel a business' registration
- Ban or suspend individuals from having a role in a supervised business
- Issue a statement censuring the business.

HMRC will usually publish details of penalties and sanctions issued. For more information on the penalties please see https://www.gov.uk/guidance/money-laundering-regulations-appeals-and-penalties

Not complying with the Regulations may also lead to money laundering charges under the Proceeds of Crime Act 2002.

Financial Sanctions

UK financial sanctions apply within the territory of the UK and to all UK persons, wherever we are in the world.

Inter City Money Limited will undertake activities within the UK's territory and would comply with the EU and UK financial sanctions that are in force. Inter City Money Limited is established under

UK law, including our branches, will also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

Inter City Money Limited under EU law will comply with the EU financial sanctions that are in force, irrespective of where our activities take place.

OFSI works closely with the EU Commission and EU member states in implementing sanctions. The UK imposes sanctions applied by the UN and EU as well as a limited number of its own sanctions (e.g. Terrorist Asset-Freezing etc. Act 2010).

Inter City Money Limited would report to OFSI as soon as practicable if we know or have reasonable cause to suspect that a designated person has committed an offence. Inter City Money Limited report any transactions carried out for persons subject to sanctions or if they try to use our services.

We can obtain Information on the current consolidated list of asset freeze targets and persons subject to restrictive measures at:
https://www.gov.uk/government/organisations/office-of-financialsanctionsimplementation

Where can I find out more?

Following web-sites contain the details of different issues discussed in this documents:

- Financial Conduct Authority (FCA) website www.fca.org.uk
- HM Revenue & Customs (HMRC) www.hmrc.gov.uk/
- [Which has detailed information on anti-money laundering regulations.]
- Office of Foreign Assets Control (OFAC) www.treasury.gov/ofac
- HM Treasury www.hm-treasury.gov.uk

The Money Laundering Regulations in the United Kingdom

The legislation governing money laundering and Terrorist Financing and the fight against it is contained in the following:

1. Proceeds of Crime Act 2002
2. Terrorism Act 2000
3. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
4. Criminal Finances Act 2017
5. Regulation (EU) 2015/847 on information accompanying transfers of funds (the Payments Regulation)
6. Payment Service Regulations 2017
7. Money Laundering and Terrorist Financing (Amendment) Regulations 2019 – transposing 5th AMLD.

Our obligations

In accordance with our responsibilities, under the regulations, Inter City Money Limited has appointed a Money Laundering Reporting Officer (MLRO).

Our MLRO: Mr. Taliq Hussain

Tel: - +447870679430

Email: - Taliq@intercitymoney.com

Our obligations contain, but are not limited to:-

- Ensuring all staff of Inter City Money Limited are trained regularly in anti-money laundering
- Ensuring that they understand their training
- Adopting a risk-based approach to customer due diligence and enhanced due diligence including ongoing monitoring of any business relationships.

Money Laundering Reporting Officer

A MLRO is the person within an Organization who is responsible for overseeing all activity related to anti-money laundering matters.

As mentioned above Inter City Money Limited's MLRO is: **Mr. Taliq Hussain**

The MLRO's responsibilities include:

- Receiving disclosures from employees (also known as suspicious activity report-SAR).
- Deciding if disclosures should be passed on to the National Crime Agency (NCA).
- 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 SAR's 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
- Decision 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

Our Risk Based approach

a) Applying Due diligence at the start of customer engagement
b) This means identifying the customer and verifying the customer's identity on the basis of

documents, data or information obtained from a reliable and independent source.

c) Identifying where there is a beneficial owner who is not the customer, the beneficial owner* and taking adequate measures, on a risk sensitive basis to verify his identity (including in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure).
d) Creating policies and procedures that relate to customer due diligence, ongoing Monitoring, internal reporting and record keeping. If any suspicions are identified, then these should be raised to the MLRO for further investigation by completing the relevant internal Suspicious Activity Report (SAR) form which is included

*DEFINITION: A beneficial owner is a person who owns or controls more than 25% of the shares or voting rights in a body (e.g. Company/business) and hence, carries an element of control over the management of the Organization.

There have been several cases where failure to learn the identity of ultimate owners of a business, have led to penalties and fines being issued by the FCA.

It is a part of the money laundering regulations to practice satisfactory EDD whereby ultimate / beneficial owners have been clearly identified.

Use of An Agent

As Inter City Money Limited uses agents, we must enter into a written agreement or arrangement with the agent outlining what we expect them to do for us. In addition, we must obtain from the agent the customer information that was obtained according to the agreement or arrangement.

Our agents are required to fully comply with our procedures for client identification. We consider following factors:

- Perform the necessary background checks and due diligence, such as a recent change from another product/service provider, length of time in business, ownership structure, creditworthiness, financial viability, class of trade or industry, licensing and regulatory structure and other regulatory licensing or registration to which the MSB may be subject.
- Obtain appropriate additional information to understand the applicant's business, such as offering other MSB services, Agent's past record of legal and regulatory compliance, expected nature and level of transactions and customer base, and geographical exposure.
- Upon approval, conduct new agent AML/CFT training encompassing applicable AML/CFT requirements, AML Compliance program responsibilities, and MSB internal policies and procedures.
- Provide AML/CFT compliance materials, tools, and training to agents on an ongoing, periodic basis.
- Utilize a baseline risk assessment tool that monitors agent activity to measure transaction-related risk or identify agents that exhibit risk behaviours, such as structured transactions, customer identification sharing or biographical information sharing, higher volume

senders or payees, unusual and unexplained spikes, ratios or seasonal fluctuations in transaction volume, inferior data quality entered at point of origination or payment, related or poor quality of STR/SAR activity, higher volume agent-to-agent corridors, unusual agent patterns, or unusual product or service concentration.

- Provide prompt attention and remediation of risk behaviours by onsite or offsite contact with the agent, which may result in further training, or probation, suspension or termination of the agent.
- Provide guidelines and assistance to the agent to assess its own compliance program regime and to develop its own risk assessment based upon its unique risk profile for its products and services, customers and geography.
- Ensure compliance regime adherence to internal policies and external regulation, such as reporting suspicious or attempted suspicious activities, large transactions, monitoring the risk behaviours described above, reporting and recordkeeping, through periodic AML compliance program reviews.

Agent Monitoring

Agent monitoring is a very important element in an effective MSB AML/CFT program. While all agents will get adequate training, new or changing services or products, and poor individual judgment or performance, the risk-based approach requires a higher level of monitoring to locate and eliminate the few agents that knowingly or through willful blindness act in a way that may conceal their customers conduct from routine monitoring. The degree and nature of agent monitoring will depend on the transaction volume and principal volume of the agent with whom the MSB shares responsibility for effective AML/CFT, the monitoring method being utilised (manual, automated or some combination), and the type of activity under scrutiny. In applying a risk-based approach to monitoring, the degree of monitoring will be based on the perceived risks, both external and internal, associated with the agent,

The following are examples of common risk indicator that we as principal and our agents take care of:-

- Represent more than one participant
- Are reluctant to provide information regarding their customer's identity to the principal
- Record unusual or suspicious customer information (many transactions attributed to a single customer or customer details that may be false or incorrect)
- Have a high volume of business with single customer to a high-risk country
- Process a customer sending money to several destinations or the same recipient on the same day
- Have a pattern of customers in the office that doesn't support the turnover
- Have an unusually high transaction size
- Have a size and frequency of transactions that:
    a) Are different from the customer's normal pattern
    b) Have changed since the agency relationship was established
    c) Are higher than comparable agencies

d) Change significantly under new management of the agency

- Have transactions that seem unnecessarily complicated, or seem to use front men or companies.
- Undertake business outside normal business hours
- Have records in which fake identities repeat common fields, for example a different surname with all the other details like birth day and address the same
- Transactions too fast to be possible

Training and Awareness

Inter City Money Limited will provide appropriate training to its staff and agents with regards to money laundering and combating terrorism financing as successful control relies on both training and awareness. We will ensure:

- Enterprise-wide effort to provide all relevant employees and agents with at least general information on AML/CFT laws, regulations and internal policies.
- Applying a risk-based approach to the various methods available for training gives each MSB additional flexibility regarding the frequency, delivery mechanisms and focus of such training. Training schedule will be documented and training records will be maintained according to applicable record keeping requirements. A MSB should review its agent base and available resources and implement training programmes that provide appropriate AML/CFT information that is at the appropriate level of detail.
- Training may include onsite or offsite initial training (i.e., upon activation), and ongoing training via web-based programmes, periodic mailings or newsletters, password-protected informational websites or pop-up messages at point of origination. In conjunction with or in addition to such training, the MSB may provide periodic compliance program reviews involving a comprehensive assessment of the agent's and staff's compliance with internal and external AML regulatory requirements.

Each member of Inter City Money Limited staff is always ready to deal with the risks posed by their role. Their regular training keeps their knowledge and skills up to date. It covers: -

- The staff member's duties
- The risks posed to the business
- The business policies and procedures
- How to conduct customer due diligence and check customer's documents
- How to spot and deal with suspicious customers and activity
- How to make internal reports, including disclosures of suspicious activity data protection requirements
- Record keeping
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer)
- Regulations 2017: Part 7 of the Proceeds of Crime Act; and section 18 and 21A of the Terrorism Act

CDD (Customer Due Diligence)

Customer due diligence means:

- Identifying all customers and verifying their identity (more details below)
- Identifying all beneficial owners, where applicable, and taking adequate risk based measures to verify their identity
- Obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the customer, and the risk assessment
- Retain records of these checks and update them when there are changes Inter City Money Limited do customer due diligence when:
- Establishing a business relationship with a customer
- Identify and verify the customer when a money transmission transaction is of any value.
    a) Carrying out an occasional transaction with a customer of **GBP 8000 or more**.
- Money laundering or terrorist financing is suspected
- You suspect that information obtained for due diligence checks on a customer is not reliable or adequate

Non-compliance with Customer Due Diligence

If we find that customer is not complying while performing the customer due diligence measures, then we do not: -

- Carry out a transaction with or for the customer
- Establish a business relationship or carry out an occasional transaction with the customer.

You must: -

- Terminate any existing business relationship with the customer
- Consider making a suspicious activity report
- If no suspicious activity report is made, record the reasons why it is considered that a report is not required

Ongoing monitoring of a business relationship

Inter City Money Limited always keep the information collected for this purpose up-to-date. We checked them periodically and expired documents replaced with copies of newly issued documents

Simplified due diligence

Inter City Money Limited may apply a simplified form of due diligence in some cases. While risk assessing the customer to establish that they are low risk.

This does not mean we do not have to perform customer due diligence, we still required to verify customer and beneficial owner identity:

- Verifying the customer or beneficial owners' identity:

a) during the establishment of a business relationship or
b) use one document to verify identity
c) use information you have to determine the nature or purpose of a business relationship without requiring further information, for example, if your customer is a pension scheme you can assume what the purpose is

To apply simplified due diligence, you need to ensure that:

- Decision is supported by your customer risk assessment
- Enhanced due diligence does not apply
- While monitoring the business relationship or transactions we ensure that there is nothing unusual or suspicious
- It is not prevented by information on risk provided by HMRC or any other authority
- The customer is not from a high risk third country identified by the EU
- The customer is not a politically exposed person, a family member or a known close associate of a politically exposed person
- The customer is seen face to face as is any co-owner
- The source of funds or wealth are transparent and understood by our business
- The transaction is not complex or unusually large, that is, over £1 million although your risk assessment may indicate that a lower sum would be considered large in your geographical location
- where the customer is not an individual, that there is no beneficial ownership beyond that legal entity.

To decide whether a customer is suitable for simplified due diligence we consider among other factors the type of customer, the underlying product or service and the geographical factors, in our risk assessment. One factor, on its own, should not be taken to indicate low risk.

We consider all of the factors, for example a customer from another EU state is not automatically low risk simply because they are from the EU. All of the information we have on a customer must indicate a lower risk.

We record evidence, as part of your risk assessment, that a customer or service provided is eligible for simplified due diligence. We conduct ongoing monitoring in line with your risk assessment to ensure that the circumstances on which we based our original assessment have not changed.

We discontinue with simplified due diligence if we:

- Suspect money laundering or terrorist financing
- Doubt whether documents obtained for identification are genuine
- Circumstances change and your risk assessment no longer considers the customer, transactions or location as low risk

Customer due diligence on transactions below GBP 800

For transactions below GBP 800 where there's no ongoing business relationship we consider the money laundering and terrorist financing risks when deciding if you should do customer due diligence on a particular customer.

Money transmission businesses must obtain information on the payer and payee and verify the payer information on electronic transactions of more than GBP 2499 in 30 days and any cash transaction or anonymous e-money (no minimum threshold) to comply with the Regulation. However, HMRC expects that money transmission businesses should obtain and verify the identity of customers for all money transfers, regardless of value.

Identifying individuals

As part of your customer due diligence measures you must identify individuals. You should obtain a private individual's full name, date of birth and residential address as a minimum.

You should verify these using current government issued documents with the customer's full name and photo, with a customer's date of birth or residential address such as:-

1. A valid passport
2. A valid photo card driving licence (full or provisional)
3. A national identity card
4. A firearms certificate
5. An identity card issued by the Electoral Office for Northern Ireland

When verifying the identity of a customer using the above list of government issued documents, we take a copy and keep it in the customer's file.

Where the customer doesn't have one of the above documents we ask for the following:-

- A government issued document (without a photo) which includes the customer's full name and also secondary evidence of the customer's address, for example an old style driving licence or recent evidence of entitlement to state or local authority funded benefit such as housing benefit, council tax benefit, pension, tax credit.
- Secondary evidence of the customer's address, not downloaded from the internet, for example a utility bill, bank, building society or credit union statement or a most recent mortgage statement.

If Inter City Money Limited verify the customer's identity by documents, Inter City Money Limited see the originals and not accept photocopies, nor accept downloads of bills, unless certified (see "Additional measures to take") as described below:-

Photocopies identity documents can be accepted as evidence provided that each copy document has an original certification by an appropriate person to confirm that it is a true copy and the person is who they say they are for standard customer due diligence an appropriate person is for

example a bank, financial institution, solicitor or notary, independent professional person, a family doctor, chartered accountant, civil servant, or minister of religion.

The documents must be from a reliable source not connected to the customer. Inter City Money Limited check the documents to satisfy yourself of the customer's identity. This may include checking: -

- Spellings
- Validity
- Photo likeness
- Whether addresses match

More information on official documents and how to spot counterfeits and forgeries is published by the Home Office in their 'Basic Guide to Forgery Awareness'. Our Nominated Officer and other responsible person for performing transactions, should be aware of the issues within this and cascade relevant parts to staff as part of our training programme.

If a member of our staff has visited an individual at their home address. A record of their visit may corroborate the individual's residential address (instead of the need for a second document). This should be covered in the risk assessment.

Where an agent, representative or any other person acts on behalf of the customer we ensure that they are authorised to do so, identify them and verify the identity using documents from a reliable and independent source.

Know Your Customer (KYC) / Know Your Business (KYB)

KYC & KYB requirement are key aspects in Inter City Money Limited relationships with its clients.

The requirement to carry out customer due diligence and enhanced due diligence has given it an increased importance. Our Due Diligence (DD) policy requires us to request the following;

Clients who wish to remit payments will follow Inter City's threshold specified in this document.

Compliance Committee

Our Compliance Risk Committee is responsible for the implementation of Compliance Policies and programs and in case of any emergency Committee will report board directly.

Our Compliance Committee Consist of three senior members

1. Mr.Taliq Hussain
2. Mr. Mudassar Hussain
3. Mr. Kaleem Bajwa

QUICK GUIDE FOR CDD/EDD

TRANSACTIONS THRESHOLD

Mandatory Fields:

You must need to collect following information while making Transaction.

- First Name
- Last Name
- Full Address
- Date of Birth
- Nationality
- Place of Birth
- Phone No
- Job description
- Relationship to Receiver
- Purpose of Transfer
- Source of Fund

For Cash Transaction

Account	Frequency	Requirments
£1-2499	30 Days	1 Photo ID
£2500 (Above & Equivalent)	30 Days	1 Photo ID , Proof of address /Electronic Verification, Bank Statement/ Payslip to verify the Funds, Source of Fund declaration

For Online Transaction

Account	Frequency	Requirments
£1-3999	30 Days	1 Photo ID
Above £4000 (Above & Equivalent)	30 Days	1 Photo ID , Proof of address /Electronic Verification, Bank Statement/ Payslip to verify the Funds, Source of Fund declaration

Account	Frequency	Requirments
Above £5000 (Above & Equivalent For Cash)	90 Days	1 Photo ID , Proof of address / Electronic Verification, Bank Statement/Payslip to verify the Funds, Source of Fund declaration
Above £7500 (Above & Equivalent For Online)	90 Days	1 Photo ID , Proof of address / Electronic Verification, Bank Statement/Payslip to verify the Funds, Source of Fund declaration

Attention

The Threshold will be applied from 13th July 2021 which are based on ICM Risk Assessment. The Aggregated monthly amounts are calculated on calendar days, meaning, the last 30 days prior to the day order was placed. E.g For orders placed on 13th of July the aggregated amount will be calculated from 13th of June 2021.

Your all the transactions will be screened in accordance with these thresholds.

Documents required when the above threshold are reached in a single or aggregate transaction in Calendar month.

Important Notice

Please note that we may request proof of address, if information provided does not match or is incomplete

These thresholds are for reference only, Compliance department may ask for further documentation/information irrespective of transaction amount. Transactions placed just below the threshold shown above will be treated as unusual transactions and further actions will be taken accordingly.

£12,000 aggregated in a year, will require Proof of occupation. In some cases if it is a single transaction of more than £12,000 proof of funds and proof of occupation will be required.

For online Bank Transfers, the 1-year limit will be £15000. Once this limit will be exceeded we will be required proof of funds and proof of occupation.

Inter City Money

Proof of ID: A non-expired Government issued document which must contain the full name, photograph and date of birth of the sender. We accept only the following documents as valid proof of ID:

- Passport
- Driving license
- National identity card
- Residence permit card

Proof of Address: Must contain as a minimum the full name and full address of the sender. We accept only the following documents as valid proof of address (Utility Bill, Bank Statement, any government issued IDs/letter, Wage Slip etc.)

Proof of source of funds: Acceptable documents include but are not limited to the following documents. INTER CITY MONEY may ask for additional documents as part of EDD:

- **Bank statement:** the transferred money must be in the bank account for 2 clear calendar days, funds came into a bank a/c on a Monday, can be transferred on the following Thursday.
- **Pay slip:** any pay slip issued within the last 60 days from the date of transaction. Letters of contract/employment are also acceptable.
- **Loan confirmation letter/agreement:** letter/agreement must be dated within 30 days from the date of transaction and/or there must be a clear account trail showing the original source of the money being transferred. This is only acceptable if funds were transferred electronically from the same account.
- **Property mortgage/sale documents:** must be dated within 30 days from the date of transaction and/or there must be a clear account trail showing that the same money is the one being transferred, and funds must be transferred electronically from the same account. Such documents include completion statement and confirmation from solicitor.
- **Other documents:** Proof of benefit, letter from accountant/solicitors, tax return, P60

Attention

- Bank transfer of any amount must be made from the sender's personal bank account
- Proof of Address: Must contain as a minimum the full name and full address of the sender.
- INTER CITY MONEY accepts only the documents listed above as valid proof of address.
- Declaration of Purpose of Transfer and Source of Fund: Declarations are valid for one day only.

EDD (Enhanced Due Diligence)

It is Inter City's Policy that EDD is applied to relationships which present a higher risk of money laundering and/or sanctions.

CDD and EDD is conducted on appropriate customers using a risk-based approach. Additional procedures and review is undertaken for customers who have a high-risk score as part of the customer risk assessment; PEPs and Correspondent Business relationships are also defined as requiring EDD.

The KYC procedures for higher risk customers are completed by following the guidance in the P&P's, which includes obtaining information on the source of funds by confirming the origination of the funds (e.g. salary, personal savings, investments/ loan, personal funding, business, properties etc.) and the source of wealth (i.e. confirmation of how the customer has accumulated their wealth, establishing whether they have any savings, shares, property or inheritance. Evidence must be provided by the customer of the source of wealth).

In addition, adverse media searches are required to be performed on the top agents, including ultimate beneficial owners, to identify whether there is any adverse news on the customer. This check serves as an additional check to see whether the customer has been involved in any criminal activity. Approval for the opening of all high risks account is required by the Compliance Department. For accounts classified as high risk, a full file review is conducted annually, however for PEPs and Correspondent Business, this is supplemented by performing regular reviews of transactional activity, as part of the EDD process.

We are using LEXIS NEXIS platform to perform adverse Media Check.

All customer files will be reviewed and enhanced in accordance with the revised standards at periodic review stage. Compliance will be assessing these customer files, as part of its Compliance Monitoring Plan.

Ongoing Due Diligence

Ongoing Due Diligence is undertaken periodically (24 months for Low risk, 18 months for Medium Risk and annually for High risk) and enhanced due diligence is conducted at both on-boarding and periodic file review stage, where the account is deemed to be High Risk.

Inter City is required to define and implement procedures where it becomes aware that the customer's circumstances have changed. Specific trigger events may then lead to a re-fresh of CDD information, including identification documentation, and a re-review of the customer's risk assessment rating.

ICM's Staff Obligations:

As a PSD agent of Inter City Money Limited You must perform EDD when:

- If we have identified in our risk assessment that there is a high risk of money laundering or terrorist financing.
- HMRC or another supervisory or law enforcement authority provide information that a particular situation is high risk
- a customer or other party is established in, or operates in a high risk third country identified by the EU, FATF or HMT.
- Person has given you false or stolen documents to identify themselves (immediately consider reporting this as suspicious activity)
- A customer is a Politically Exposed Person, an immediate family member or a close associate of a Politically Exposed Person.
- The transaction is complex, or unusually large, or with an unusual pattern and have no apparent legal or economic purpose
- A customer is a third country national who is applying for residence rights in or citizenship of an EEA state in exchange for transfers of capital, purchase of a property, government bonds or investment in corporate entities in that EEA state.

Inter City Money Limited **Enhanced Due Diligence (EDD)** policy is designed to obtain as much information as possible in order to ensure the validity of the transaction and that Inter City Money Limited complies with ML Regulation (2017), POCA (2002), Terrorism Act (2000) and the EU Money Laundering Directives.

The checking is meant to be thorough in its nature to ensure that we record enough information that will help us form a true picture of the client. As follows:

1. 1 form of photographic ID
2. 1 form of proof of address
3. Disclaimer/questionnaire for the origin of funds not being derived from the proceeds of crime
4. Source of funds verification in the form of a recent Bank statement showing the movement of funds.
5. If funds have been generated/received via a 3rd party (i.e., solicitor for a house sale). Then additional correspondence or documentation is to be collected and put-on file.
6. If unusual Documents you found, please consult with MLRO and External Consultant for further verification.

Additional Measures to Take if Country is identified as High-Risk Country by EU, FATF or HM Treasury.

According to Financial Action Task Force, Due to strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing, FATF places **PAKISTAN** under increased monitoring, it means the Pakistan has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the 'grey list'.

http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2020.html

Additional Measures to Take:
Pakistan is High Risk Country so in case of HIGH RISK EDD is mandatory and ICM Staff must do more to verify identity and scrutinise the background and nature of the transactions than for standard customer due diligence. How this goes beyond standard due diligence must be made clear in your risk assessment and procedures. For example:

- Obtain additional information or evidence to establish the identity from independent sources, such as more documentation on identity or address or electronic verification alongside manual checks.
- Take additional measures to verify the documents supplied such as by checking them against additional independent sources, or require that copies of the customer's documentation are certified by a bank, financial institution, lawyer or notary who are competent at document inspection and impostor detection, or a person from a regulated

industry or in a position of trust

- If receiving payment ensure it is made through a bank account in the name of the person you are dealing with.
- take more steps to understand the history, ownership, and financial situation of the parties to the transaction
- In the case of a politically exposed person establish the source of wealth and source of funds
- Carry out more scrutiny of the business relationship and satisfy yourself that it is consistent with the stated purpose.
- Measures which must be taken when either party to a business relationship, or relevant transaction is established in a high-risk third country (a business is established in a country if they are incorporated there, is their principal place of business, or they are regulated there as a financial or credit institution; an individual is established in a country if they are resident there)
    a) Obtain additional information on the customer and the customer's beneficial owner
    b) Obtain additional information on the intended nature of the business relationship
- Obtain information on the source of funds of the customer and of the customer's beneficial owner
- Obtain information on the reasons for the transaction
- Obtain the approval of senior management for establishing or continuing the business relationship
- Enhance monitoring of the business relationship by increasing the number and timing of controls applied, and select patterns of transactions which require further examination

Risk Based Approach

Current regulations state that a financial services company must adopt a risk based approach to all clients. Inter City Money Limited has acted on this and categorized the risks posed by clients on the following basis;

- Geographic area of operation product
- Customer
- Delivery channel

Clients of Inter City Money Limited will be classified according to their risk level IE:

- Low Risk
- Medium Risk
- High Risk

The determination of the risk level will be the responsibility of the MLRO/NO. If a client is a high or medium risk then Enhanced Due Diligence will be practiced and any ongoing business activity should be monitored by senior management in practice, the MLRO.

******All high-risk client accounts will only be opened on the approval of the MLRO******

(PEPs) Politically Exposed Persons

Politically exposed persons are persons that are entrusted with prominent public functions, **held in the UK or abroad.** Typically, this includes

- Members of parliament or similar legislative bodies includes regional governments in federalized systems and devolved administrations, including the Scottish Executive and Welsh Assembly, where such bodies have some form of executive decision-making powers does not include local government in the UK but it may, where higher risks are assessed, be appropriate to do so in other countries.
- Members of the governing bodies of political parties generally only apply to the national governing bodies where a member has significant executive power (e.g. over the selection of candidates or distribution of significant party funds). political parties who have some representation in a national or supranational Parliament or similar legislative body.
- Members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstance this includes judges of the Supreme Court does not include any other member of the judiciary
- Members of courts of auditors or boards of central banks
- Ambassadors, and high-ranking officers in the armed forces where persons holding these offices on behalf of the UK government are at Permanent Secretary or Deputy Permanent Secretary level, or hold the equivalent military rank e.g. Vice Admiral, Lieutenant General or Air Marshal
- Members of the administrative, management or supervisory bodies of state-owned enterprises this only applies to for profit enterprises where the state has ownership of greater than 50% or where information reasonably available points to the state having control over the activities of such enterprise
- Directors, deputy directors and members of the board, or equivalent of an international organization. Includes international public organizations such as the UN and NATO. does not include international sporting federations

The Regulations require that family members of PEPs must also have enhanced due diligence measures applied to them. For these purposes, the definition of “family member” includes:

- Spouses/civil partners of PEPs;
- Children of PEPs and their spouses/civil partners; and parents of PEPs

In order to comply with regulations, Inter City Money Limited will ensure that all accounts relating to PEP’s must;

a) **Be approved by the MLRO**
b) **Be subject to enhanced due diligence**

Sanctions

The UK financial sanctions regime plays an important part in delivering the Government's foreign policy objectives. It is also used by the government to prevent and suppress the financing of terrorism and terrorist acts.

- Any client found on a sanctions list will be declined and no transactions will be carried out
- Our bespoke remittance software automatically identifies sanctioned entities.

Enhanced Customer Due Diligence (EDD)

Clients

There are certain clients who are not based local to any of our branches or agents and hence cannot provide their ID/V in person.

For such clients 'proof of Identity' requirements need to be sent via post and should be Certified True Copies from Originals.

Certified copies must sign by a person of appropriate experience and position, EG;

- Solicitor
- Bank Staff/official Post Master
- Doctor
- Chartered Accountant
- Police Officer

*****Facsimile copies are not acceptable*****

Proof of Funds

Clients who are making remittances and are required to prove the source of the funds being remitted. For example:

- If funds are from a Bank or savings account, customers should be requested to provide their latest bank statement [Last 2 Months]
- If funds are from a loan or remortgage then the loan/mortgage agreement should be provided
- Credit card statement or cash advance receipt
- Statement showing proceeds from sale of an asset or assets

If large cash funds are presented and the client advises that funds have been kept at home (IE under the mattress) then these funds require declaration to HMRC and MLRO to decide on the instruction

Linked Transactions

Definition

Transactions that part from a single arrangement or scheme or part of a series of transactions are known as "**Link transaction**".

The Customer may attempt to disguise a remittance payment by breaking into several smaller sums and utilizing his/her friend or close associates to send the funds usually to a single beneficiary.

In anticipation that a customer will avoid requiring proof of funds and have structured transactions in the reaching the limit amount, the customer may divide the amount among his / her friends and send the money at the same time to a single beneficiary. In this case, our remittance front-end IT system is highlighting the records based on name or contact number similarity and will assist the Compliance team towards detecting link transactions.

Compliance team must exercise personal Judgement and consider the following:

1. Are the number of transactions carried out by the same customer within a short period?
2. Could several customers be carrying out transactions on behalf of the same individual or group individuals?
3. In the case of money transmission, are several customers sending payments to the same individual?

We are catering Link Transactions by applying the following checks:

- The system will trigger Link Transactions if the full name gets a match with other customers.
- The system will trigger a link transaction if the last 07 digits of the receiver's mobile number get a match with any other sender.
- In case if the mobile number is not available, we make it mandatory in our system to enter the receiver's Father's Name.

In short Linked transactions may be a series of transactions by a legitimate customer, or they may be transactions that appear to be independent but are split into two or more transactions to avoid detection. This typically happens when a customer tries to avoid antimoney laundering controls by splitting transactions into several smaller amounts, below the level at which you check ID or enquire about the source of funds. Inter City have systems to detect linked transactions, and to undertake enhanced due diligence on them, and report any suspicious activity when they're detected.

The value of the transaction here means the gross value of the transaction, not the value of your commissions, fees, or charges.

- Inter City put in place systems to monitor customers' transactions to identify linked

transactions. For example, to identify linked transactions you must be able to associate a series of money transfers made by the same customer to a recipient or several recipients over a period of time. Also, Inter city's system can associate a series of money transfers made by different customers to the same recipient over a period of time.

- Inter City's systems can identify linked transactions that are conducted through all agent's locations.
- There is no specific period over which transactions may be linked, after which enhanced due diligence is not necessary. The period depends on the customers, product, and destination countries.
- HMRC recommends that businesses consider checking for linked transactions over a minimum rolling 90-day period. HMRC may check that you have an adequate system in place and are operating it effectively.

- A transaction like one to Many and many to one
- Identification of Customer based on Phone Number or Father name
- If the beneficiary is registered twice system identifies that and trigger that the Beneficiary already exist

Example 1

Multiple customers made transactions to similar beneficiary/beneficiaries by using our one of Branch/Agent location

Sr. No	Date	Branch/Agent Prefix	Customer Name	Beneficiary Name
1	01-12-2020	ABC	Mr. A	Mr. X
2	01-12-2020	ABC	Mr. B	Mr. X
3	01-12-2020	ABC	Mr. C	Mr. X
4	01-12-2020	ABC	Mr. D	Mr. X

Link transactions do not involve any fixed number of Transactions or Amounts, the aim is to avoid identification requirements and due diligence checks.

Hint: Link transactions mostly involve the nominal amount.

Example 2

Multiple customers made transactions to similar beneficiary/beneficiaries by using our multiple Branch/Agent locations.

Sr. No	Date	Branch/Agent Prefix	Customer Name	Beneficiary Name
1	01-12-2020	ABC	Mr. A	Mr.
2	01-12-2020	BCA	Mr. B	Mr.
3	01-12-2020	CBA	Mr. C	Mr.
4	01-12-2020	DBA	Mr. D	Mr.

Single customer made transactions to similar beneficiary/beneficiaries by using our multiple Branch/Agent locations.

Sr.No	Date	Branch/Agent Prefix	Customer Name	Beneficiary Name
1	01-12-2020	ABC	Mr.	Mr.
2	01-12-2020	BCA	Mr.	Mr.
3	01-12-2020	CBA	Mr.	Mr.
4	01-12-2020	DBA	Mr.	Mr.

Example 3

Multiple customers remitting money to a similar beneficiary in multiple days by using our Branch/Agent location.

Sr.No	Date	Branch/Agent Prefix	Customer Name	Beneficiary Name
1	01-12-2020	ABC	Mr.A	Mr.
2	02-12-2020	ABC	Mr.B	Mr.
3	03-12-2020	ABC	Mr.C	Mr.
4	04-12-2020	ABC	Mr.D	Mr.

Single customer remitting money to a similar beneficiary in multiple days by using our multiple Branch/Agent location.

Sr.No	Date	Branch/Agent Prefix	Customer Name	Beneficiary Name
1	1 -12-2020	ABC	Mr.	Mr.
2	2 -12-2020	BCA	Mr.	Mr.
3	3 -12-2020	CBA	Mr.	Mr.
4	4 -12-2020	DBA	Mr.	Mr.

This kind of link transaction can only be tracked by the mean of beneficiary' details, at the point where you found the repetition of Beneficiary Name or Contact Number you must need to confirm it with the appropriate source or refer the case of suspiciousness to the compliance department at first instance.

Special Instructions

Link transactions may have different manners; it's not fixed as described above. In addition to the link transactions, you must need to Flag the transaction as suspicious where:

- The beneficiary is not aware of the remitter's details e.g. Name, Origin of Transaction, ambiguous about the transactional amount or shows any kind of suspicious behavior

- The single beneficiary is favored repetitively
- Single Bank Branch facilitate payments at very high extend
- Payments of single or multiple agents being paid from same station/location consecutively
- Name change request for most transactions

Special Note

If you found any suspiciousness, you're firmly advised not to disclose the suspiciousness to anyone but to the Compliance Manager or MLRO.

Sanctions List and Politically Exposed Persons (PEPs)

A consolidated list of targets listed by the United Nations, European Union and United Kingdom under legislation relating to current financial sanctions regimes will be integrated to our remittance front-end IT system. Our system will automatically detect if both the client's name and receiver's name match with the names in the sanctions list.

ID System

A unique ID number will be assigned to each client. Clients are encouraged to use their ID number in all communications with us for security purposes. The outcome is that we can assure that we only deal with the right person and prevent usage of client's account by others.

Client must give the unique ID number every time he/she does a transaction. Identity checks should be done by asking security questions such as date of birth, postcode, and contact numbers.

These checks are strictly implemented before proceeding with the transaction.

Automated System and Controls

Compliance Issue

The following AML set of rules will trigger the system to hold the transaction:

- Initial limit of GBP 1 for incomplete KYC requirements
- Quarterly limit of GBP 5000 for the Sender requires declaration document to be completed
- Sender added more than 5 active beneficiaries
- Both sender and beneficiary names match with those names in the Sanctions List.

Information About Our Services to Potential Clients

Inter City Money Limited staff are not expected to carry out customer due diligence or enhanced due diligence procedures with a client where the meeting is merely to provide information to a prospective client about our services or is a first interview/discussion prior to a relationship being established.

Private Clients

In accordance with our obligations to satisfy ourselves as to the identity of a client and in accordance with the principles of Know Your Client (KYC) the procedures mentioned previously will be carried out.

After initial contact with the proposed client, the staff member is required to obtain/complete the following documents/information: -

- Sufficient information outlined in paragraph 9 to enable an identification check
- Account opening documents

The client will be informed that the information is necessary in order to enable Inter City Money Limited to satisfy itself as to his or her identity in accordance with our obligations under anti-money laundering legislation.

The information will contain but will not necessarily be confined to:

1. Full name
2. Date of birth
3. 3 Years of Address history

The information obtained will be verified by paper identification to include:

a) 1 photographic Identification
b) 1 utility bill less than 3 months old

In the event of positive identification nothing further is required and account opened as usual.

Where an applicant produces non-standard documentation staff should not cite the Money Laundering Regulations 2017 as a reason for not opening an account. The matter should be referred to Compliance for a decision EG:

- Fake or tampered identification

Where the instruction is to refer the matter to Compliance the client should be informed that there is a problem with the identification and clarification needs to be sought from Compliance.

Such clearance or refusal to establish a business relationship or open an account will be available with a reasonable period of time. In practicing KYC, Inter City Money Limited staff should satisfy themselves as to the rationale behind the instruction or business. Furthermore, they should be satisfied that instructions by a client are rational and make good business sense. A risk-based approach across the business is mandatory

INDIVIDUALS SEEN IN PERSON

The procedure to be followed in all cases with a new client will be as follows: -

a. Obtain acceptable photographic identification and photocopy same
b. A second independent verification of the address of the client will be obtained it will be photocopied and retained.

****NB: it must be a recent document not older than 3 months**

Note the unique reference number of the photographic identification on the account opening forms. The unique reference number will be: -

- Passport number
- Driving license number
- National identity card number

c. Certify the documentation by signing and dating and including the words EG: 'original seen'

INDIVIDUALS NOT SEEN IN PERSON

Original documents should not be sent through the post. Additional checks are required. These include one or more of the following;

- Additional documents at least one other photographic and one other address
- Certification, by a regulated entity
- First payment from an account in the client's name from a regulated entity.

CORPORATE CLIENTS

Inter City Money Limited offers a bespoke service for all commercial and corporate clients. Our services are tailored to best suit the needs for those firms who require specialist support and wish to maximize their profitability and protect their bottom line against adverse currency fluctuation.

RELATIONSHIP

Once we have a client signed documents and ID back, the business manager will either accept or reject the facility request. Subject to all documents being in place and business relationship approved, our relationship will commence and we will be obliged to offer services and support in line with our customer service standards. In turn, business customers will be expected to maintain their business and transactions according to our policies and procedures.

The points below are to be noted:

- In adopting a risk-based approach staff should ensure they understand the company's legal form structure and ownership.
- The following information/documents must be obtained/completed in respect of corporate clients: -
    I. Account opening documents

II. Full corporate name
III. Corporate registered number
IV. Corporate registered office
V. Corporate trading address

- Additionally, in respect of private companies Inter City Money Limited requires the names of all directors and the names of beneficial owners holding over 25%.
- Verification of ownership shall be by an online search of Companies House or other electronic search engine for companies.
- The identity of all Directors, beneficial owners and all authorized signatories will be verified.
- It is important that Inter City Money Limited is satisfied that a person acting on behalf of a corporate client has authority to do so. Evidence of such authority is required on the account opening document
- Corporate and Legal Entities provide an attractive vehicle for money laundering. The use of "brass plate" or shell companies is common place. Care must be taken to verify the identity of the client (i.e., the Company). Limited liability partnerships are to be treated as corporate clients.

*NB Where it is clear that the client in question is a shell or "dummy" company this business shall be declined and the matter referred to the MLRO.

- In order to verify the information provided by the corporate client, the following procedures are to be followed: -
  I. Registered number
  II. Registered corporate name and any trading name
  III. Registered address and any separate trading address
  IV. List of Directors
  V. List of beneficial owners and shareholders
  VI. Memorandum and Articles of Association

- Publicly listed companies whether UK or non-UK are generally considered to be low risk.

When they are listed on a recognized or approved stock exchange no further identification steps are required.

Obligation of customers to provide information (CORPORATE BODIES/ TRUSTS/ CHARITIES)

Corporate bodies in the UK, who are not listed on a regulated market have obligations to keep a register of people with significant control (a PSC register) and must provide this information when requested. When a corporate person enters into a transaction with a money service business you can request that they provide the following information: -

- Name, registered number, registered office and principal place of business

- Names of the board of directors or equivalent body
- Names of the senior person responsible for its operations
- The law to which it is subject
- Its legal and beneficial owners
- Its memorandum of association or similar documents

Guidance on the requirements to maintain PSC registers is available at:-

http://www.gov.uk/government/publications/guidance-to-the-people-with-significant-control-requirements-for-companies-and-limited-liability-partnerships.

This information will assist in identifying beneficial owners but for other information we need to ask for other information need to verify their identity, for example the address or date of birth of the individual.

Trustees have similar obligations to tell you that they are acting as a trustee, to identify all of the beneficial owner of the trust and any other person that may benefit.

Beneficial owners

Inter City Money Limited identify the existence of any beneficial owners (the section on customer due diligence gives information on who is a beneficial owner). Inter City Money Limited verify the beneficial owner's identity so that we are satisfied that we know who the beneficial owner is. If it is a legal person Inter City Money Limited take reasonable measures to understand the ownership structure.

Inter City Money Limited will not have satisfied your obligation to identify, verify and understand the structure of a beneficial ownership if we rely solely on the information contained in a register of persons with significant control.

Where a customer is incorporated and in exceptional circumstances, where we have made unsuccessful attempts, and have exhausted all ways, to identify the beneficial owner of a corporate body we may treat the most senior person managing the customer as the beneficial owner. Inter City Money Limited keep records of all the steps you have taken to identify the beneficial owner and why we have been unsuccessful.

Staff Training

One of Inter City Money Limited key controls in mitigating the threat of being used for money laundering is having staff that are aware of and alert to the threat. All staff, whether on a full-time, part- time or contract basis, are made aware of our anti-money laundering policy, manual and the obligations arising from them for both themselves and Inter City Money Limited. We provide training on anti-money laundering

This training comprising two key elements: -

a) **Induction Training -** The MLRO is responsible for identifying relevant new staff who are required to undertake induction training. The training is provided by the MLRO or the MLRO will engage external AML Advisors and is face to face training. The content of the training includes awareness training, covering Money Laundering and Terrorist Financing.
b) Understanding of the subject matter is assessed throughout the training through case studies. Until a new member of staff has been signed off as competent no direct customer contact is allowed.
c) **Refresher Training -** all relevant staff will must undertake face to face refresher training on an annual basis. The training is provided by the MLRO or the MLRO will engage AML Advisors and assessment of staff understanding is carried out throughout the training.

Inter City Money Limited impart Training to our employees in one or the other following ways to keep their knowledge up to date: -

- Face to face training through external advisors
- Online training through external advisors
- HMRC webinars
- Reading publications
- Meeting at regular intervals to look at the issues and risks

Inter City Money Limited will obtain acknowledgement from staff that they have received the necessary training by requesting staff to sign their attendance at training sessions. Overall monitoring of attendance is recorded manually and stored on the AML file.

Record Keeping

Inter City Money Limited keeps the records of customer due diligence checks and business transactions:

- For 5 years after the end of the business relationship
- For 5 years from the date an occasional transaction was completed
- Keeping supporting records for 5 years after the end of a business relationship
- Keeping the records from closed branches or agents

The records should be reviewed periodically to ensure, for example, that a fresh copy of expired documents, such as driving licenses or passports are held. This review need only include ongoing relationships.

Inter City Money Limited will not keep the customer transaction records that are part of a business relationship for more than 10 years, where a business relationship is ongoing.

After the period above the records must be deleted unless you are required to keep them in relation to legal or court proceedings or any other legislation.

Inter City Money Limited risk assessment and policies, controls and procedures must be kept up to date and be amended to reflect any changes in our business.

Inter City Money Limited can keep records in the form of original documents or copies in either hard copy or electronic form. Copies should be clear and legible. The aim is to ensure that the business meets its obligations and, if requested, can show how it has done so.

This evidence may be used in court proceedings.

If someone else carries out customer due diligence for you, you must make sure that they also comply with these record keeping requirements. You must be able to demonstrate that records of customer due diligence checks carried out by an outsourcing service, and which are stored on their server, will be available to you should you wish to move to another service or should that service go into liquidation.

All electronic records must be subject to regular and routine backup with off-site storage.

THE PROCEEDS OF CRIME ACT 2002

SUSPICIOUS ACTIVITY

The Proceeds of Crime Act 2002 (POCA) requires (amongst other things) that when in the course of business a member of staff of Inter City Money Limited comes across what is described as Suspicious Activity that it should be reported in the first instance to the MLRO.

There is no definitive list of what constitutes suspicious activity, however if the principles of KYC are rigorously applied then in the course of conducting business with the client sufficient information should be available, to make a judgment about what constitutes suspicious activity in each case.

When suspicious activity is suspected, the following procedures will be followed: -

a) The person suspecting should immediately make a written report or e- mail to the MLRO
b) if urgent telephone first, then follow up with a written report
c) no discussion with other members of staff should take place
d) a record of the date and time of report should be recorded
e) Acknowledgement of the receipt of the report should be obtained from the MLRO. This can be done via a receipt email from the MLRO.
f) New suspicion of the same client means a new report must be made Failure to report knowledge or suspicions of laundering of the proceeds of crime2:

Maximum Five years imprisonment and/or an unlimited fine

Tipping Off

Any staff member needs to make a judgment 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. Maximum 2yrs imprisonment/or an unlimited fine.

MONEY LAUNDERING

It is an offence to conceal, disguise, convert, transfer or remove criminal property from the United Kingdom:

a. Maximum Fourteen years imprisonment and/or an unlimited fine
b. Section 330 of the Proceeds of Crime Act 2002
c. Section 333a of the Proceeds of Crime Act 2002

It is an offence to enter into or become concerned in an arrangement which he knows or suspects facilitates the acquisition retention use or control of criminal property by or on behalf of another

a) Maximum Fourteen years imprisonment and/or an unlimited fine
b) It is an offence to acquire use or have possession of criminal property.
c) Maximum Fourteen years imprisonment and/or an unlimited fine

GENERAL

If in doubt report your suspicion to the MLRO, you have then complied with your obligation. He will use his own judgment whether to report further to National Crime Agency.

All contact with Law Enforcement Agencies will be handled by the MLRO or his deputy.

The MLRO will be responsible for providing information and updates to the legislation as and when they occur.

Inter City Money Limited consider any failure to comply with any of the relevant legal or regulatory requirements by any member of staff to be gross misconduct and will lead to immediate dismissal of that member of staff.

- Section 327 of the Proceeds of Crime Act 2002
- Section 328 of the Proceeds of Crime Act 2002
- Section 329 of the Proceeds of Crime Act 2002

NCA (National Crime Agency)

Introduction

NCA tackles serious organized crime that affects the UK and its citizens. This includes Class A drugs, people smuggling, human trafficking, major gun crime, fraud, computer crime and money laundering.

Reporting to NCA

Regulations oblige us to report any activity which is deemed illegal or a threat (including potential threat). The document which is used in the industry to inform NCA is called a Suspicious Activity Report or commonly referred to as a "SAR".

*NOTE

It is the role of the MLRO of Inter City Money Limited to submit SAR's to NCA /UKFIU.
At no cost should Inter City Money Limited staff makes direct contact.

SAR (Suspicious Activity Report)

Introduction

A SAR is a piece of information, usually found on a form, which alerts law enforcement (NCA) about certain clients and/or their activity.

Inter City Money Limited has their own internal SAR document which is annexed in this document.

Q. Who should complete a 'SAR'?

A SAR can be completed by a member of staff who wishes to inform the MLRO about their suspicions, no matter how small or great.

Q. When to complete a 'SAR'?

A SAR should be completed as soon as suspicious activity has been detected, has taken place or is about to take place.

Triggers for raising a SAR:

The following are examples triggers are and just for guidance. Ultimately, a person may just have a series of small suspicions which when combined, justify raising a SAR.

- Unusual clients or customers / people making unusual requests
- Customers who are not telling the truth or concealing known information Out of sync payments / payments do not make sense
- Large / Bulky payments
- Customers who provide false documentation are clear evidence that payments are fraudulent
- Clients who have been making payments more frequently and cannot offer suitable or unusual explanation as to why.

New customers

Inter City Money Limited consider following in deciding risk and whether or not to submit a suspicious activity report when we take on new customers: -

- Checking the customer's identity is difficult
- The customer is reluctant to provide details of their identity or provides fake documents
- The customer is trying to use intermediaries to protect their identity or hide their involvement
- No apparent reason for using your business's services – for example, another business is better placed to handle the transaction
- Part or full settlement in cash or foreign currency, with weak reasons
- They, or associates, are subject to, for example, adverse media attention, have been disqualified as directors or have convictions for dishonesty.

Regular and existing customers

Inter City Money Limited consider following when deciding risk and whether or not to submit a suspicious activity report in relation to our regular and existing customers:-

- The transaction is different from the normal business of the customer
- The size and the frequency of the transaction is different from the customer's normal pattern
- The pattern has changed since the business relationship was established there has been a significant or unexpected improvement in the customer's financial position.

Transactions

Inter City Money Limited consider following when deciding risk and whether or not to submit a suspicious activity report in relation to the transactions we carry out:-

- A third party, apparently unconnected with the customer, bears the costs, or otherwise pays the transaction costs
- An unusually big cash or foreign currency transaction
- The customer won't disclose the source of the funds
- Unusual improvement of third parties, or large payments from private funds, particularly where the customer appears to have a low income
- Unusual source of funds

5 Step process to completing a SAR

1) Locate blank SAR document
2) Complete
3) Fax/Email directly to MLRO
4) Await confirmation from MLRO
5) Do not inform anyone*

Once a SAR has been completed and sent to the MLRO, the person should not inform any one or discuss their concerns with colleagues etc. Once the SAR has been received, the MLRO will revert with further instructions / guidance.

***Tipping off applies.**

Risk Assessment of Our Business

As per the Money Laundering Regulations, each PI must exercise a 'risk-based approach' to its customers, products and business practices.

Inter City Money Limited operate a regimented system based upon processes, our 5-step approach is:

- Identify the money laundering risks that are relevant to our business
- Carry out periodic risk assessments on various parts of our business, focusing on
- Customer behavior, delivery channels, patterns, irregularities
- MLRO to design and put in place effective controls to manage and reduce the impact of the risks
- MLRO/Compliance to monitor the controls and improve efficiency
- Maintain records of processes/systems that were checked and why we checked them.

Our Risk Assessment Process

As a medium sized entity, we review ourselves internally and base our assessment on our chosen business models, our products and services.

When undertaking risk-based assessments of our business, we evaluate core aspects of our business, including:

- Our client bases
- Where our customers are based
- Our client overviews
- How customers have approached us
- Our products and the services we offer
- Our delivery channels and payment processes

- How our customers give us funds and where these funds come from/go to.

Risk Assessment of your Payments Business

The 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.

Risk Ranking	Grading
Low Risk	L
Medium Risk	M
High Risk	H

Below are summarized some of the operational risks that have been assessed and identified within our Company's business.

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 sets outs amendments for high risk factors:

Amendments to regulation 33 of the MLRs requires firms to include new additional high-risk factors when assessing the need for enhanced due diligence, and seek additional information and monitoring in certain cases. These may occur where:

- There are relevant transactions between parties based in high-risk third countries
- The customer is a third-country national seeking residence rights or citizenship in exchange for transfers of capital, purchase of a property, governments bonds or investment in corporate entities
- Non-face to face business relationships or transactions without certain safeguards, for example, as set out in regulation 28 (19) concerning electronic identification processes.

Country Risk - Areas of Operation

Inter City Money Limited uses the Know Your Country (https://www.knowyourcountry.com/country-ratings-table) rating tables information for measuring money laundering risks of the countries.

Know Your Country risk ranking tool is based upon data collected from many international and government agencies, tool is subjectively weighted the findings to provide a free rating tool that is predominantly focused on money laundering and sanctions issues. Please see below weightings and a list of all data subject sources that tool is based upon:

	Indicator / Sub Indicator	Weighting
1.	Money laundering/terrorist financing risks	56
	1.1. FATF Uncooperative / AML Deficient	25
	1.2. FATF Compliance with 40+9 Rec	10
	1.3. US State ML Assessment	15
	1.4. US Secretary of State terrorism	06
2.	International sanctions	15
3.	Corruption risks	10
4.	World Governance Indicators	03
5.	Narcotics Major List	03
6.	Human Trafficking	03
7.	EU Tax Blacklist	05
8.	Offshore Finance Centre	05

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.

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 licenses enable us to carry out specific activities business and to offer all related services subject to regulatory terms and conditions being met. Our business may add in the future some or all of the service listed below (unless indicated by a value then the activity is not carried out).

Product	% of total business	Risk Ranking
Retail money remittance service	94	L
High value money transfer service	5	M
Private Client	1	M

Transaction

How are they are processed	% of total business	Risk Ranking
'Face to Face'	100	L
'Non-Face to Face'	0	M

Size of Transaction	% of total business	Risk Ranking
Below £1000	80	H
£1001 to £9999	15	H
Above £10000	5	H

How are they funded?	% of total business	Risk Ranking
Non cash transactions	30	L
Cash transaction	70	M

Customers:

Retail Customers(via agents)	% of total business	Risk Ranking
in a business relationship	90	L
occasional customers	5	M
one off customers	5	M

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

Type of ID Provided	% of total Customer	Risk Ranking
EU/UK Passport/driving license (photo card) plus proof of address	80	L
Non-EU Passport plus leave to remain in UK plus proof of address	10	M
Any other form of other ID (unusual ID)	10	H

Other Characteristics

Characteristics	% of Customers	Risk ranking
Customer is a PEP	N/A	H
Customer is non-face to face (first transaction)	N/A	H
Customer is sanctions list match	N/A	H

Customer is sending more money than would be justified by given employment status	N/A	H
Customer is sending money on behalf of a group of other people	N/A	H
Customer is otherwise behaving in an unusual way which may be suspicious (see below)	N/A	H

Unusual Activity which may be suspicious

- One off cash transaction above GBP 1500 – 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

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 H).

Risk Ranking	Summary of red flags	Action of MLRO
H	Sanctions list match	Freeze transaction and report to NCA/HM Treasury

H	Customer previously reported to NCA and NCA withheld consent	Freeze transaction and report to NCA
H	Customer provides fake ID	Freeze pending transaction and
H	Customer previously reported to NCA and consent given	EDD required
H	Transaction being processed non face to face (and customer not previously identified)	EDD required
H	Single cash transaction above 5,000 Euros (or local equivalent) where no source of funds established	EDD required
H	Retail customer has sent cash transactions above 15,000 Euros (or local equivalent) within 12-month period (and no source of funds established)	EDD required
H	Customer is a PEP	EDD required
H	Customer is processing level of transactions incompatible with work status	EDD required
H	Customer is demonstrating unusual behavior (which may be suspicious)	EDD required
H	Customer is an MSB who is transacting outside anticipated parameters set at start of business relationship	EDD required
H	Customer is an MSB and ownership is not clear/MSB not able to verify ownership	EDD required
M+ or Less		No action required

CUSTOMERS WHO POSE A RISK TO US

As a money service business (MSB), we are at risk of money laundering from:

- New customers who carry out large, one-off transactions
- Customers who have been introduced to us via agents (because agents may not have carried out
- 'due diligence' thoroughly)

- Customers who are not local or usual for our business to service
- Customers involved in a business that handles large amounts of cash
- Businesses with a complicated ownership structure that could conceal underlying beneficiaries
- Customers - or a group of customers - who makes regular transactions with the same individual
- or group of individuals

CHECKING SOURCE OF FUNDS

The way customers present themselves to us and the source of their funds are key indicators of potential risk.

Through our risk-based approach we should be able to show that we have taken all reasonable steps to satisfy ourselves that the transaction is not suspicious, including, where appropriate, identifying the source of funds.

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

FATF

Our policies are formed by the FATF guidance on the Risk-Based Approach that MSB's should adhere to in order to effectively combat Money Laundering and Terrorist Financing.

The FATF guidance supports Inter City Money Limited in the development of:

- A common understanding of what the risk-based approach involves
- Outlining the high-level principles involved in applying a risk-based approach
- Promoting Inter City Money Limited in the eyes of its partners, as our risk-based approach indicates a good public and private sector practice.

The FATF identified **Pakistan** as having strategic deficiencies in its anti-money laundering and counter-terrorist financing ('AML/CFT') regime that pose a risk to the international financial system, for which it has developed an action plan with the FATF.

1. The AML/CFT framework in force in Pakistan and the manner in which that framework is applied reveal strategic deficiencies. The deficiencies include the supervision and enforcement of AML/CFT controls by financial institutions, including money service businesses; insufficient measures to prevent illicit cross-border transportation of currency; no robust track record of terrorist financing investigations and prosecutions, including the lack of necessary coordination between various authorities; insufficient implementation of targeted financial sanctions and of United Nations Security Council Resolutions 1267 (1999) and 1373 (2001); insufficient enforcement of prohibition of funds and financial services.

2. Considering the high level of integration of the international financial system, the close connection of market operators, the high volume of cross border transactions to or from the Union, as well as the degree of market opening, the Commission considers that any AML/CFT threat posed to the international financial system also represents a threat for the Union financial system.
3. In accordance with the latest relevant information, the Commission's analysis has concluded that Pakistan should be considered as a third-country jurisdiction which has strategic deficiencies in its AML/CFT regime that pose significant threats to the financial system of the Union in accordance with the criteria set out in Article 9 of Directive (EU) 2015/849. However, this country has provided a written high-level political commitment to address the identified deficiencies and has developed an action plan with the FATF, which would allow the requirements laid down in Directive (EU) 2015/849 to be met. The Commission will reassess this country's status in the light of the implementation of that commitment.
4. Delegated Regulation (EU) 2016/1675 should therefore be amended accordingly,

*Staff are advised to visit FATF site and learn up to date readings and recommendations
http://www.fatf-gafi.org/

Bribery Prevention Policies and Procedures

Policy Statement

It is the policy of this company that all members of staff shall actively avoid and prevent incidents of bribery involving the company, its staff, and any persons or organizations associated with it or acting on the company's behalf. This policy has as its objectives:

- Ensuring the company's compliance with all applicable laws and guidance, including but not exclusively the Bribery Act 2010, and requirements of the company's supervisory body Protecting the company, its principals, and all its staff as individuals from the risks associated with breaches of the law, guidance and supervisory requirements
- Preserving the good name of the company against the risk of reputational damage presented by implication in bribery and corrupt practices
- Making a positive contribution to the elimination of bribery and corrupt practices within the sphere of the company's operations.

To achieve these objectives, it is the policy of this company that:

- Every member of staff shall meet their personal obligations on bribery prevention as appropriate to their role and position in the company, and breaches of these policies and procedures may lead to action under the company's disciplinary procedures
- The company shall appoint an Officer/Bribery Prevention Officer, and they shall be afforded every assistance and cooperation by all members of staff in carrying out the duties of their appointment
- All members of staff shall refer issues involving potential bribery offenses to the

company's

- Bribery Prevention Officer, including any knowledge or substantiated suspicion of bribery
- offenses arrived at in the course of their work, whether or not the company is directly involved
- Commercial considerations shall never be permitted to take precedence over the company's anti-bribery and corruption commitment.

The Bribery Prevention Officer is Mr. Taliq Hussain

Policy and Procedure on Commissions

Policy

It is the policy of this company that the company shall not offer or pay any "commissions" to individual persons, or corporate entities under their effective control, in order to induce them to act, or reward them for having acted, improperly in their employment or official capacity by favoring the company, in breach of the Bribery Act 2010.

It is the policy of this company that no member of staff of the company, or of any organization appointed to act of the company's behalf, shall request or accept payment of any „commission", to themselves as individuals or to the company, as inducements to act, or reward for having acted, improperly in their employment in breach of the Bribery Act 2010.

Procedure

- Payments shall not be offered or paid to individual persons, or to corporate entities which are effectively controlled by them or acting on their behalf, to induce them to act or reward them for having acted improperly by favoring the company in business arrangements over which they have influence due to their employment, appointed position, or official capacity.
- Payments shall not be requested or accepted by members of staff, either personally or on behalf of the company that may be interpreted as inducements to act, or rewards for having acted, improperly in their employment by the company.
- All members of staff responsible for making or receiving legitimate payments that may reasonably fall under the heading of „commissions" shall assess the risk that such payments might represent a bribery risk, and if so, shall refer the matter to the company's Bribery Prevention Officer for prior approval.
- This policy and procedure is in addition to, and does not replace, the company's controls and approval procedures governing legitimate expenditure of this nature.
- The company's Bribery Prevention Officer shall maintain a record of all requests for approval of the payment of commissions, and whether approval was granted.

Policy and Procedure on Offering Business Gifts

Policy

It is the policy of this company that the offering of "business gifts" on behalf of the company shall not be considered routine. Where the decision is made to offer a gift, its nature and value shall be appropriate and proportionate, and it shall be offered only as a token of appreciation of past business conducted, with no implication regarding future business. For the purposes of this procedure, the term "gift" shall include charitable donations and contributions made by the company or in the company's name.

Procedure

- Business gifts shall not be offered to potential clients or any other person when it would be likely to be seen as anticipating future business. Such gifts could be interpreted as inducements for the recipient to act improperly by favoring the company in future business arrangements, thereby constituting a bribery offense.
- Where an exception to Point 1 of this procedure is thought to be appropriate, specific approval must be requested in advance from the company's Bribery Prevention Officer, irrespective of the value of the proposed gift(s).
- All business gifts to be offered on the company's behalf as a token of appreciation of past business must be approved in advance by the company's Bribery Prevention Officer.
- Approval for the offering of business gifts below the value of £150.00 may be requested on a "batch" basis when the gifts, their recipients, and the reasons for offering them, are similar in nature.
- Approval for the offering of business gifts of the value of £ 150.00 or above must be
- requested individually with details of the gift, the recipient, and the reason for offering it.
- This policy and procedure is in addition to, and does not replace, the company's controls and approval procedures governing expenditure of this nature.
- The company's Bribery Prevention Officer shall maintain a record of all requests for approval of the offer of business gifts, and whether approval was granted

Policy and Procedure on Accepting Business Gifts

Policy

It is the policy of this company that "business gifts" offered to members of staff by suppliers, clients, potential clients and other persons in connection with the company's business, shall be accepted only if appropriate and proportionate, and offered as a token of appreciation of past business conducted, with no implication regarding future business.

Procedure

- Gifts shall not be accepted from clients or any other person when it would be likely to be seen as anticipating future business. Such gifts could be interpreted as inducements for the recipient to act improperly by favoring the giver in future business arrangements, thereby constituting a bribery offense.
- Where an exception to Point 1 of this procedure is thought to be appropriate, specific approval must be requested in advance from the company's Bribery Prevention Officer, irrespective of the value of the gift(s) being offered.
- Business gifts may be accepted from clients or other persons when it is clear that

- they are tokens of appreciation of past business conducted, without any implication regarding future business, subject to the notification and approval procedures below.
- Business gifts meeting the conditions of Point 3 and of the value of £ 200.00 or less may be accepted without prior approval but must be notified to the company's Bribery Prevention Officer within five working days of receipt.
- Business gifts meeting the conditions of Point 3 but above the value of £200.00 may not be accepted without the approval of the company's Bribery Prevention Officer. Requests for approval must include details of the gift, its value, the giver, and the reason it has been given.
- When a business gift cannot be accepted under the terms of this procedure, it shall be declined diplomatically with the explanation that the company's procedures do not permit its acceptance. The reasons behind this must not be expressed, as it must not be implied that the offer had any improper motives.
- The company's Bribery Prevention Officer shall maintain a record of all notifications and requests for approval of the acceptance of business gifts.

Policy Procedure on Offering and Accepting Hospitality

Policy

It is the policy of this company that benefits of this nature shall be offered and accepted on behalf of the company only in the context of enhancing business relationships with clients, potential clients, suppliers and other parties through personal contact in a non-business environment, and where the cost of the benefit is appropriate and proportionate.

Procedure

- Benefits in this category shall be offered or accepted only where personal contact between members of the company's staff and the personnel of the other party is involved, and enhancement of the business relationship is actively promoted.
- All benefits in this category must be approved in advance by the company's Bribery Prevention Officer and by the senior management.
- Approval for the offering or acceptance of benefits in this category below the value of
- £200.00 may be requested on a „batch" basis when the benefits, the participants, and the reasons for offering or accepting them, are similar in nature.
- Approval for the offering or acceptance of benefits in this category of the value of
- £200.00 or above must be requested individually with details of the benefit, the participants, and the reason for offering or accepting it.
- This policy and procedure are in addition to, and does not replace, the company's controls and approval procedures governing expenditure of this nature.
- The company's Bribery Prevention Officer shall maintain a record of all requests for
- approval of the offer and acceptance of benefits in this category, and whether approval was granted.

Policy Procedure on Offering, Accepting Travel and Accommodation Costs

Policy

It is the policy of this company that payment for travel and accommodation costs incurred by members of the company's staff, or the personnel of suppliers, clients, potential clients and other persons in connection with the company's business, shall be offered or accepted only when the travel and accommodation in question are:

- Necessary for the effective conduct of the company's business
- Made use of by persons directly involved in the business in question
- Of an appropriate level of cost considering the normal and reasonable expectations of the persons concerned.

Procedure

- Travel and accommodation costs shall be offered or accepted only when the travel is necessary for the effective conduct of the company's business, and the facilities are made use of by persons directly involved in the business being conducted.
- Costs meeting the conditions of Point 1 and of the value of £500.00 or less may be paid or accepted without prior approval but must be notified to the company's Bribery Prevention Officer within five working days.
- Costs in this category meeting the conditions of Point 1 but above the value of
- £500.00 may not be offered or accepted without the approval of the company's Bribery Prevention Officer. Requests for approval must include details of the travel and accommodation, its cost, which is paying, and the reason it has been offered or accepted.
- When a benefit in this category cannot be accepted under the terms of this procedure, it shall be declined diplomatically with the explanation that the company's procedures do not permit its acceptance. The reasons behind this must not be expressed, as it must not be implied that the offer had any improper motives.
- This policy and procedure are in addition to, and does not replace, the company's controls and approval procedures governing expenditure of this nature.
- The company's Bribery Prevention Officer shall maintain a record of all notifications and requests for approval of the offer or acceptance of benefits in this category.

Policy Procedure on Appointing Staff and Outside Persons Organisations

Policy

It is the policy of this company that when appointing new staff, or outside persons or organizations to act on the company's behalf, the exposure to bribery risk of the role to be filled shall be taken into consideration. Where the risk is high, steps shall be taken to ensure that the person or organization being appointed is of appropriate integrity, and aware of the company's policies on bribery prevention.

Procedure

- When a new member of staff is to be recruited, or an outside person or organization appointed to act on the company's behalf, the member of staff responsible for the appointment shall assess the exposure to bribery risk of the role to be filled.
- Where the exposure to bribery risk is high, the member of staff responsible for the

appointment shall ensure that the person or organization being considered accepts the need to comply with the law and guidance and the company's bribery prevention procedures. Appropriate steps should be taken to verify CVs, references, financial statements, etc. supplied in support of the proposed appointment.

- If the person or organization being considered has previous experience in roles exposed to high bribery risk, they must make clear their understanding that actions which in these were considered a normal part of doing business may now constitute offenses under the Bribery Act.
- Where the exposure to bribery risk is high, the member of staff responsible for the appointment shall inform the company's Bribery Prevention Officer of the steps taken to ensure that the appointee has appropriate awareness and integrity.

Policy Procedure on Training and Communication

Policy

It is the policy of this company that all staff and outside persons, agents, and their staff shall be made aware of the company's bribery prevention policies and procedures, and that appropriate ongoing training and communication measures shall be instigated and maintained to ensure an appropriate understanding of these policies and procedures and the importance of following them.

Procedure

The company's Bribery Prevention Officer shall ensure that all members of staff, and all outside persons, agents, and their staff's behalf, receive information making them aware of the company's bribery prevention policies and procedures, and have access to this information for reference at all times.

The company's Bribery Prevention Officer shall ensure that all members of staff, and all outside persons, agents, and their staff's behalf, receive appropriate training on the relevance and importance of bribery prevention in their everyday work.

The company's Bribery Prevention Officer shall instigate and maintain an ongoing program of assessment to ensure that all members of staff exposed to bribery risk demonstrate their awareness of bribery issues, the company's bribery prevention policies and procedures, and their importance and relevance to their work.

The company's Bribery Prevention Officer shall keep records of the training received by staff and the results of awareness assessments to ensure that the company can demonstrate that every member of staff has received appropriate training and has an appropriate level of awareness.

Complaints Handling Policy

Our commitment to our Customers

At Inter City Money Limited each of our customers are important to us, and we believe you have the right to a fair, swift and courteous service at all times. Inter City Money Limited has

established a complaints procedure to ensure your complaint is dealt with promptly, efficiently, in positive manner and by the correct person.

As our customer, you are in a good position to judge how we are performing, and we need you to tell us if things have gone wrong. We will treat your complaint seriously and in confidence.

This leaflet sets out the complaint procedures you should follow. However, please bear in mind that as we have to work within a framework set by law. Any decisions we make have to be in line with relevant laws, we may not always be able to meet your expectations.

How to make a complaint

If you are not satisfied with the service you have received, please get in touch with the person executing the deal to which your complaint refers. They can deal with most complaints informally and quickly.

If you prefer to make a formal complaint, such complaints must be made in writing, by post, fax or e- mail and addressed to the Client Services Manager at Inter City Money Limited. The Client Services Manager will be keen to put the matter right (if they can) and to learn from any mistakes that may have been made.

Please provide as many details as you can in your complaints. All letters you receive from us give the contact details of the person who sent, and usually a reference number.

To help us investigate and resolve the problem as quickly as possible, whether you wish to resolve it informally or you are making a formal complaint, please make sure you always give us the following information:

- Full name and address;
- Your transaction reference number (if your complaint relates to a particular transaction);
- Your daytime phone number (if possible); and
- Full details of your concern or complaints, including any previous dealings with us about it;
- Copies of any relevant documents such as letters;
- Details of what would you like us to do;

We will acknowledge the receipt of your complaint in writing within 48 hours and confirm who will handle your complaint, and how you can contact them.

We shall investigate your concerns and respond to you promptly and at the latest within 15 days of receipt of the compliant. In exceptional situations, if the answer cannot be given within 15 business days for reasons beyond our control, we will send a holding reply, clearly indicating the reasons for a delay in answering to the complaint and specifying the deadline by which we will receive the final reply. In any event, the deadline for receiving the final reply shall not exceed 35 business days.

In our final response we will include:

- Summary of the complaints;
- A summary of the outcomes of your investigations;
- Whether we acknowledge there has been any fault on our part and whether the complaint will be upheld;
- Details of any offer to settle the complaint and the duration of the offer;
- If you are a retail client, a notification of your right to refer to the Financial Ombudsman Service.

If you are not satisfied with the Complaints Handling or you are dissatisfied with the final response you have received, you can write to The Financial Ombudsman Service (FOS) - Alternative dispute resolution at:

The Financial Ombudsman Service (FOS), Exchange Tower
E14 9SR
Telephone No.: 0800 023 4567 or 0300 123 9123.
Online compliant form: https://help.financial-ombudsman.org.uk/help
The FOS has been established as the official independent expert in settling complaints between consumers and businesses providing financial services. You can obtain a copy of the FOS explanatory leaflet from Inter City Money Limited or by contacting FOS directly at the above given address.

Remember, Inter City Money Limited values customer's feedback. Help us to get it right every time.

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-process able' 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:

- Processing personal data fairly, legitimately, lawfully and proportionately;
- Informing individuals regarding our processing of their personal data;
- Abiding by restrictions on the international transfer of personal data;
- 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;
- Maintaining an appropriate registration with the Commissioner's office; and
- Responding appropriately when data subjects seek to exercise their statutory rights of access, correction and objection.

INTER CITY MONEY LIMITED
COMPLIANCE DEPARTMENT
AML POLICY AND PROCEDURES VERSION 4.0

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.
Our Data Protection Officer is Mr. Taliq Hussain

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:

- 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
- 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:

- Processing is justified if it is necessary to fulfill 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.
- 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.
- 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.
- 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,

- Information only needs to be made available where it is practicable to do so;
- 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
- 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

- Our identity;
- The purposes for which we expect to process the data; and
- 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:

- Our identity;
- 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
- The following further information, which, we consider, needs to be provided to ensure that our processing of customer data is fair:
- 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);

- 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
- 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:

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.

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:

Satisfy ourselves that the service provider will have appropriate technical and organisational security measures in place;

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

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

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.

ANNEXURE –I

SUSPICIOUS ACTIVITY REPORT FORM (INTERNAL)
SAR Reference: ICM/BR/Month/Sr. No

Details	Comments
Date / Month:	
Sender Name & Address	
Sender DOB	
Customer ID	
Transaction No. & Amount	
Nature of unusual activity:	
Complete details of suspicion: **[Please provide Full fact of Activity]**	
Arrange Call/ Visit/Email to Customer after this SAR **If yes, then what are the outcomes?**	
Refer to NCA: **MLRO Decision**	
If You don't refer to NCA: **Reason for Decision: [Please provide full Details]**	
Signature by MLRO:	
Date referred to NCA:	
Please Email document at Compliance@intercitymoney.com	