RISK ASSESSMENT

Last Updated by : December 2020

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

Contents

Document Objectives

The objective of this document is to outline Inter City Money Limited's ("INTER CITY") risks and vulnerabilities to money laundering and terrorist financing and the arrangements it has put in place to mitigate and manage those risks.

The key purpose of this risk assessment is to refine and improve the management of Inter City's financial crime risks through identifying the money laundering, terrorist financing, fraud and sanctions inherent risks and determining how these risks are mitigated by the controls currently in place and what, if any, enhancements are required to be made to the current systems and controls framework.

Inter City has identified the inherent risks posed by its own customers, business relationships, jurisdictions, delivery channels, services, governance arrangements and systems and controls and, the effectiveness of the controls in place to mitigate those risks.

This risk assessment covers operations in the period January 2020 to December 2020. This period is known as the 'assessment period'. The results included in this report are accurate for the information gathered during the assessment period.

This risk assessment provides the basis for the customer due diligence procedures, both at the start of a relationship and ongoing, and the nature and extent of the ongoing monitoring of the relationship.

Review and Updating

This documented risk-based strategy and business risk assessment is kept under review by the MLRO, in consultation with Inter City executive management. The MLRO conducts a risk assessment on an annual basis and more frequently, where a trigger event occur, such as a significant change in regulation or business strategy (e.g. changes to the business's products/services, means of delivery and its customer base) or during the intervening period.

Regulatory Environment

Inter City is complying with the Money Laundering Regulations 2017 ("MLR") and 2019 regulations (amendments) by:

- Taking appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject i.e. a risk assessment;
- Establishing and maintaining appropriate and proportionate policies, controls and procedures to mitigate and manage such risks;
- Conducting due diligence on new business relationships and/or an occasional transaction;
- Completing ongoing monitoring of business relationships, which includes scrutinising transactions and keeping customer information and due diligence up to date;
- Performing enhanced due diligence and ongoing monitoring, when a higher risk

relationship presents itself.

- Keeping records pertaining to customer due diligence and transactions; and

- Ensuring that all relevant staff are aware of their legal requirements and how to recognise and deal with transactions, which are considered suspicious. i.e. training and competence.

• The requirement for a Risk-Based Strategy

- The **Money Laundering Regulations 2017 - Regulation 18*** requires all UK businesses and other regulated firms to assess their money laundering/terrorist financing risks and determine how they will be managed.

The FCA also requires that in accordance with senior management responsibilities and corporate governance requirements, all regulated financial services firms (including INTER CITY'S) must conduct and document in writing an AML/CTF risk assessment.

* Money Laundering Regulations 2017 – Regulation 18 provides:-

(1) A relevant person must take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject.

(2) In carrying out the risk assessment required under paragraph (1), a relevant person must take into account

a) information made available to them by the supervisory authority under regulations 17(9) and 47, and

b) Risk factors including factors relating to-

i. Its customers;
ii. The countries or geographic areas in which it operates;
iii. Its products or services;
iv. Its transactions; and
v. Its delivery channels.

(3) In deciding what steps are appropriate under paragraph (1), the relevant person must take into account the size and nature of its business.

(4) A relevant person must keep an up-to-date record in writing of all the steps it has taken under paragraph (1), unless its supervisory authority notifies it in writing that such a record is not required

(5) A supervisory authority may not give the notification referred to in paragraph (4) unless it considers that the risks of money laundering and terrorist financing applicable to the sector in which the relevant person operates are clear and understood.

(6) A relevant person must provide the risk assessment it has prepared under paragraph (1), the information on which that risk assessment was based and any record required to be kept under paragraph (4), to its supervisory authority on request.

As part of carrying out the risk assessment, consideration is given to the following risk factors in relation to Inter City's:

- Customers;
- The countries or geographic areas in which we operates;

- Services;
- Sector/ industry; and
- Delivery channels.

Inter City's risk-based strategy and assessment is documented, as part of its anti-money laundering policies and systems and controls.

Inter City's Risk-Based Strategy

Inter City's risk-based strategy includes

- Assessing Inter City's vulnerabilities to money laundering and terrorist financing;
- Assessing the risk that is posed by the services, including its characteristics, the way they are delivered and how they are used;
- Assessing what risk is posed by the customers, including the means by which the customer is acquired, who the business's customers are, where they are located, their organisational structure, where applicable and what they do;
- Designing and implementing controls and procedures to manage and mitigate the money laundering and terrorist financing risks that have been determined, paying particular attention to the factors that have been assessed as presenting higher levels of risk;
- Applying increased levels of customer due diligence and monitoring to reflect increasing levels of risk;
- Monitoring a customer's instructions, transactions and activity in their accounts against known and expected behaviour and characteristics;
- Monitoring transactions against HMT Consolidated Financial Sanctions List, OFAC and EU Sanctions lists;
- Recording the results of the risk assessment and the controls that have been put in place;
- Regularly monitoring and reviewing the business's risks and keeping this information relevant and up to date.

Inter City's Background

Inter City's is authorised and regulated by the Financial Conduct Authority – FRN 514406. Inter City's principal permission is:

- Money Remittance

INTER CITY'S has offices in the following locations:

- Keighley-West Yorkshire

The offices operate as administrative offices, to support the agent network.

The AML/CTF status of the UK

Supervision in the UK

The HM Treasury is responsible for appointing supervisors and for the Money Laundering Regulations 2017 ("the Regulations") which set out the role of the supervisors and gives them powers to effectively monitor their respective sectors. In order to improve the transparency and accountability of supervision and to encourage good practice, the HM Treasury has worked with supervisors to produce an annual report, which covers supervisory activities in the assessment year.

HM Treasury has 28 appointed AML/CTF supervisors which oversee eight broad sectors and a diverse range of firms, which include financial institutions, credit institutions, law firms, accountancy firms, estate agents and casinos. Some have been supervisors for AML/CTF purposes since the Regulations were first implemented in 1993; others were introduced when the Regulations were updated in 2007.

The supervisors are a highly diverse group, including large global professional bodies, smaller professional and representative bodies, and a number of public sector organisations. In each area of supervision, the supervisor's approach needs to be proportionate to the nature and associated risks of the firm being supervised.

All supervisors are expected to attend the AML Supervisors Forum which meets on a quarterly basis. Supervisors meet on a regular basis in smaller affinity groups, based on the industry sector they supervise to encourage the exchange of sector relevant material.

AML/CFT supervisors

The AML/CTF supervisor's relevant to Inter City's operations are:

- Financial Conduct Authority (FCA)
- HM Revenue & Customs (HMRC)

Sanctions risk assessment results

Summary of inherent risk ratings

AML/ CTF Risk	Customer Risk	Geography Risk	Services Risk	Delivery/ Distribution Channel Risk	Transaction Risk	Overall Inherent Risk	Mitigation Measures	Residual Risk
Inherent Risk Rating	MEDIUM	HIGH	HIGH	HIGH	MEDIUM	HIGH	▪ EDD Measures ▪ Ongoing Monitoring ▪ Internal Control Mechanism	MEDIUM

Inter City's has considered each of the inherent risks posed and further detailed analysis is provided below. The overall assessment of inherent risk based on the analysis, is considered **HIGH**.

Customer Type Risk

The broad objective of the requirement to assess customer risk is to ensure that the Inter City's knows who its customers are, what they do and whether or not they are likely to be engaged in criminal activity. The profile of a customer's behaviour will build up over time, and this will permit relevant employees to identify transactions or activity that may be suspicious.

INTER CITY'S Customers

Inter City's identifies the business partners that it serves and assess whether these are known to be frequently used by money launderers or for terrorist financing.

Inter City segment its business partners by industry, size or type (e.g., agent or aggregator). Inter City can then assess the risk of money laundering associated with each of these types.
When assessing the risk, Inter City considers whether there are any characteristics that are known to be used by money launders.

When Inter City has assessed the level of risk associated with each customer type, it will identify any mitigating actions that need be taken to address that risk.

The main type of customers that Inter City serves are retail customers from the non-resident Pakistani (NRP) community in the UK.

Inter City only services the Pakistani communities.

Inter City customers have been classified as falling within a range of risks - high, medium and low for money laundering/terrorist financing purposes.

CUSTOMER PROFILE

	PERCENTAGE OF CUSTOMERS
In a business relationship	80%
Regular customers doing one-off transactions	15%
Passing trade	05%
HOW ARE CUSTOMERS INTRODUCED TO THE BUSINESS?	
Through recommendation/word of mouth	90%
Through advertising	0%
Off the street passing trade	10%
Other sources	0%
Are there any non-face-to-face customers?	0%
Are there any potential Politically Exposed Persons?	No
General description of usual types of customer and Purpose of	All individuals send money to families in
Any significant customers outside normal Customers profile?	No
What is percentage of cash transactions?	70%

The customer type risk has been assessed as **'Medium'**. The primary reasons for the assessment outcome are:

- Accounts of 79 agents comprising of sole traders, partnerships and limited companies which are classed as either high, medium or low risk.
- 99% of all customer accounts are agents which are classified as medium risk.

Agents – Inter City conducts compulsory CDD, after which the agent may be reclassified as either, medium or low risk, based on the prevailing risk assessment which is prepared after the consideration of various factors:

- Number of transactions
- Amount of transactions
- ATS
- Number of Customers (Attempted Vs Cancelled)
- Threshold Values
- Customer Risk
- Payout Channel Risk
- Inherent risk

Retail Customers - most of Inter City's retail customers are from the non-resident Pakistani (NRB) community in the UK and other countries and over the assessment period, approximately 98% were rated as low-risk transactions (transaction value less than £8500) and were therefore subject to CDD and approximately 2% of customer transactions were rated high risk (transaction value over £5000) and were therefore subject to EDD.

Customer due diligence processes serve as one of Inter City's most important controls on the types of customer it will accept. For Inter City's, its CDD processes also serve to determine the level of risk attributed to each transaction, and subsequently, the level of CDD conducted on the customer.

Jurisdiction Risk

Inter City's agent network is only geared to do remittance in Pakistan.

Inter City's has assessed the risk of money laundering associated with Pakistan. When assessing geographic risk, Inter City considered factors such as whether there is a perception of corruption in that country, whether there is known to be criminal activity, or if the country is on the sanctions list.

Inter City's needs to consider the following sources of information to determine those countries or geographies, where money laundering or terrorist financing risk is high.

- Financial sanctions listings
- Countries identified by Financial Action Task Force as being high-risk jurisdictions
- European Union's High Risk Third Country List, as amended in March 2019
- HM Treasury's National Risk Assessment 2017
- FCA AML Annual Report 2017/2018

The retail customer jurisdiction risk has been assessed as follows:

Outgoing transactions

The outgoing country is Pakistan which is considered as HIGH RISK and the majority of activity is initiated from the UK, which is considered low risk.

Incoming Destinations

The incoming destinations are detailed below. The majority of transactions are sent to Pakistan, which is considered high risk.

The overall jurisdiction type risk has been assessed as **'High'** the primary reasons for the assessment outcome are:

- All the 79 agents' accounts (100%) have residence or are incorporated in the UK and EU (Low risk).
- All outgoing transactions are initiated within the UK, which is considered low risk.
- The transactions (100%) are received into Pakistan, which is considered high risk.

High Risk Countries

PAKISTAN is high risk country.

In order to cater risk we have enhanced policies and procedures in place for on boarding new agents and monitoring each transactions.

For On boarding agents following checks are mandatory:

- Adverse Media check
- PEP / Sanction check
  Independent Electronic check over individual and Limited companies (Credit Safe)

For Transaction screening:

- Sender basic information with identification document
- Adverse Media check
- PEP / Sanction check over sender and receiver
- Independent Electronic check (Credit Safe)
- Beneficiary Link Report to examine sender/Receiver's Transactions behaviour.
- Customer not in same town as agent

All the pay-out arrangements made through Pakistani banking channel.

Compliance Daily Report			
CONTEXT TYPE	PARAMETERS	OBSERVATIONS	RECOMMENDATIONS
Business	Total Number of Transactions Total Volume of Transactions Average Transaction Size (ATS)	Examining business and ATS of transactions to evaluate high risk business including slab of payments to ensure business is genuine.	If any
Sender's Report	Number of senders sending more than 1 transactions Sender who made highest Transaction for different beneficiaries	to trigger link transactions.	If any
Beneficiary's Report	Number of receivers who received more than 2 Transactions	to trigger link transactions.	If any
Duplicate Customer	Duplicate customers who made transactions with different Agents	by applying duplicate checks we identify agent/customer behaviour if someone deliberately try to create multiple account of same customer.	If any
Special Cases	Senders who made more than 3 transactions for more than 3 different beneficiaries	All the unusual transactions	If any
Large Amount Tranx	Senders who made transactions more than 5000 & Number of Corporate Transactions	The basic purpose of this report to rechecking of documents.	If any
Data Integrity	Review profiles of senders	Compliance officer validate the information as per enclosed documents.	If any

Services Risk

Inter City's primary and sole services is money remittances only which is at high risk and could be used by criminals to launder money or finance terrorism.

Services Type	Number of Accounts	% of total Accounts	Risk Rating
Money Remittance	**79**	**100%**	**High**

The services risk have been assessed as **`High'**. The primary reason for this assessment outcome is that, a significant proportion (100%) of the Inter City's services which is money remittance only, is classified as high risk.

Delivery / Distribution Channel Risk

UK and international standards accept that there is a greater potential for money laundering or terrorist financing when the customer or the customer's representative does not transact on a face-to-face basis. All business undertook non-face to face, including non-face to face remittance business, has been classified as presenting a higher level of risk.

Inter City identifies all the methods of interaction it has with its agents, and customers. Some delivery channels can increase the risk because it can make it more difficult to determine the identity of a customer.

The risk factors we take into account are:

- Whether Inter City meets its agents or customers face-to-face;
- Whether Inter City's agents or customers were introduced through an intermediary and whether they only correspond with that intermediary;
- the extent to which Inter City relies on the CDD of the referrer or intermediary (and the procedures Inter City's employ to justify reliance) or the quality of evidence obtained from them to support Inter City's own CDD.

The delivery channel has been assessed as **Medium** because 95% of Inter City's customers including its agents are face-to-face customers.

- All 79 agent accounts are considered face-to-face and Inter City's team make regular visits to these types of customers. They, therefore, present a lower risk of money laundering or terrorist financing.
- All retail customers (99%) are considered face-to-face and present a low risk of money laundering or terrorist financing.

Distribution Channel- Retail Channel

1. Network of Agents – Face-to-Face

Transaction Type	% of transactions	Risk Rating
Bank	**5%**	**Low**
Cash	**95%**	**High**

The overall payment method type risk has been assessed as **High** because **95%** of transactions are conducted in cash.

Summary of Residual Risks

Governance and Culture

Governance and culture are the foundation of a Financial Crime control environment. It includes

- A robust governance structure with senior management responsibility;
- Internal Control mechanism and policies and procedures; and
- Adequate resources to mitigate the AML and sanctions risk.

The Financial Crime governance and culture controls in place at Inter City's have been assessed as **"Effective"**.

The primary reasons for the assessment outcome are:

The 2020 annual review of the Compliance Policy & procedures has been completed to ensure implementation of Inter City's AML/CTF mitigation measures and that supporting guidance allows staff to consistently follow AML/CTF procedures, or where applicable, how exceptions to procedural standards are reported, tracked and resolved.

It is accepted that culture within Inter City can be improved on an on-going basis, supported by clearly articulated desired behaviours.

Governance Structure

Inter City operates a two lines of defence model and the Compliance function, acting as the second line of defence, is independent of the business.

Inter City has regular monthly compliance meetings set up to discuss transactions and relationships where escalated to the MLRO and discuss practical issues in relation to Inter City's higher risk customers, including PEPs and money remittance business.

The Inter City management has the ultimate responsibility of ensuring that Inter City's complies with its regulatory environment.

The Policies and Procedures

Inter City's Policy and Procedures are contained within the "Compliance Policies and Procedures" (herein referred to as the "P&Ps"). The P&Ps provides a high-level review of the legislation and regulation that is applicable to Inter City and the controls in place to prevent financial crime.

The latest version of the P&Ps (2020) were updated by the MLRO. We are using LEXIS NEXIS platform to screen PEP's.

The P&Ps includes updated changes resulting from the 5th EU Money Laundering Directive and the Money Laundering Regulations 2019 (Amendments). In addition, the P&Ps have been updated to reflect the FCA's Guidance on PEP procedures [FG17/ 6: The treatment of politically exposed persons for anti-money laundering purposes, July 2017]. The P&Ps and its associated appendices are accessible to all employees.

This is to ensure that the P&Ps, provide sufficient coverage on enhanced requirements and that enhanced supporting guidance allows staff to consistently follow AML/CTF procedures, or where applicable, how exceptions to standards are reported, tracked and resolved.

Resources

Financial Crime activities within the Compliance function are currently resourced by an MLRO, a Compliance Manager and a team comprising of two Compliance Officers. There are currently 04 staff out of a total of 06 members engaged in the mitigation of AML/CTF.

The primary second-line activities performed by Compliance includes dispositioning suspicious activity transaction monitoring alerts, reviewing potential PEP matches from screening, sample reviews of AML, periodic risk reviews and reviews of new account opening checks undertaken by the first line.

Customer due diligence

Customer due diligence (CDD) is central to an effective AML program that proactively identifies individuals and further business relationships who carry a heightened risk of money laundering, thus allowing Inter City's to apply subsequent risk- based controls to mitigate the risk.

CDD is also essential for effective screening processes to be undertaken. For example, incomplete and/or inaccurate data may result in a sanctioned entity not being identified by Inter City's throughout the lifecycle of the customer relationship.

Inter City's due diligence process for its business relationships requires sufficient information to be collected, recorded and retained to ensure that Inter City's know with whom it is doing business and is satisfied that any monies the business is handling has not been illegally acquired or the activity being undertaken is not with a view to committing money laundering or for financing terrorism and there is sufficient understanding about the customer's economic background, the nature and purpose of the customer's expected activity and the expected, or predictable, pattern of transactions.

In addition, Inter City's staff and agents are required to understand the rationale behind a request to open an account with Inter City, for example where the client does not have any visible local connection with the local area of Inter City's offices.

Finally, checks are required to be made with all new customer details against the prescribed sanctions, PEPS and, where applicable, adverse media lists, before any transactions are conducted and against these lists regularly thereafter.

Given the various CDD controls in place, Inter City have been assessed as **EFFECTIVE** as at December 2020. The primary reasons for the assessment outcome are:

- Continual improvements have been made to Inter City's AML Due Diligence processes. Whilst existing CDD practices are considered good, but any new processes require embedding as part of the customer on-boarding and periodic review process.
- The rationale and methodology behind the assessment of customer risk, including the sources used to determine High/ Medium/ Low risks has been documented.
- Inter City's has enhanced the quality of its CDD/EDD information obtained for high risk clients and once we found that customer is PEP, we do not establish business relationship with them and therefore we do not have any PEP as our customer.
- A client file review is constantly in progress and 2nd line Compliance perform all KYC refresh duties.
- Procedures have been developed outlining circumstances where Inter City's must reapply CDD measures on a risk sensitive basis following trigger events.
- Specific EDD procedures in relation to higher risk situations have been enhanced to ensure that red flag scenarios and other checks required to mitigate risks are fully embedded within the existing due diligence processes.

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.

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.

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.

Customer screening

Inter City have risk-based procedures in place to ensure that it is able to determine whether a customer is a specifically designated national (SDN) or appears on any sanctions list or is a PEP.

The customer screening controls in place at Inter City have been assessed as **EFFECTIVE**. The

primary reasons for the assessment outcome are:

- Embedded controls for sanction screening, PEP screening, and adverse media screening at on boarding, real time and periodic risk review stages.

- Management Information (MI) on declined customers is incorporated into the Compliance monthly report and also highlighted at the periodic compliance committee meetings.

Customer Screening Tools

Inter City conducts screening at customer on-boarding and on an on-going daily basis on all customers, beneficial owners, controllers and other significant associated parties including remittance transactions. The system's screen against Sanctions and PEP lists, which include those deemed relevant for meeting its UK legal requirements i.e. OFAC, EU and HM Treasury lists.

Real time Sanctions checking is performed automatically using the remit ERP system, for all transactions that go in and out of the business system on both the sender and beneficiary.

Adverse media screening is conducted on all business relationships, prior to on boarding by credit safe platform searches and through open source internet searches in line with Inter City's on-boarding process, as well as during periodic risk reviews.

Alert investigation

If there is a potential hit against any one of the sanctions lists, the system blocks the transaction and it is directed to the Security Queue List for review. The Compliance team reviews and discounts the alerted items on a daily basis, seeking further information from the customer and referring to Compliance/ the MLRO.

Screening results

Where any true sanctions matches or "hits" are identified these are escalated to Compliance and "blocked". The potential matches are reviewed and cleared by Compliance.

Where matches are identified with respect to PEPs or adverse media through LEXIS NEXIS platform and internet screening, these are assessed by the Compliance Department and the case will be referred to the MLRO to consider whether the account should be suspended or closed as we do not onboard PEP or adverse media matched clients.

Transaction Monitoring

Transaction monitoring

Inter City conducts ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile.

Monitoring customer activity helps identify unusual activity, which it cannot be rationally explained, may involve money laundering or terrorist financing.

Suspicious transaction monitoring controls in place at Inter City have been assessed as **Effective.**

The primary reasons for the assessment outcome are:

- Increased transaction monitoring is in place, in accordance with pre-defined rules to detect suspicious activity, with respect to both AML and CTF.
- Improved transaction monitoring rules for Inter City's remittance business and correspondent business, which have been incorporated into the Business's existing Transaction Monitoring system.
- Compliance watch list for the monitoring of selected higher risk customers and transactions is in place.

Suspicious Activity Reporting (SARs)

Suspicious Activity Reporting controls in place at Inter City have been assessed as **Strong**.

Inter City's has a documented process in place for the identification and reporting of potential suspicious activity to:

- Report to the MLRO, or in their absence, the Manager Compliance;
- Not discuss the suspicion with anyone without consent from the MLRO; and

- Not to execute the transaction until the MLRO adjudicates.

A Money Laundering Suspicion Report for staff or agents to document and report their reason for suspicion is available as an Appendix item of the AML/CTF Policy). Staff or agents who have a suspicion are encouraged to speak with and report to the MLRO.

A SARs log is maintained by the Compliance Department and access is restricted to the MLRO and Manager Compliance.

Training and Education

Training is a vital part of ensuring that all Inter City's staff understand the regulatory and legislative requirements, as per Regulation 24 of the Money Laundering Regulations 2017.

All "relevant persons" have a responsibility to escalate any suspicious behaviour to the Compliance function. Therefore, it is imperative that all staff and agents complete AML and sanctions training when they join Inter City, as well as refresher training annually and on a risk-based approach.

Induction training is given to all staff and typically delivered by the MLRO.

The AML and sanctions training and education controls in place at Inter City have been assessed as **Satisfactory.**

One of the Inter City's 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 are made aware of our anti-money laundering policy, manual and the obligations arising from them for both themselves and Inter City Money Ltd.

The 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, ML and CTF.
b) Refresher training- all relevant staff 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's Compliance will ensure minimum training standards/ requirements for AML/CTF Compliance staff, e.g. industry sponsored training courses will be provided.

Enhanced Due Diligence

Enhanced due diligence applies in situations that are high risk. It means taking additional measures to identify and verify the customer identity and source of funds and doing additional ongoing monitoring.

Agents/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.

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

Risk indicators

The following is an example list of common risk indicators that call for enhanced due diligence. It's not an exhaustive list, and neither are these signs always suspicious. It depends on the circumstances of each case.

Money transmitters

The following are examples of common risks for money transmitters:

- Criminals use money transmitters to disguise the origins of criminal funds and move money between different jurisdictions. Criminals try to identify weaknesses in money transmitters' anti-money laundering controls and exploit them.

- A further risk associated with money transmission is that some jurisdictions have weak anti-money laundering systems. Some jurisdictions are high risk because they are especially vulnerable to criminal activity such as drug smuggling, people trafficking and terrorism.

New customers

The following are examples of common risk indicators for 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
- There is no apparent reason for using our business's services, for example, another business is better placed to handle the size of transaction or the destination of the transmission
- The customer is unable to provide satisfactory evidence of the source of the funds
- Unusual source of funds
- The transmission is to a high-risk country
- Non face-to-face customers
- The customer owns or operates a cash-based business
- There is an unusually large cash transaction
- The size and frequency of the transaction is different from the customer's normal pattern
- The pattern has changed since the business relationship was established
- The transaction seems to be unnecessarily complicated, or seems to use front men or companies
- The customer sends or receives money to or from himself
- The customer is acting on behalf of third parties without there being an appropriate family or business relationship between them
- Other people watch over the customer or stay just outside
- The customer reads from a note or mobile phone

- An under-age person sends or receives funds from multiple sources
- There has been a significant or unexpected improvement in the customer's financial position
- The customer (or two or more customers) is using more than one local Money service business, perhaps to break one transaction into smaller transactions

Transactions

The following are examples of common risk indicators where transactions:

- Are just below the threshold for Enhanced due diligence checks
- Appear to have no obvious economic or financial basis benefit
- Route through third countries or third parties
- Regularly go to or from tax haven countries
- Information accompanying the payment appears false or contradictory
- Are destined for money service businesses around the borders of countries at high risk of terrorism.

Additional Measures to Take:

In case of HIGH RISK EDD is mandatory and Agents/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)
- Obtain additional information on the customer and the customer's beneficial owner
- 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 Assessment

Customer Risk Assessment (CRA)

A customer risk assessment matrix has been implemented to assess customer risk and determine the level of due diligence required.

A risk rating is calculated for a customer based on a range of factors including customer type, jurisdiction, industry, services and delivery channel, as well as a number of factors relating to transactional activity.

Inter City has since made changes to the Customer Risk Assessment, including sources used to determine High/Medium/Low for certain risk factors and how the overall scoring is determined.

The specific requirements have been reviewed as part of the update to the P&P's in December 2020.

Enterprise-Wide Risk Assessment

The Money Laundering Regulations 2017 - Regulation 18 requires all UK businesses and other regulated firms to assess their money laundering/terrorist financing risks and determine how they will be managed.

The FCA also requires that in accordance with senior management responsibilities and corporate governance requirements, all regulated financial services firms (including Inter City's) must conduct and document in writing an AML/CTF risk assessment.

The purpose of a comprehensive risk assessment is to assess the enterprise-wide money laundering and terrorist financing risk profile of Inter City's and all subsidiaries. By determining the enterprise wide AML/CTF risk profile, Inter City's evaluate the adequacy of existing processes and where required, modify and update the risk management processes, in an effort to more effectively identify and mitigate risk.

An enterprise wide risk assessment has been conducted in December 2020.

Risk Assessment

Inter City is a medium sized entity and we review ourselves internally and base our assessment on our chosen business models, our customers and services.

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

- Our client base
- Where our customers are based
- Our client overviews
- How customers have approached us
- Our delivery channels and payment processes
- How our customers give us funds and where these funds come/go to INTER

  CITY'S have been determined risk assessments as **Effective.**

Agent Risk Assessment Parameters (ARAP)

In Risk Assessment we have taken several parameters to check and assess the risk level of each agent.

Agent are evaluated on the bases of following parameters:

1. No of Transactions (All transactions are compared with the Average no of transaction of each Agent)
2. Total Volume (Volume compared with average volume)
3. Average Transaction Size (less than 500 is low, Less than 700 is medium and more is high)
4. Total Number of Customers Consumed (Compared with average)
5. Cancelled Payments (less than 10 % is low, less than 20% is medium and above is high)
6. Amount Slabs (Each slab is compared with average)
7. BASEL AML Index (Divided the BASEL AML index with 3 to assign a risk ratting)
8. Pay-out Chanel (Branch = Low, though banks= Medium, and exchange companies = High)
9. Customer Risk level (Customer Risk is assessed on following Parameters of customer only)
    a) Customer's transaction (Compared with Average)
    b) Total Amount remitted (Compared with Average)
    c) Average Transaction Size (Same as for agents)
    d) Cancelled Payments (On percentage bases)
    e) Total Number of receivers consumed (Compared the ratio between total transaction and total receivers and assigned the ratting on the bases of percentage of receivers)

After thoroughly assessing all the above mentioned parameters an overall risk rating is assigned to the agent and based on that rating each and every agent is assigned a risk level, it is "Low", "Medium" or "High".

The primary reasons for the assessment outcome are:

- The rationale and methodology behind the assessment of customer risk, including the sources used to determine High/ Medium/ Low risks have been documented.
- A comprehensive enterprise-wide risk assessment has been completed to assess the money laundering and terrorist financing risk profile of Inter City's and all its subsidiaries.
- Inter City's acknowledges that the risk assessment process is effective, but requires some time, (at least 1 full year of execution), before it can be considered to be fully embedded.

Overall AML/CTF Risk Assessment

Given the control framework in place, Inter City's has assessed its residual risk of facilitating money laundering and CTF as **MEDIUM.**

This is based on the overall inherent risk posed by its customer type, jurisdiction, transaction type, products and services and delivery channel risks having been assessed as **HIGH** and the effectiveness of its control framework having been assessed as averaging '**EFFECTIVE**'.

Risk appetite statement

The principle risks and uncertainties facing the company are compliance and operational risk, financial risk and strategic risk. The risk identification and mitigation activities are built into the day-to-day operations of Inter City.

It is the responsibility of the Inter City's management Board to adopt and oversee the implementation of risk management and risk appetite throughout Inter City's and its affiliates globally.

In summary Inter City's is exposed to the following types of risk.

- Operational & Compliance risks (i.e., risks associated with people, processes and systems)
- Financial risks (e.g., Credit, Liquidity & Capital)
- Strategic risks (e.g., reputation risks)

Each risk category is further broken down into specific risk types.

Operational and Compliance Risks

Internal Fraud - Loss due to acts intended to defraud, misappropriate property or circumvent regulations, the law or company policy (excluding discrimination events) which involve at least one internal party. Inter City strives to minimise the likelihood of fraud manifesting in the business and allocate human and technology resources to minimise its impact on its business activities and its client's. Inter City has no appetite for internal fraud and has adopted a continuous improvement approach to the policies and procedures designed to deter and detect internal fraud. Non-compliance results in disciplinary action, which may include dismissal and qualified withdrawals for approved persons.

External Fraud - Loss due to acts intended to defraud, misappropriate property or circumvent the law, which involve a third party. Inter City has adopted a continuous improvement approach to the policies and procedures designed to deter and detect external fraud. The firm accepts that external fraud may happen from time to time. Nonetheless, Inter City has no appetite for external fraud.

Regulatory Risk – regulatory risks refer to the fact that a change in laws or regulations may materially impact the business or market. Inter City complies with all relevant legislation and regulations in all the jurisdictions it operates in and Inter City Compliance monitors the regulatory framework and actions any adjustments to its operations in order to achieve compliance. The company also employs external compliance audits to ensure best practice.

Employment Practices and Workplace Safety - Losses arising from acts inconsistent with health or safety laws or agreements, from payments of personal injury claims, discrimination or harassment events. Inter City will take all reasonable steps to ensure its employees are treated with dignity and respect and will have adequate business processes in place to ensure that employees are provided with a safe and comfortable environment to work in. Inter City will ensure that its vendors and suppliers can evidence that they have taken all reasonable steps to combat modern slavery. Inter City will ensure there are adequate HR policies and procedures in place and fostering positive working relationships with employees that are consistent with the core values, and monitor team performance against recommended areas of improvement.

Damage to Physical Assets - Losses arising from loss of damage to physical assets from natural disaster or other events.

Business Disruption - Losses arising from disruption of business or system failures. The Inter City's operations team remain pro-active at all times to ensure that Inter City can deal with any unforeseen situations that could hamper the running of day to day operations.

Clients, Products and Business Practice - Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.

Execution, Delivery and Process Management - Losses from failed transaction processing or process management, from relations with trading counterparties, clients, vendors and/or critical outsourcers.

Data Security – Inter City will take proportionate measures to protect employee, client and other third- party data, intellectual property and put in place good business practices with respect to data protection and retention standards.

IT Security – Inter City employs robust IT security practices in the application development lifecycle, monitors and protects its perimeters and takes measures to deter and detect insider threats.

Financial Risks

Currency Risk – Inter City's operates United Kingdom only dealing in multiple currencies such as GBP and USD. Inter City will therefore be exposed to movements in exchange rates.

Inter City mitigates the risk by having a dedicated team of foreign exchange specialists and tracking conversion rates of the trading currencies. The pay-out currencies are mainly linked to USD and the company obtains confirmed rates for most of the trading currencies from different providers.

This allows Inter City opportunity to, not only minimise the foreign exchange loss, but also to make foreign exchange gains from the favourable shifts in the exchange rates. Economic data is collected from external sources at real time and their impact is closely monitored.

Market Risk - Losses arising as a result of adverse changes in market prices. Inter City is an Authorised Payments Institution (API) and does not take outright market risk. Where market risks are inherent to the business activities (e.g. structural market risks such as those arising with respect to capital, liquidity and shareholder value) Inter City's has implemented policies and procedures to manage market risk.

Credit Risk - Losses arising as a result of one or more clients and/or trading counterparties failing to meet their financial obligations as they become due. Credit and counterparty risks are inherent in the business model through exposure to counterparty aged transactions and pre-settlement risks. The main credit risk faced by Inter City's relates to agents failing to remit monies collected on behalf of customers. The risk is managed by setting agent credit limits and performing a daily reconciliation of outstanding amounts.

Liquidity and Capital Risks - Losses arising as a result of the firm failing to meet its financial obligations as they become due. Inter City will maintain sufficient liquidity and capital to fulfil business and regulatory requirements to enable meeting financial obligations as they become due, and have access to sources of funding that will allow it to enact a contingency funding plan.

Strategic Risks

Business Risk - Losses that arise from the decisions that the Inter City's Board takes about the services that the organisation supplies, or the geographies that the organisation operates in. They include risks associated with developing and marketing those services, economic risks affecting sales and costs, and risks arising from changes in the regulatory, legal and/or technology environments which have an impact on those services or the way in which they are delivered. Inter City seeks to expand and diversify its business activities globally whilst taking account current and projected market conditions, and differences in culture and business practices in its chosen geographies. Inter City balances its investment decisions between revenue generation and control, investing in innovative technology solutions to remain cost-effective, and monitors changes to client preferences to remain competitive.

Reputation Risk - Losses that arise as a result of damage to the brand, howsoever caused. Inter City actively promotes its brand in the market place, take pro-active steps to generate feedback from clients and employees and adheres to its core values and fulfil its corporate responsibilities by ensuring it acts responsibly, ethically and with integrity.

Annex A - Rating Definitions

Inherent Risk Rating	Definition
LOW (1-2)	there is a low exposure to money laundering, terrorist financing and sanctions risk in the absence of any control environment being applied.
MEDIUM (3-4)	there is a moderate exposure to money laundering, terrorist financing and sanctions risk in the absence of any control environment being applied.
HIGH (5-10)	there is a high exposure to money laundering, terrorist financing and sanctions risk in the absence of any control environment being applied.

Ref	Dependency	Risk Description	Absolute Risk L	Absolute Risk I	Absolute Risk L + I	Treated	Residual Risk L	Residual Risk I	Residual Risk L + I			Risk L	Risk I	Risk L + I
1	Financial Crime (CTF, AML, Fraud, AB&C)	Payment Services Firms are required to have Financial Crime Prevention Controls to manage and mitigate risk of Anti-Bribery and Corruption, Money Laundering, CTF and Fraud in line with HMRC Guidance for Payment Services Firms.	**4**	**4**	**8**	Full control Financial Crime Environment in place; a separate assessment and procedures are available to support this risk item	**3**	**3**	**6**	SYSC implementation has been in place for a number of years; new HMRC Guidance on ML Reg 2019 (amendments) continues to be subjected to the Compliance Monitoring Program and Testing	MLRO	on going	**2**	**2**	**4**

2	Internal Fraud	The risk of personnel going rogue is key to organising a control environment which includes management's attitude as to the importance of the establishment and maintenance of a strong internal control system; having organizational units clearly defined to perform the necessary functions of the business; management oversight, risk assessment and fraud data controls and monitoring this risk being mitigated, as will tailored controls on the ground.	**3**	**3**	**6**	Properly trained personnel; delegation of authority or limitation of authority to provide assurances that responsibilities are effectively performed; having policies and procedures including a code of ethical conduct available to employees; and requiring background checks on personnel that have access to personal information, positions of accounting and financial oversight, and positions of trust	**3**	**2**	**5**	Compliance Monitoring Program was expanded to include operational arrangements that may have an impact on internal fraud prevention; testing and monitoring	MLRO /MD	In place and being expanded as additional control to on going monitoring	**1**	**1**	**2**
3	FX Risk	(Also known as FX risk, exchange rate risk or currency risk) is a financial risk that exists when a financial transaction is denominated	**3**	**3**	**6**	Liquidity is strictly pegged to the need for FX; strictly speaking all liabilities in relation to FX are to support back to back	**2**	**2**	**4**	Fx exposures are hedged every day and kept to a minima	MD	In place	**1**	**1**	**2**

		in a currency other than that of the base currency of the company.				client transactions only									
4	Operational Risk (Staff)	Operational risk is "the risk of a change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and systems, or from external events, differ from the expected losses"	**3**	**3**	**6**	Extensive training has been given to all staff, in the context of their duties and company obligations; staff have been given job descriptions and are regularly monitored. External references and checks are in place to check criminal convictions and previous employment	**2**	**2**	**4**	Compliance Monitoring program and external testing are carried out to determine performance of operational processes; employees are subject to on going performance reviews to ensure they are adhering to processes	MLRO /MD	In place	**1**	**1**	**2**
5	Counterparty risk (banks)	Banks provide indirect access to payment infrastructure; loss of bank accounts translates on inability to settle funds in the UK or to process pay out transactions overseas.	**3**	**4**	**7**	Business model has been adjusted as the business has been de risked by banks in the EU	**3**	**2**	**5**	At present, the business is looking for bank accounts to address the issue of having to pay high fees to third parties cash processing firms.	MD	In place and under close monitoring	**2**	**2**	**4**

6	Data Security (Access)	Firms must ensure Data Access is granted on a secure environment, satisfying regulatory requirements and going forward GDPR	**4**	**4**	**8**	The business has implemented Privacy and GDPR standards	**2**	**2**	**4**	External testing, reviews and audit are being use to further add MI to Management; this is an on going and regular process. Comprehensive IT Security arrangements, with defined access rights, and monitoring arrangements which are tested internally in an ongoing basis	MD	In place and subject to on-going monitoring	**1**	**1**	**2**
8	Data Monitoring	Firms must ensure Data access , use, and process is aligned with regulatory requirements. As such monitoring must be implemented to support existing regulatory requirements	**3**	**4**	**7**	IT Policy contains a number of system driven controls, along with a combination of automated and manual monitoring tools. There is ongoing testing in place to ensure auditable records of monitoring exist.	**2**	**2**	**4**	External testing reviews is in place to further monitoring the performance of data monitoring systems	MD	In place and subject to on-going monitoring	**1**	**1**	**2**

9	Business Continuity and Recovery	Business continuity encompasses planning and preparation to ensure that an organisation can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a reasonably short period.	**3**	**3**	**6**	Arrangements have been organised as per EBA Guidance, fully implementing Major Incident Reporting arrangements, along with intermediary report and final conclusion reports	**2**	**2**	**4**	Arrangements have been tested to ensure performance and ability to operate in "worst case scenario" situations.	MD	In place	**1**	**1**	**2**
10	Data Security (Infrastructure)	Data security refers to protective digital privacy measures that are applied to prevent unauthorised access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type. Data security is also known as information security (IS) or computer security.	**3**	**3**	**6**	Firm currently uses Cloud based infrastructure which supports their operations, along with infrastructure provided by the group. Services are designed to operate in an environment benchmarked against the standards of PSR, as defined by the EBA, in a proportional manner to the type, size and nature of the business	**2**	**2**	**4**	Infrastructure is tested regularly, as a consequence of the PSD2 implementation plan deployed by the business; on going external texting has been put in place to further test the adequacy of existing arrangements and follow up monitoring	MLRO /Director	In place	**1**	**1**	**2**