2023

INTER CITY MONEY LIMITED

ANTI MONEY LAUNDERING POLICIES & PROCEDURES

Contents

Version and Changes Page

Document	**AML Policy & Procedure**
Current Version	**8.0**
Date Created	**12 July, 2017**
Created By	**Arshad Mehmood**
Reviewed By	**Taliq Hussain**
Last Reviewed Date	**18 April, 2023**
Next Review Date	**18 April, 2024**
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. 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

Version 6.0

Amendment of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Update Regulation 33(3) SCHEDULE 3ZA High-Risk Third Countries. As per mentioned updates Pakistan is High-Risk third Country. A statutory instrument came into force on 29 March 2022.

Version 7.0

- Amendments in agent monitoring as per new agent agreement.
- Addition of Terrorist asset-freezing Act 2010, Bribery Act 2010, Data Protection Requirement in Relation to AML_GDPR 2018, Anti-Terrorism, Crime and Security Act 2001 in AML relevant regulation.
- Removal of Pakistan from High-Risk Jurisdictions.
- Inclusion of Card Acceptance and Mobile App Payments.
- Agent monitoring requirement as per HMRC AML/CFT thematic report, audit and compliance requirements for agent and ending a relationship with agent procedures.

Version 8.0

- Addition of pay out corridors.
- Addition of Pay out banks.
- Transaction Threshold

Declaration

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 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 not withstanding its translation into any another language, the English version shall be the definitive version, which shall be referred to for all legal purposes.

Anti-Money Laundering Policy and Procedures Policy Statement

The changing trends and pattern of Money laundering (ML) and Terrorist Financing (TF) is a major global concern. In money-laundering schemes, the funds come from illegal activities and are injected into the legal economy using numerous techniques and vulnerable sectors of the economy. In relation to terrorism, the funding may be derived from criminal activities and origins, but also from legitimate sources or origins. The main concern is to identify those sources to combat ML/TF.

Inter City is committed to the highest standard of money laundering and terrorist financing prevention. We aim to have adequate and proportionate risk assessment tools specific to financial crime risks.

The company also has a dedicated due diligence program with measures and controls in place to ensure compliance with the current regulations, laws and standards. Our aim is to ensure a continuous practice of monitoring and training for an inclusive approach.

The company understands that it has a responsibility to identify and combat money laundering across a broad spectrum. This includes financial transactions, including possessing, or in any way dealing with, or concealing, the proceeds of any crime. Our organization operates in a transparent environment with assessment, monitoring and reporting at the core of all business functions. We are dedicated to the prevention of financial crime and continue to improve upon existing measures.

Inter City understands that the best way to fulfil this commitment is to:

- Establish effective internal policies and procedures to notify whenever it has suspicions of any criminal activity by individuals engaged in a money transfer transaction.
- Carrying out the activities and services provided in accordance with strict ethical standards and current law regulations.
- Implement codes of conduct, monitoring and reporting systems to prevent the company from used for money laundering and terrorism financing.
- Ensure that all employees follow “Know Your Customer” policies and procedures.
- Apply strict compliance with applicable anti-money laundering and terrorism financing laws, as well as with the recommendations issued on this subject by the

International Financial Action Task Force.

The present policies are based on the provision of the relevant UK regulatory framework. 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).

Business Model of the Company

Inter City money limited specializes in providing money remittance services to Pakistan, India, Bangladesh, UAE, China, Ghana, Morocco, Philippines, Thailand and Nigeria. We understand that sending money to the loved ones can be a challenging task, which is why we offer fast and reliable services to make the process easier for our customers.

Inter City money limited offers money remittance services to individual customers to meet the diverse financial needs of our valued customers. We take pride in offering competitive exchange rates, low fees, and fast transfer times. Our experienced team provides excellent customer service and ensuring that the money arrives safely and securely to its destination.

Our money remittance services are conducted via our extensive network of agents designed to provide the customer with a seamless and reliable experience, backed by our commitment to exceptional customer service and industry-leading security measures.

Inter City money limited provide three convenient options for sending money:

- cash
- online transfers
- Mobile Apps (Card Payments)

With our cash transfer service, customer can visit our registered office and initiate transactions at our authorised agent locations conveniently located across the United Kingdom and send money to their recipient in Pakistan, India, Bangladesh, UAE, China, Ghana, Morocco, Philippines', Thailand and Nigeria and rest of the world.

Whereas for those seeking the convenience of online transactions to send money from the comfort of their home, with just a few clicks on their computer or mobile devices through our website and APP. The secure online platform provides a user-friendly interface, enabling

the customers to send money to Pakistan, India, Bangladesh, UAE, China, Ghana, Morocco, Philippines', Thailand and Nigeria. Inter City Money Limited online services are designed to prioritize security while providing the flexibility and ease of transferring funds at customer's convenience.

Online transactions can be made through customer's debit card. We have partnered with TRUST PAYMENT, a trusted payment gateway, to bring customer a seamless and secure card payment experience. After the successful card transaction through the secure checkout of TRUST PAYMENT, all remittance amount is transferred to our account held at FGC Bank.

With the integration of card payments, customer can enjoy the following benefits:

- **Convenience**
  Paying with the card offers a quick and hassle-free checkout process. No need to worry about cash or manual bank transfers—simply enter the card details, and the payment will be processed instantly.
- **Security**
  Inter City prioritise the security of customer financial information. TRUST PAYMENT utilizes industry-leading encryption and security measures, ensuring that your card details are protected and kept confidential throughout the payment process.
- **Versatility**
  Whether the customer prefer to use Visa, Mastercard, or any other major card networks, our payment gateway supports a wide range of card types, providing the customers with flexibility and choice.
- **Fast Transaction Processing**
  By utilizing TRUST PAYMENT's advanced infrastructure, customer card payment is processed in real-time, allowing for instant verification and faster transaction processing.
- **Seamless Integration**
  TRUST PAYMENT's checkout basket seamlessly integrates with our online platform, ensuring a smooth and user-friendly experience.

For final settlement of payments, we ensure prompt and reliable delivery of funds to the beneficiaries in Pakistan, India, Bangladesh, UAE, China, Ghana, Morocco, Philippines', Thailand and Nigeria. To do so, Inter City Money Limited has established strong partnership with pay-out banks in the destination countries. Our trusted pay-out partner Banks assists

us in settling the payment efficiently and securely, ensuring that the beneficiary receive the funds without any hassle.

Money laundering and Terrorist Financing overview

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

Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the 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 either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or like methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

SOURCES OF MONEY LAUNDERING:

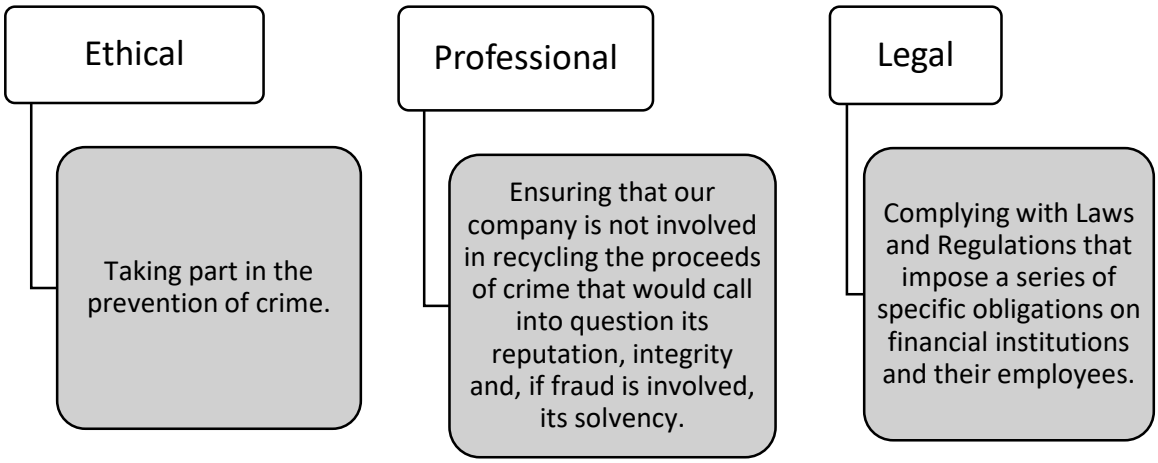
Money laundering may not just involve wealth related to Drug Trafficking / Terrorism financing. List of crimes identified by Financial Action Task Force (FATF) as generators of criminal wealth also included:

- Illegal arms sales.
- Gun running

- Organized crime including drug trafficking and prostitution.
- Embezzlement
- Smuggling (including movement of nuclear materials)
- Counterfeiting (including making of imitation and copies of original products/goods)
- Fraud, especially computer-supported fraud 8. Benefiting from insider trading.
- Bribery and kickbacks
- Tax evasion
- Under and over-invoicing of trade transactions.
- Bogus trade transactions to launder money through round-tripping.
- Facilitating illegal immigration
- Real Estate Transactions

Why should money laundering be prevented?

The prevention of ML and TF from the point of view of a Financial Institution has three dimensions:



It is prohibited to conduct a financial transaction while knowing that the money would be used to fund terrorism, drug trafficking, or other illicit actions. Additionally, it might be illegal to ignore or turn a blind eye to such transactions. Under the legal theory known as "wilful blindness," it is possible for a person or business to face criminal charges for ignoring "red flags" that suggest that funds may be used for illicit activity.

Financial Regulators in UK

The United Kingdom, which is a major player in global finance, is one of the most significant players in the fight against money laundering and terrorism financing. Due to the size and complexity of the financial and real estate markets, AML/CTF poses a serious concern in the UK. One of the most advanced nations in the fight against financial crimes like fraud, money laundering, and financing of terrorism is the UK. The strong anti-money laundering laws in the UK are designed to catch financial criminals.

In the UK, several regulators and authorities stop financial crimes like money laundering and terrorism financing. By lowering the risks associated with money laundering using the money laundering law they have decided upon, these policies seek to limit the negative impacts of corruption on the economy. Institutions that break these regulations' relatively tight standards are subject to administrative sanctions. The regulator also keeps an eye on businesses' AML vulnerabilities and presents businesses with appropriate AML standards. The following are a few of the AML regulators in the UK:

The Financial Conduct Authority (FCA)

The UK's Financial Conduct Authority (FCA), which operates independently of the national government, oversees overseeing the financial services sector. FCA seeks to regulate the actions of financial institutions in both the retail and wholesale markets. Implementing Customer Due Diligence (CDD) measures that take a risk-based approach is required by FCA regulations. Regulations also seek to identify and stop financial crimes including money laundering and sponsorship of terrorism. To reduce the danger of money laundering, all institutions covered by the UK Money Laundering Regulations must adhere to their policy and procedural requirements. Through routine inspections, FCA keeps an eye on and audits these companies. Institutional AML controls should be organized according on the size, services, and products of the organization.

HM Revenue and Customs (HMRC)

The taxing authority for the UK government is called His Majesty's Revenue and Customs (HMRC). In general, HMRC oversees tax collection, guarding the UK's borders from illegitimate activity, and making sure employers pay the minimum wage. Along with all these duties, HMRC collaborates with FCA to investigate allegations of money laundering. The law that HMRC creates to prevent financial crime aims to launder money within these rules. Additionally, HMRC organizations seek to lessen the risk of money laundering.

National Crime Agency (NCA)

The National Crime Agency (NCA) is in the forefront of efforts to stop large, organized crime's

operations in the UK. Senior NCA officers assist front-line law enforcement personnel by pursuing the most serious and dangerous criminals. It eliminates the offences it uncovers and imposes harsh penalties on each individual and institution necessary. The NCA is fighting a crime that involves both money laundering and terrorist financing.

NCA works with regional and global partners to combat risks from money laundering and terrorism financing. NCA can identify money launderers and apprehend them to stop illegal activity. As a result, it makes the UK a difficult location for those looking to utilize it for money laundering. The NCA seeks to train and educate financial workers on how to spot symptoms of money laundering and create innovative techniques for apprehending criminals.

AML LAWS AND LEGISLATIONS

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.
8. Terrorist asset-freezing Etc. Act 2010
9. Bribery Act 2010
10. Data Protection Requirement in Relation to AML_GDPR 2018
11. Anti-Terrorism, Crime and Security Act 2001

Proceeds of Crime Act (POCA) in the UK

The POCA (Proceeds of Crime Act) deals with locating and freezing assets acquired unlawfully. By keeping money and support for crime hidden, POCA keeps working to reduce the number of criminals. The goal of the law is to stop criminals from using black money for their own gain. Activities including the concealing of illicit property and the conversion of criminal property are regarded as crimes in the UK, according to the 2002 POCA. Additionally, all institutions subject to legal restrictions should create a suspicious report for any money laundering operations.

Terrorist Asset-Freezing Act 2010

The Terrorist Asset-Freezing etc. Act 2010 gives HM Treasury power to freeze the assets of individuals and groups reasonably believed to be involved in terrorism, whether in UK or abroad, and to deprive them of access to financial resources.

The Terrorism Act 2000

The Terrorism Act sets out the primary offences relating to terrorist funding. Regulated businesses like money service businesses must report a belief or suspicion of offences related to terrorist financing, such as:

- fund-raising for the purposes of terrorism
- using or possessing money for the purposes of terrorism
- involvement in funding arrangements
- money laundering -facilitating the retention or control of money, which is destined for, or is the proceeds of, terrorism.

Counter-Terrorism Act 2008, Schedule 7

The Treasury has powers under Schedule 7 to the Counter-Terrorism Act 2008 to require financial firms to takes specified actions in relation to a country of concern, or counter parties based in that country. Use of this power can be triggered if the risk of money laundering or terrorist financing activities is identified in a country.

Criminal Finances Act 2017

The Criminal Finances Act 2017 make important amendments to the Proceeds of Crime Act, the Terrorism Act and the Anti-terrorism Crime and Security Act to expand the provisions for confiscating funds to deal with terrorist property and proceeds of tax evasion.

The Fifth Anti Money Laundering Directive (5AMLD) for the UK

For EU Member States, the Fifth Anti-Money Laundering Directive (5AMLD) went into effect on January 10, 2020. The UK opted to pursue this directive despite having previously left it. The Fifth Money Laundering Directive (5AMLD) amends the Fourth Money Laundering Directive (4AMLD) to stop financial system misuse, money laundering, and financing of terrorism. Before beginning a commercial relationship with a new customer, it is necessary to take "strict Customer Due Diligence (CDD) steps" to investigate the current firm and important property data, according to 5AMLD.

Inconsistencies between information collected from customers and information on registered beneficial properties should be reported by all companies to the relevant

competent authorities. Additionally, 5AMLD mandates that all trusts be expanded from the UK's tax consequences trusts and that trust records be made publicly available. The UK government anticipates that this order, part of the country's Anti-Money Laundering and Counter-Terrorist Financing regime, will successfully combat these crimes and reduce the constraints placed on businesses.

Anti-Terrorism, Crime and Security Act 2001

In December 2001, Parliament passed the Anti-Terrorism Crime and Security Act 2001 (ATCSA), Part 4 of which allowed the Home Secretary to order the indefinite detention of foreign terrorist suspects who could not be deported on the grounds that they faced a real risk of ill-treatment contrary to Article 3 ECHR. The objective of the Anti-Terrorism Crime and Security Act 2001 (ATCSA) is to ensure that the Government has the necessary powers to counter the terrorist threat to the UK. Part 7 of the Act is intended to improve the security of dangerous substances that may be targeted or used by terrorists.

Bribery Act 2010

The United Kingdom Bribery Act of 2010 ("UK Bribery Act") is the primary anti-corruption law in the United Kingdom. It came into force in July 2011 and applies to both public and private sector bribery. The Ministry of Justice, in its Guidance on the Bribery Act 2010, presents six principles for implementing adequate procedures to prevent bribery.

These are:

- Proportionality.
- Top-Level Commitment.
- Risk Assessment.
- Due Diligence; Communication; and
- Monitoring and Review.

As per the Bribery Act 2010, all parties involved with bribery are offenders, meaning, both the person or entity giving or offering or promising the financial or non-financial gifts or benefits or other advantages and the person or entity receiving or supposed to receive the financial or non- financial gifts or benefits or other advantages, are offenders under this act.

Under the Bribery Act 2010, even if the financial or non-financial gifts or benefits or other advantages are offered or promised by a third party or are received or supposed to be received by a third party who is not the same party accomplishing or performing the functions

as agreed, this third party will also be an offender.

Offences as per Section 1, 2 and 6 of the Bribery Act 2010

- The act of one giving, offering or promising any financial or non-financial gifts, benefits or any other advantages (with the intention of inducing another party to perform improperly a relevant function or activity, or reward the said party for performing the same act).
- The act of requesting, accepting, or agreeing to accept any financial or non-financial gifts, benefits or any other advantages (intending that, in consequence, a relevant function or activity should be performed improperly).
- The act of giving, offering or promising any financial or non-financial gifts, benefits or any other advantages to a foreign public official (with the intention of influencing the foreign official in the individual's capacity as a foreign public official.)

Non-Compliance with these laws and Regulations

In The UK, as discussed, regulators had introduced laws to prevent money laundering and terrorist financing. And if any organization does not comply with these regulations or delays complying with them, the competent authorities initiate some criminal proceedings. These penalties can be financial penalties depending on the nature and severity of the crime and up to 14 years in prison. Regulated institutions must also comply with a risk-based approach to comply with these laws. Therefore, regular risk assessments must be conducted and as a result, a unique AML Compliance Program must be established.

Money Laundering Offences:

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

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

It is an offence to enter 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.

- *Maximum Fourteen years imprisonment and/or an unlimited fine*
  It is an offence to acquire use or have possession of criminal property.
  Maximum Fourteen years imprisonment and/or an unlimited fine

The MLRO will handle all contact with Law Enforcement Agencies.
The MLRO will be responsible for providing information and updates to the legislation as and when they occur.

Inter City 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

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 several:

- 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

Penalties

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-financial-sanctions-implementation

Following websites contain the details of different issues discussed in this document:

Financial Conduct Authority (FCA) website;	https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing
HM Revenue & Customs (HMRC)	www.hmrc.gov.uk
	fit and proper https://www.gov.uk/government/publications/money-laundering-supervision-fit-and-proper-test-and-approval/money-laundering- supervision-guidance-on-the-fit-and-proper-test-and-hmrc-approval penalties https://www.gov.uk/government/publications/money-laundering-supervision-enforcement-measures/money-laundering-supervision-civil-measures MSB Anti ML Supervision [link below]
Office of Foreign Assets Control (OFAC);	www.treasury.gov/ofac
HM Treasury	www.hm-treasury.gov.uk

Role of Senior Management:

The senior management of Inter City oversees handling all business risks, including ML and TF risks. Obligations of Senior Management 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.

The senior management is also responsible for the following to ensure that the company's policies, processes, systems, and controls are successful in combating money laundering and terrorist financing:

- The creation, implementation, and maintenance of efficient risk-sensitive AML/CFT policies, processes, systems, and controls; the prompt and frequent dissemination of information about the management of money laundering risks.
- Creating, delivering, and maintaining a suitable continuous AML/CFT training programme for all Inter City future employees.
- Ensuring that the proper steps are taken to integrate ML and TF into daily operations. Additionally, the risk analysis should be updated via an event-driven review anytime senior management notices that events have changed ML/TF risks. AML policies, controls, and procedures may need to be changed in response to a new analysis, which could have an impact on, for instance, the relevant employees' training programmes.

Responsibilities of MLRO

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: - +4401535685754
Email: - info@intercitymoney.com

The MLRO is the focal point within the company for the oversight of all activity related to anti-financial crime issues. The critical role of MLRO in an organization places immense responsibility on MLRO.

Responsibilities of MLRO at Inter City include but are not limited to the following:

- Carry out a risk assessment identifying where the business is vulnerable to money laundering and terrorist financing.
- Prepare, maintain and approve a written policy statement, controls and procedures to show how the business will manage the risks of money laundering and terrorist financing identified in risk assessments.
- Review and update the policies, controls and procedures to reflect changes to the risk faced by the business.
- Make sure there are enough trained people equipped to implement policies adequately, including systems in place to support them.
- Monitor effectiveness of the business's policy, controls and procedures and make improvements where required.
- Have systems to identify when you are transacting with high risk third countries identified by the EU or financial sanctions targets advised by HM Treasury and take additional measures to manage and lessen the risks.

- Help management create and maintain a culture of anti-money laundering and counter-terrorist financing compliance.
- Ensuring the company's risk management guidelines, risk assessment methodology, and implementation are properly documented.
- Creating internal policies in accordance with legal standards and pertinent sector recommendations.
- Ensuring that all reports of internal suspicious activities are investigated right away.
- Ensuring that all reasonable suspicions are reported via a SAR to the appropriate law enforcement agency.

- Ensuring that all staff are aware of their personal obligations and the firm's policies and procedures and that the basis for the firm's risk-based approach is understood and applied.
- Ensuring that staff comply with the stated policy and monitor operations and development of the policy to this end.
- Ensuring that all relevant staff are adequately trained in money laundering and terrorist finance prevention and that the standards and scope of the training are appropriate, and that appropriate training records are kept.
- Regularly reviewing the effectiveness of money laundering compliance policies and procedures to prevent money laundering and counter the financing of terrorism.
- Making recommendations for action to remedy any deficiencies in policies, procedures, systems or controls and follow up on those recommendations.
- Representing the firm to all external agencies, e.g. regulators or law enforcement agencies, and in any other third-party enquiries related to money laundering prevention, investigation or compliance.
- Remaining aware of any relevant sanctions, prohibitions or advisory notices. Also, if necessary, advise management and relevant staff of the names of any individuals and institutions on the sanctions list.
- Promptly responding to any reasonable request for information from the regulator and/or law enforcement agencies.

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 wilful 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:
    - Are different from the customer's normal pattern.
    - Have changed since the agency relationship was established.
    - Are higher than comparable agencies.
    - 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 birthday and address the same.
- Transactions too fast to be possible.

Under the instructions contained in **HMRC AML/CFT Thematic review report**, following checks will be made by Inter City money limited (on agents) to fully comply with the said rule:

- Adopting and applying a written policy to risk assess our potential agents.
- Documenting the assessment of each agent risk.
- Having appropriate equipment, software, reporting, and appropriately trained staff as are needed to effectively.
- Monitoring the agents and ensuring that sufficient time is available to those staff, having regard to the risks involved.

- Establishing expected levels of transactions for each agent.
- Establishing the main geographical corridors served and understanding the likely variations in business levels due to religious festivals, holidays, and other seasonal factors.
- Reacting promptly to any significant fluctuation in expected activity and obtain and record reasonable explanations for them.
- Allocating sufficient resources to agent monitoring, and keeping those resources under review when, for example, there is significant growth in their agency network (the number of agents, locations served, business volumes, etc); and
- Ensuring sufficient protection against conflicts of interest such as agent monitoring staff being independent of local/regional agent sales/recruitment teams

Training and Awareness

Training on money laundering typologies has long been seen as a crucial component of AML-CFT controls since employees and agents are a company's greatest line of defence against individuals who finance terrorism and money laundering. People and criminal organisations constantly attempt to take advantage of the services provided by the businesses and utilise them for illicit purposes. It would be simpler for criminal organisations to smuggle the proceeds of their crimes into the financial system if the personnel of an organisation were not taught on AML.

To ensure that every member of the Inter City money limited.'s staff is aware of their responsibility to abide by AML/CFT laws, regulations, and internal standards, 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

Audit and Compliance (for agents)

Audit and compliance for agents are critical to ensure the legality, security, and transparency of financial transactions. Inter City money limited consider the following when conducting audit and compliance of agents:

- Regulatory Compliance
- AML and CTF Program
- Internal Controls
- Record-Keeping
- Training and Awareness
- Risk Assessment
- Technology and Security
- Reporting and Regulatory Filing

To conduct audit and compliance Inter City will:

- Consider whether it is appropriate to carry out a selective audit of an agent's compliance with the requirements placed upon them. The selection of agents is to be

primarily risked based – that is to say at least half of the agents should be selected by the application of criteria designed to address the highest risk agents.

- Consider whether it is appropriate to carry out an independent internal audit within the business of the Inter City to assess the extent of the compliance and that of the agents with this guidance. HMRC encourages businesses to have internal independent review of the risk assessment of ML and TF.
- Make copies of such audit or review reports available to HMRC; and
- Take appropriate steps to address non-compliance with our requirements by our agents, having regard to the extent, seriousness and impact of that non-compliance.
- Promptly report such steps and the circumstances that gave rise to them to HMRC.

Ending a Relationship

Inter City will comply with the legal obligations to make a Suspicious Activity Report (SAR) where a relationship with an agent is ended because of suspicions that the agent is involved in money laundering or other criminality.

When a business relationship with an agent ends Inter City will:

- Immediately report that change, with a brief explanation, to HMRC.
- Secure and remove records of business conducted via that agent; and
- Promptly remove any unused stationery, exterior or interior signage, etc. that bears the name or logo of the principal or otherwise suggests the agent has a relationship with the principal.

Our Risk Based approach.

Our risk-based approach involve.

- applying Due diligence at the start of customer engagement
- which means identifying the customer and verifying the customer's identity based on documents, data or information obtained from a reliable and independent source.
- 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).
- 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.

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.

KNOW YOUR CUSTOMER POLICY (KYC)

One of the main Anti-Money Laundering strategies is the Know Your Customer Policy (KYC) KYC Policy: "**Know Your Customer**" (KYC) is a set of guidelines designed for proper identification of an account holder or customer for the scrutiny or monitoring of large value cash transactions. It aims to prevent financial institutions from being used intentionally or unintentionally by criminal elements for committing financial frauds or for the transferring or depositing of funds derived from criminal activity. The adoption of ''know your customer policy" or procedures by Inter City Money Limited has proven extremely effective in detecting suspicious activity in a timely manner.

KYC Approach:

Inter City Money Limited KYC policy is at the heart of the anti-money laundering measures adopted by the company. The Company strictly follows all the due diligence policies and procedures of Her Majesty's Revenue and Customs (HMRC) to identify the customer before the transaction takes place.

The three main areas of the policy are aimed at are:

- Ensuring that reasonable measures are taken to obtain information about the identity of the persons on whose behalf a transaction is made.
- There are record keeping procedures that are followed – all necessary records on transactions, either domestic or international are created and maintained for a specific period.
- Special attention is given to all complex, unusual large transactions.

The policy framework of Inter City Money Limited is intended to regulate the operations to

ensure the flow of only legal money through the remittance channels.

We aim to:

- Determine the true identification of each customer seeking to conduct a transaction.
- Complete the identification and verification process for all customers carrying out a transaction of £ 3000 or above.
- Complete the identification and verification process for all transactions regardless of the size of the transaction.
- Be aware of any unusual transaction activity to prevent the creation of fictitious accounts.
- Implement all regulatory and internal procedures properly.

Inter City Money Limited will focus on correctly profiling the customer in the Remittance application forms by obtaining and recording the following evidence of identification:

- Where the individual is a UK national resident in the UK and will be seen in person by the member of staff carrying out the verification, identity will be conducted by examination of:
    - one document confirming the individual's name, such as a passport.
    - one document confirming the individual's address, such as a utility bill.
- The company's MLRO will maintain a list of acceptable documents. Only originals or certified documents, not copies, will be accepted for examination. In the case of larger transactions, further evidence of permanent address and evidence of income is required.
- Where clients are an individual person or persons acting on their own behalf, the identity of the individual(s) will be verified by members of staff authorised by the company's MLRO, who will ensure that staff so authorised receive appropriate training.
- In cases where a client cannot produce acceptable documents, the MLRO will make a risk-based decision on accepting the documents that are available, consulting with the compliance director if appropriate.
- Where the client is a corporate entity such as a private limited company, the compliance team will check that the entity is appropriately incorporated and registered and take the necessary steps to determine who are the principal beneficial owners, and who exercises control, and their identity will be verified according to this

procedure.

- Where the client is a listed company or a regulated firm, the compliance team will check that the client is appropriately registered, and that the person with whom the company is dealing is properly authorised to act on the client's behalf and will verify the identity of that person according to this procedure, in addition to that of the client entity.
- In all cases where enhanced client due diligence is required, MLRO to decide on additional steps to verify the client's identity.
- All verification of identity processes will be recorded. This will include keeping photocopies of documents produced, or in exceptional cases with the approval of the MLRO, recording information about where copies are held and can be obtained.

What is the business relationship?

A business relationship exists where the company sets up a process with the customer, which makes it easier for them to make regular transactions. In situations where a business relationship exists, there is an obligation to obtain a proof of ID, plus confirmation of the purpose of transaction and source of funds. There is an obligation on the company to monitor all transactions carried out in the business relationship (see transaction monitoring).

CDD (Customer Due Diligence)

Customer due diligence (CDD) is a series of checks to help us verify the customers' identities and assess their risk profiles. CDD is a regulatory requirement for companies entering into business relationships with a customer and is a big part of anti-money laundering (AML) and Know Your Customer (KYC) directives.

Inter City money limited has adopted a Customer Identification program and will seek identification, collect certain minimum customer identification information from each customer and record such information. Formal identification evidence must be obtained for all new customers conducting transactions with the company. Documentation must be from a reputable and identifiable source.

To verify the identity of the customer the firm will apply Customer Due Diligence procedure which includes the following:

- 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.
- 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.

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.

We 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.

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, which does not imply that we do not have to perform customer due diligence, we still verify customer and beneficial owner identity. We verify the customer or beneficial owners' identity during the establishment of a

business relationship and use one document to verify identity. And use the information to determine the nature or purpose of a business relationship without requiring further information, for example, if our customer is a pension scheme, we 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 threshold 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 the factors, for example a customer from another EU state is not automatically low risk simply because they are from the EU. All 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.

For transactions below GBP 8000 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 850 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.

As part of our customer due diligence measures, we must identify individuals. We will obtain. a private individual's full name, date of birth and residential address as a minimum.

We 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:-

- A valid passport
- A valid photo card driving licence (full or provisional)
- A national identity cards.
- 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 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:-

- Photocopy's 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.

Transaction Monitoring

Inter City money limited is committed to continuously monitoring the effectiveness of its 1st Line controls, which mitigate the risks of money laundering and terrorist financing presented by transactions, So all our transaction will be undergoing continuous transaction monitoring and once all the checks are done by compliance team then only to ensure that Inter City money limited.'s AML/CTF policies and procedures have been adhered to and that the

operating effectiveness of the 1st Line defines has been demonstrated.

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

QUICK GUIDE FOR CDD/EDD

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 bills (gas and electricity) Landline telephone bill TV/Home broadband bill Bank/Mortgage/Credit Card statement Document issued by any other government agency, e.g., HMRC, UKVI, NHS Electronic AML Check Pay slip/ Wage slip Water bill. P45/ P60 Council tax TV License	**90 days** **90 days** **90 days** **90 days** **1 year from the search date** **90 days** **180 days** **1 year**
Driving license (only when not used as proof of ID)	**1 year from the date of transaction or up to the expiry date of the license, whichever is shorter. Reusable every year up until the actual expiry of the license.**

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

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)

Enhanced due diligence (EDD) involves determining, based on a risk-based approach, to investigate clients more thoroughly – requiring significantly more evidence and detailed information about reputation and history to be collected. Enhanced due diligence applies in situations that are of high risk. It means taking additional measures to identify and verify the customer identity and source of funds and doing addition ongoing monitoring.

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 are 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.

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 is undertaken periodically (normally after every 12 months) 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.

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

- 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 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.

Amendment of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Update **Regulation 33(3) SCHEDULE 3ZA High-Risk Third Countries.**

Inter City money limited risk has decreased to medium level but still we will ensure that we record enough information that will help us form a true picture of the client. As follows:

- 1 form of photographic ID
- 1 form of proof of address
- Disclaimer/questionnaire for the origin of funds not being derived from the proceeds of crime.
- Source of funds verification in the form of a recent Bank statement showing the movement of funds.
- 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.
- If unusual Documents you found, please consult with MLRO and External Consultant for further verification.

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 Postmaster
- Doctor
- Chartered Accountant
- Police Officer

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 mortgage, 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 (i.e. under the mattress) then these funds require declaration to HMRC and MLRO to decide on the instruction

Pay-out-Partner Evaluation:

Inter City Money Limited currently deals with remitting money to Pakistan, India, Bangladesh, China, Ghana, Morocco, Philippines', Thailand and Nigeria, which is not considered a high-risk country, therefore we have to do enhanced due diligence on all transactions associated with high risk country, yet we tend to perform the Risk Based Approach and take additional measure in case if customer is acting suspicious or our internal procedure encourage us to perform the EDD on that transaction, Our EDD Procedures include:

- 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 customers 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 customers.
- 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.

Country wide evaluation (Pay-out-Partner)

Nigeria:

Nigeria is on the FATF List of Countries that have been identified as having strategic AML deficiencies.

Thailand:

Thailand is no longer on the FATF List of Countries that have been identified as having strategic AML deficiencies.

Philippines:

The Philippines is on the FATF List of Countries that have been identified as having strategic AML deficiencies. This country is also considered as Blacklist for EU Tax base. Having high criminal and terrorism rate.

Morocco:

Morocco is no longer on the FATF List of Countries that have been identified as having strategic AML deficiencies.

Ghana:

Ghana is no longer on the FATF List of Countries that have been identified as having strategic AML deficiencies Corruption index (transparency International) 43%.

(DNFBPs), whose operations are largely cash-based, present significant money laundering/terrorist financing risks and continue to represent the largest gaps in Ghana's AML/CFT regime.

China:

In September 2018, the US State Department imposed sanctions under Caatsa against third parties in China for dealing with blacklisted Russians. Officials said that they decided to act against the Chinese military procurement organisation, the Equipment Development Department, after it purchased military equipment from Moscow in November 2017. China is not on the FATF List of Countries that have been identified as having strategic AML deficiencies

UAE:

The United Arab Emirates is on the FATF List of Countries that have been identified as having strategic AML deficiencies. United Arab Emirates is categorised by the US State Department as a Country/Jurisdiction of Primary Concern in respect of Money Laundering and Financial Crimes

Bangladesh:

Bangladesh is no longer on the FATF List of Countries that have been identified as having strategic AML deficiencies. According to that Evaluation, Bangladesh was deemed Compliant for 9 and Largely Compliant for 27 of the FATF 40 Recommendations. It was deemed Highly Effective for 0 and Substantially Effective for 3 of the Effectiveness & Technical Compliance ratings.

India:

India is categorised by the US State Department as a Country/Jurisdiction of Primary Concern in respect of Money Laundering and Financial Crimes. India is not currently subject to any International Sanctions however the UK government has had a stated policy on exports to nuclear and nuclear-related end users in India and Pakistan since March 2002.

Pakistan:

Pakistan is no longer on the FATF List of Countries that have been identified as having strategic AML deficiencies. Pakistan is categorised by the US State Department as a Country/Jurisdiction of Primary Concern in respect of Money Laundering and Financial Crimes. Pakistan is not currently subject to any International Sanctions however the UK government has had a stated policy on exports to nuclear and nuclear-related end users in India and Pakistan since March 2002.

Banks as a Corridors:

Inter City is dealing with following banks as a corridors for pay out banks:

- **Clear Bank:**

Clear.Bank

Inter City Money limited is working with partnership with Clear bank. This corridor is

used for customer segregated account for online payments.

- **EM Bank:**

  All API are required to have a segregated account for operations and customer funds, Inter City Money Limited is using EM Bank account for customer segregated account.

- **Choice Forex:**

  Inter City is affiliated with Choice Forex. This corridor is used for cash collection and settlement.

- **GCC Exchange**:

  We use GCC Exchange pay-out services worldwide. Both the parties are desirous to cooperate to their joint and mutual benefit under the laws of United Kingdom.

- **Trust Payments:**

  Trust Payments provide seamless and Omni Channel commerce experiences across any and every channel – Wherever our customers are, however they are wish to pay, on any device. We call this coverage commerce

(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

To comply with regulations, Inter City Money Limited will ensure that all accounts relating to PEP’s must.

- Be approved by the MLRO.
- Be subject to enhanced due diligence.

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.

Linked Transactions

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:

- Are the number of transactions carried out by the same customer within a short period?
- Could several customers be carrying out transactions on behalf of the same individual or group individuals?
- 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

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

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. A**
2	**01-12-2020**	**BCA**	**Mr. B**	**Mr. B**
3	**01-12-2020**	**CBA**	**Mr. C**	**Mr. C**
4	**01-12-2020**	**DBA**	**Mr. D**	**Mr. D**

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.**

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
1	1 -12-2020	ABC	Mr.

TRANSACTION THRESHOLD

Mandatory Fields:

You must need to collect following information while making Transaction.

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

For Cash Transaction

Account	Frequency	Requirements
£1-2500	30 Days	1 Photo ID, Proof of address/Electronic Verification
Above £5000	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	Requirements
£1-3500	30 Days	1 Photo ID, Proof of address/Electronic Verification
Above £5000	30 Days	1 Photo ID, Proof of address/Electronic Verification, Bank Statement/Payslip to verify the funds, Source of Fund declaration.

Account	Frequency	Requirements
Above £5000 (For Cash)	90 Days	1 Photo ID, Proof of address/Electronic Verification
Above £12,500 (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 3rd January 2023 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 3rd January 2023 the aggregated amount will be calculated from 6th December 2022.

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, it 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.

£18,000 aggregated in a year, will require Proof of occupation. In some cases, it is a single transaction of more than £18,000 proof of funds and proof of occupation will be required.

Automated System and Controls

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.

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.

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 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:

- Full name
- Date of birth
- 1 photographic Identification
- 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 e.g. 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. 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: -

- Obtain acceptable photographic identification and photocopy same
- 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

Certify the documentation by signing and dating and including the words e.g. '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.

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: -

- **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.
- 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.
- **Refresher Training -** all relevant staff will 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.

Suspicious Transactions

The Proceeds of Crime Act 2002 (POCA) requires (amongst other things) that when during

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 while 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: -

- The person suspecting should immediately make a written report or e- mail to the MLRO.
- if urgent telephone first, then follow up with a written report.
- no discussion with other members of staff should take place.
- a record of the date and time of report should be recorded.
- Acknowledgement of the receipt of the report should be obtained from the MLRO. This can be done via a receipt email from the MLRO.
- 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 crime may lead to Maximum Five years imprisonment and/or an unlimited fine.

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.

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

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

It is an offence to enter 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.

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

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 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.

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.

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.

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.

Inter City Money Limited consider following in deciding risk and whether 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.

Inter City Money Limited consider following when deciding risk and whether 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.

Inter City Money Limited consider following when deciding risk and whether 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 off applies.

Bribery Prevention Policies and Procedures

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 companies.
- Bribery Prevention Officer, including any knowledge or substantiated suspicion of bribery.

- offenses arrived at in the course of their work, whether 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

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, to induce them to act, or reward them for having acted, improperly in their employment or official capacity by favouring 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.

- 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 favouring 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 are 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

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.

- 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 favouring 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 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 of business gifts, and whether approval was granted.

Policy and Procedure on Accepting Business Gifts

- 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.

- 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 favouring 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 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

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.

- 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

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.
- 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

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.

- 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

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.

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 always have access to this information for reference.

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

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 must work within a framework set by law. Any decisions we make must be in line with relevant laws, we may not always be able to meet your expectations.

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 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

What is GDPR?

The **General Data Protection Regulation** (GDPR) was implemented on May 25th, 2018, transforming the way organizations within the EU handle the personal data of their customers and clients. GDPR creates, clarifies, and harmonizes data security legislation across all EU member-states – but also affects organizations from outside territories wishing to do businesses within the bloc.

Practically, GDPR limits the ways in which businesses can collect, use, and store the personal

data of their customers and clients – it also creates consequences for institutions with AML obligations.

GDPR vs. AML

Since **Anti-money Laundering** (AML) efforts require an intense focus on personal data, the restrictions introduced by GDPR may represent a challenge for financial institutions. More specifically, the legal scope of GDPR may clash with the way institutions identify customers during their due diligence procedures and how they manage their risk thereafter.

As a financial institution, delivering GDPR compliance while managing your AML obligations is an important priority – especially since GDPR **compliance penalties** can reach up to €20 million (or 4% of global revenue). With the stakes so high, it's worth exploring the points at which the two legislative frameworks clash and how any regulatory friction may be resolved.

Article 6 of GDPR requires data controllers to establish a legal basis for collecting and processing personal data – including data required for AML purposes. For institutions with AML obligations, the most relevant justifications provided by Article 6 are:

- **Article 6(c)** – which allows for the processing of personal data "for compliance with a legal obligation to which the controller is subject" – typically, AML laws or sanctions.
- **Article 6(f)** – which allows for data processing for "legitimate interests", justifiable on a case-by-case basis.

One of the most significant aspects of the GDPR is Article 17, which introduces the "**right to be forgotten"**. That right allows data subjects to request the deletion of their personal data under certain circumstances. This rule may be in contention with AML law, which requires data to be held long after a business relationship has ended.

Under GDPR Article 17(3)(b), however, legal requirements take precedence over the right to be forgotten. From an AML perspective, the EU's **4th Anti- Money Laundering Directive** (4AMLD) introduced the requirement that both customer due diligence and transaction records be retained for 5 years after the end of the customer relationship. In this context, the right to be forgotten would only be enforceable after this period had ended.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data must follow strict rules called 'data protection principles. They must make sure the information is:

- used fairly, lawfully and transparently.
- used for specified, explicit purposes.
- used in a way that is adequate, relevant and limited to only what is necessary.
- accurate and, where necessary, kept up to date.
- kept for no longer than is necessary.
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

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 to facilitate access to information relating to individuals. (Information relating to companies and other "legal" persons are 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 must 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

- 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 8.0

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.

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.

The DPA requires that all 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.

- Processing is justified if it is necessary to fulfil a UK legal obligation. This will include, for example, processing 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 such a contract. This will justify some processing of personal data relating to individual customers.
- Processing can be justified based on 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 several 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.

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.

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 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, based on legal advice, if necessary, that it can be made without breach of the DPA.

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 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.

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 based on 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.

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 based on 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 based on the automated processing of their personal data, without any human intervention.

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.

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	