Amana Express Ltd

Amaana Money Transfer

RISK ASSESSMENT APPROACH 2023

VERSION #	APPROVED BY:	REVIEWED BY:	PREPARED ON:	ASSESSED ON:	REVISION DUE:
1	MOHAMED ADEN ABDI	ABM GLOBAL COMPLIANCE UK LIMITED	11.06.2020	25.06.2020	10.06.2021
2	MOHAMED ADEN ABDI	MOHAMED ADEN ABDI	10.06.2021	29.06.2021	10.06.2022
3	MOHAMED ADEN ABDI	ABM GLOBAL COMPLIANCE UK LIMITED	15.06.2022	25.06.2022	10.06.2023
4	Ibrahim Abdulle Olow	ABM GLOBAL COMPLIANCE UK LIMITED	15.05.2023	25.05.2023	10.06.2024

148 High Street, Harlesden, London, England, NW10 4SP, and

COMPANY NO: -04741313

Contents

Policy Statement

Amana Express Ltd is a Small payment institution, which provides services of Money remittance for United Kingdom to Somalia with the turnover level of Less than £3 million per month.

Amana Express Ltd is committed to its customer's full satisfaction through years of experience in London, United Kingdom. Amana Express Ltd has earned its customer's loyalty by showing speed and reliance. Part of the Amana Express Ltd corporate objectives is to understand customer's needs and to provide them with the best service to satisfy those needs.

Amana Express is Money Transfer Company in Somalia. With so many agents in the around the world and lot of payout locations in Somalia. Amana Express is the right choice for migrants who regularly send money to their families and friends in Somalia.

In order to achieve customer satisfaction, Amana Express Ltd has built a great customer team to assist. Amana Express Ltd has provided its team with the latest technology available to ensure the right blend of professional and reliable services expected by its customers. Boards of Directors and Senior Management have over 7 year of professional experience.

In evaluating the level of risk, Amana Express Ltd has followed risk-based approach and weighed a number of factors, including the risk identification and measurement of products, services, customers, delivery channels and geographic locations.

Amana Express Ltd has establish an effective operational and security risk management framework (hereafter 'risk management framework'), which is approved and reviewed, at least once a year, by the management body and, where relevant, by the senior management. These frameworks focus on security measures to mitigate AML, operational and security risks and fully integrated into the Amana Express Ltd overall risk management processes.

Risk-based approach

- A risk-based approach is where we assess the risks that our business may be used for money laundering or terrorist financing, and put in place appropriate measures to manage and lessen those risks. An effective risk-based approach will identify the highest risks of money laundering and terrorist financing that our business faces, and put in place measures to manage these risks.
- Several features of the money service business sector make it attractive to criminals, such as its worldwide reach (in the case of money remitters), the ease of making cash transactions, the one-off nature of many transactions and the speed, simplicity and certainty of transactions.
- Risk-based approaches balance the costs to our business and customers with a realistic assessment of the risk that our business may be exploited for the purpose of money laundering and terrorist financing. It allows us to use our informed judgment to focus our efforts on the highest-risk areas and reduce unnecessary burdens on customers presenting a limited risk of money laundering and/or terrorist financing.

Risks our business may face

- Assessing our business's risk profile will help us understand the risks to our business and how they may change over time, or in response to the steps we take. This will help us to design the right systems that will 0spot suspicious activity, and ensure that staffs are aware of what sort of indicators of possible money laundering they may encounter.

- The risk profile depends on factors including the nature of our business, how it is structured (e.g., the branch network), the areas it operates in, who our customers are, where they are from and the vulnerability of our services or transactions to financial exploitation.

Risk indicators

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

Money transmitters

The following are examples of common risks for money transmitters:

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

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

New customers

The following are examples of common risk indicators for new customers:

- checking the customer's identity is difficult the customer is reluctant to provide details of their identity or provides fake documents

- the customer is trying to use intermediaries to protect their identity or hide their involvement

- there's no apparent reason for using our business's services, for example, another business is better placed to handle the size of transaction or the destination of the transmission

- the customer is unable to provide satisfactory evidence of the source of the funds

- unusual source of funds

- the transmission is to a high-risk country

- non face-to-face customers

- the customer owns or operates a cash-based business

- there's an unusually large cash transaction

- the size and frequency of the transaction is different from the customer's normal pattern
- the pattern has changed since the business relationship was established
- the transaction seems to be unnecessarily complicated, or seems to use front men or companies
- the customer sends or receives money to or from himself
- the customer is acting on behalf of third parties without there being an appropriate family or business relationship between them
- other people watch over the customer or stay just outside
- the customer reads from a note or mobile phone
- an under-age person sends or receives funds from multiple sources
- there has been a significant or unexpected improvement in the customer's financial position
- the customer (or two or more customers) is using more than one local Money service business, perhaps to break one transaction into smaller transactions

Transactions

The following are examples of common risk indicators where transactions:

- are just below the threshold for due diligence checks
- appear to have no obvious economic or financial basis benefit
- route through third countries or third parties
- regularly go to or from tax haven countries
- information accompanying the payment appears false or contradictory
- are destined for money service businesses around the borders of countries at high risk of terrorism.

Where the beneficiary of a money transmission is in a high-risk country we do enhanced due diligence checks on our customer. To check high risk country, we visit

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

https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial- supervision-and-risk-management/anti-money-laundering-and-counter-terrorist- financing/eu-policy-high-risk-third-countries_en

(Based on Directive (EU) 2015/849, Article 9, the Commission is mandated to identify high-risk third countries having strategic deficiencies in their regime on anti- money laundering and counter terrorist financing. The aim is to protect the integrity of the EU financial system)

Use of agents

The following are examples of common risk indicators that principals and agents need to be aware of:

- represent more than one principal or act as both an agent and a principal
- 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 orincorrect)
- have a high number of transactions that fall just under the threshold for due diligence or reporting to the principal
- report 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 an unusually large cash transaction
- have a size and frequency of transactions that:

- are different from the customer's normal pattern o 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 a large proportion of business with high risk countries
- undertake business outside normal business hours have records in which fake identities repeat common fields, for example a different surname with all the other details like birth day and address the same
- transactions too fast to be possible
- are located geographically in a high-risk area (e.g. in another cash intensive business, or in a border area)
- remit funds overseas in cash through couriers or parcel companies
- former money service businesses re-registering as different cash businesses

- money service businesses not disclosing money service business activity to their bank
- multiple money service business premises operating in very small area
- money service businesses with bank accounts held in higher risk countries rather than the UK

Risk Assessment of our Payments Business

The 5th AMLD require that each MSB must adopt a new 'risk-based approach' to its customers, products and business practices.

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

RISK RANKING	GRADING
Low Risk	L
Medium Risk	M
High Risk	H

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

Products:

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

Product	%of total business	Risk Ranking
Retail payment services	100	H
High value money transfer Services	0	H
Foreign Exchange Plus Onward Transfer	0	H
Payment Account Services	0	H
Credit Card Services	0	H

Pre-paid payment cards, debit cards, direct debit and standing order services	0	H
Foreign Exchange	0	H
Bureau de Exchange	0	H

Transaction:

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

Size of Transaction	% of total business	Risk Ranking
Below £1000	90	L
£1001 to £9999	10	M
Above £10000	0	H

How are they funded?	% of total business	Risk Ranking
Non-cash transactions	0	L
Cash transaction	100	H

Customers:

Retail Customers	%of total business	Risk Ranking
In a business relationship	90	H
Occasional customers	5	M
One off customers	5	M

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

Type of ID Provided	% of Customers	Risk Ranking
EU/UK Passport/driving license (photo card) plus proof of address	90	L
Non EU Passport plus leave to Remain in UK plus proof of address	10	M
Any other form of other ID (‘unusual ID)	0	H

Unusual Activity which may be suspicious

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

Risk Matrix–high, medium and low risk customers

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

Risk Ranking	Summary of red flags	Action of MLRO
H	Sanctions list match	Freeze transaction and report to NCA/HM Treasury
H	Customer previously reported to NCA and NCA withheld consent	Freeze transaction and report to NCA
H	Customer provides fake ID	Freeze transaction pending enhanced due diligence check
H	Customer previously Reported to NCA and consent given	EDD required
H	Transaction being processed Non face to face (and customer not previously identified)	EDD required
H	Single cash transaction above 13,000 EUR(or Local equivalent)where no source of funds established	EDD required
H	Retail customer has sent Cash transactions above13,000 Euros(or local equivalent) within 03 months period (and no source of funds established)	EDD required
H	Customer is a PEP	EDD required
H	Customer uses unusual ID to Identify himself	EDD required
H	Customeris processing level Of transactions incompatible with work status	EDD required
H	Customer is demonstrating Unusual behavior (which may be suspicious)	EDD required
M+ or Less		No Action Required

Our Business Model: Third Party Payment

Our payment process is through third party payments, which is considered as high risk. This is the way how third party payments works,

Sanctions List check

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

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

Asset Freezing Unit

HM Treasury 1 Horse Guards Road London SW1A2HQ

E-mail: assetfreezingunit@hm-treasury.gov.uk Fax: 02072705430

Telephone: 02072705664 or 02072705454

Transaction monitoring

The number and volume of transactions going through the company will be monitored, together with scrutiny of transactions, according to risks parameters relating to

- Customers
- Products
- Delivery channels
- Geographical area of operation.

The MLRO will keep under review all the transactions which are being processed by each customer. This means the MLRO will review on a daily, weekly and monthly basis whether the volume of transactions which is being processed by the customer is consistent with what was anticipated when the customer was registered, keep a watch out for a sudden increase in business from an existing customer, look out for uncharacteristic transactions which are not in keeping with the customer's known level of activity, lookout for peaks of activity at particular locations or at particular times, lookout for unfamiliar or untypical types of customer or transaction, lookout for transactions related to potential sanctions list matches or PEP's.

To assist with transaction monitoring, the company has defined a transaction monitoring protocol

Ongoing monitoring of Transactions

We continue to monitor a business relationship after it is established. We monitor transactions, and where necessary the source of funds, to ensure they are consistent with what we have in our Threshold.

You also keep the information we collect for this

purpose is up to date. It is checked on regular basis and expired documents replaced with copies of newly issued documents.

Occasional transaction

An occasional transaction is a transaction of (or the sterling equivalent) that is not part of an ongoing business relationship. It also applies to a series of transactions totaling €15,000 or more, where there appears to be a link between transactions (linked transactions). (At least 90 days period)

Proof of source of funds

What is it?

Amana Express Ltd considers proof of funds to be a document that demonstrates that a person has the ability and funds available to use for his/her transaction. The document will usually come in the form of a bank statement.

Why is it important?

To ensure that the funds have been legally obtained and the client is the legitimate owner of the funds.

Acceptable proofs will include:

- Wage slip
- Mini statement
- Bank statement less than three months old
- Letter of secured or unsecured loan
- ATM receipt
- Or other acceptable document (i.e. source of funds declaration)

If the customer fails to provide any of these documents, the transaction must be refused.

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 re-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

When we do EDD:

- Enhanced CDD is now required where either of the parties to a transaction or the transaction itself is "established in a high risk third country".
- ✓ Established means in relation to persons incorporated, resident, having principal place of business.
- ✓ The FATF's list of high-risk third countries will be considered and should be regularly checked
- Linked transactions as per our Threshold
- PEP
- Sanction List 'match'

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

Ongoing monitoring of Customers

We must also manually review the customer's pattern of behavior, looking for any signs of suspicious activity such as:

- Is the pattern of transactions consistent and regular?
- Are the size and frequency of recent transactions consistent with the normal activities of the customer?
- Has the pattern of transactions changed since the person first became a customer?
- Are there sudden increases in the frequency or value of a customer's transactions without reasonable explanation?
- Is there a significant and unexpected improvement in the customer's financial position, which the customer is unable to explain satisfactorily?
- Does a third party make repayments on behalf of the customer without a satisfactory explanation?
- Are there frequent address changes?

Ongoing Monitoring of ID Documents

Documentary evidence of an individual's identity issued by a government department or agency, when verifying identity-using documents (as opposed to electronic checks), the documents should be:

Either a government-issued document, which incorporates the customer's full name and photograph, and either his or her residential address or date of birth, such as:

Valid passport
Valid driving license (full or provisional)

National ID card (for EU nationals)
Firearms certificate or shotgun license

This must be supported by secondary evidence of ID, which incorporates the customer's full name and residential address and Date, such as:

Current council tax letter or statement
Current bank or credit/debit card statements
Utility bills

These other documents are intended to confirm a customer's address, so they should have been delivered to the customer through the post, rather than being accessed by him from the internet.

Whichever documents are used, we must check them carefully. For example, checks on photo ID may include:

- Does the date of birth on the evidence match the apparent age of the customer in the photo?
- Is the ID valid?
- Is the spelling of names the same as other documents provided by the customer?

Checks on secondary evidence of ID may include:

- Do the addresses match the address given on the photo ID?
- Does the name of the customer match the name on the photo ID?

- We must also consider whether the documents may be forged. In all cases where customers are unable to provide the standard evidence, we must establish and document the reasons for this.
- Some categories of financially excluded customers may represent a higher risk of money
- Laundering, so we should consider enhanced monitoring of these customers' transactions.

For Transaction screening:

- Sender basic information with an identification document
- Adverse Media check
- PEP / Sanction check over sender and receiver

- Independent Electronic check (Credit Safe)
- Beneficiary Link Report to examine the sender/Receiver's Transaction behavior.

Record Keeping

- An account file must be set up for each customer with whom we have a business relationship, and for each large occasional transaction.
- Copies of ID and verification must be kept on file and details of all transactions with that customer recorded.
- All information used to set up a business relationship must be recorded and kept on the file.
- Details of any suspicious activity, report to Nominated Officer and disclosures to NCA must be kept on file.

- Evidence of customer's identity record must be kept for five years beginning on the date on which the occasional transaction is completed or the business relationship ends.
- Records of the transaction (whether undertaken as occasional transactions or part of a business relationship) must be kept for five years beginning on the date on which the transaction is completed.
- All other records must be kept for five years beginning on the date on which the business relationship ends.

Extent of Customer due Diligence Measures

The extent of customer due diligence measures depends on the degree of risk. It depends on the type of customer, business relationship, product or transaction.

It goes beyond simply carrying out identity checks, this is because even people we already know well may become involved in illegal activity at some time, for example if their personal circumstances change or they face some new financial pressure. Our due diligence measures should reduce the risk of this, and the opportunities for staff to be corrupted.

We consider the level of identification, verification and ongoing monitoring that is necessary, depending on the risk you assessed.

Risk Assessment

Our risk assessment is how we identify the risks our business is exposed to. We must be able to understand all the ways that our business could be exposed to money laundering and terrorism financing risks, operational and security risks and design systems to deal with them.

Our Business Risk Assessment includes:

- Identification and monitoring the risks of money laundering and terrorist financing that are relevant to our business
- Note of information on risk and emerging trends from sources including the National Risk Assessment and HMRCs risk assessment.
- Assessment and kept under regular review, the risks including those posed by our:
  - **Customers and any underlying beneficial owners** – detailed assessment is made by analyzing risk indicators as stated above, customer's behavior and also accepting abroad customers, we make use of

    Transparency International corruption perception index
  - **Services –** Money remittance our main business services is at high risk of AML but our mitigation measures make it moderate.
  - **Delivery channels, for example cash over the counter, wire transfer, online or agents** – use of agents and cash-based remittance is at high risk but our regular monitoring and due diligence process on the basis of risk assessment makes it lower.

- **Geographical areas of operation**, including sending money to, from or through high risk third countries, for example countries identified by the EU or Financial Action Task Force (FATF) as having deficient systems to prevent money laundering or terrorist financing.- we use **https://www.knowyourcountry.com/country-ratings-table** and **http://www.fatf-gafi.org/publications/high-risk-and-other-monitored- jurisdictions/documents/increased-monitoring-june-2020.html** for regular updates and assess jurisdiction risk and due diligence measures to mitigate the same accordingly.

  For details, please see ANNEXURE 1 – Business Risk Assessment

  Operational and Security Risks

  Operational or security incident – as defined in Directive (EU) 2015/2366 - A singular event or a series of linked events unplanned by the PSP which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.

  Security risk - The risk resulting from inadequate or failed internal processes or external events that have or may have an adverse impact on the availability, integrity, confidentiality of information and communication technology (ICT) systems and/or information used for the provision of payment services. This includes risk from cyber- attacks or inadequate physical security.

  For details, please see ANNEXURE 2 & 3 - Operational and security risk Analysis & Controls.

  Testing of security measures

  Testing of security measures is indispensable part of our assessment to ensure effectiveness of our security measures. The testing includes:

- We establish and implement a testing framework that validates the robustness and effectiveness of the security measures and ensure that the testing framework is adapted to consider new threats and vulnerabilities, identified through risk- monitoring activities.

- The testing framework encompass the security measures relevant to

  Payment terminals and devices used for the provision of payment services

  payment terminals and devices used for authenticating the User and

  devices and software to generate/receive an authentication code

- Tests are carried out by independent testers who have sufficient knowledge, skills and expertise in testing security measures of payment services and are not involved in the development of the security measures for the corresponding payment services or systems that are to be tested, at least for final tests before putting security measures into operation.

- Tests include vulnerability scans and penetration tests adequate to the level of risk identified with the payment services.

- We perform on-going and repeated tests of the security measures for their payment services. For systems that are critical for the provision of their payment services, is performed annually. Non-critical systems are also tested regularly on a risk-based approach, but once in two years.

Situational Awareness, Training and Continuous Learning

5th AML Directive requires each money services business to provide Situational awareness and continuous education and/or training of appropriate personnel concerning their responsibilities under the Amana Express Ltd Compliance Program. Training and awareness must include helping employees to recognize security issues and reporting any fraud issues or customer complaint to management and to detect potentially suspicious transaction activity and it's reporting.

The Compliance Officer is responsible for ensuring that each employee receives training appropriate to their role and responsibility within the business. Employee training is documented in order to maintain affirmative, documented proof that the training have indeed taken place, time and dated. The training program of the Company consists of the following components:

1. Periodic updates covering the status of the AML Compliance Program and any changes or clarification to The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, Proceeds of Crime Act 2002, Terrorism Acts (several), MLR 9 HMRC and the Payment Services Regulation 2017;
2. Firm conducts and implement periodic security awareness programmes in order to educate their staff and to address information security related risks which includes identification and constant monitoring security and operationalthreats that could materially affect their ability to provide payment services. These programmes focus on staff to report any unusual activity and incidents.
3. Compliance Officer is trained to perform appropriately;
4. Training provided to new employees of the Amana Express Ltd takes place shortly after hire as appropriate to their roles and responsibilities and its ensured that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures in order to reduce human error, theft, fraud, misuse or loss;
5. Training provided to all employees annually; currently consultancy agreement provides for such training to take place at a date to be determined by Amana Express Ltd and,
6. Additional job specific training for staff covering topics such as internal reports, recognizing, and reporting suspicious activity.
7. Training records are available for audit purposes, it is been updated.

Payment service user relationship management

Payment service user awareness on security risks is also important to create the awareness among user and create healthy environment for the user to avail our service and perform transactions safely and securely.

- Our framework of contract clearly defines, establish and implement processes to enhance PSUs' awareness of security risks linked to the payment services by providing PSUs with assistance and guidance.
- We provide assistance and guidance to our users in the light of new threats and vulnerabilities, and communicate changes thereto.

- We provide the user with the option to adjust these limits up to the maximum agreed limit.

- We provide user with option to receive alerts on initiated and/or failedattempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their account.
- Users are regularly informed about updates in security procedures, which may affect them regarding the provision of payment services.
- We aim to provide timely assistance on their queries, requests for support and notifications or issues regarding security matters related to payment services by reaching us at office desk, or mail us or contact us at their convenience.

IMPACT of COVID-19 on Our Business.

As our source of income is remittance and we deal with customers, it is therefore crucial for us to reach out to our customers. Pandemic poses a greater threat to countries that rely heavily on remittance income.

- COVID - 19 has had an impact on our business as we had to close down our Premises for more than a month.
- There was a decrease in net income because of Corona Virus whereas we as a business had to use post lockdown strategy such as TV and Radio advertisements.
- During lockdown, we did not give employees remote access via home facilities as our business mainly operates with face-to-face customers.
- We furlough 4 permanent employees for one month in Covid-19 lockdown.

Precautions for Covid-19 in our Premises

It is very important to remember that continued precautions against COVID-19 are necessary at all workplaces since the pandemic is nowhere close to being over yet. The following are the key areas of COVID-19 prevention we ensure are:

- We are running our office with 2 staffs only to maintain social distancing.
- We have reduced our working hours and services.
- **Facemasks:** All Employees and Customers should be allowed entry only if they are properly wearing face covers or masks.
- **Social distancing all the time**: A minimum distance of six feet is always maintained at all times within in staffs and between our staffs and the customers.
- **Closure:** Only two Customers are allowed to enter and we performed 2 meters distance regime in our premises at a time.

Conclusion of Risk Analysis

As a result of this Risk Assessment, the Amana Express Ltd overall risk is considered to be **Medium** for potential money laundering activities, potential terrorist financing activities and Sanction.

There is an effective Compliance and security Program to reasonably address the identified risk levels considering Amana Express Ltd client base (mostly Socially and/or Financially excluded clients, its business model, target market and resources allocated to implement and monitor suitable Systems and Control mechanisms) Amana Express Ltd Compliance and Security Program has been developed to meet the risks evaluated in this analysis. The Company will continue working towards identifying, managing and mitigating risk appropriately.

The Company is demonstrating ongoing commitment to its Program and is continuing to manage compliance and security in a manner appropriate to the risks identified herein.

The Company is continuing in its efforts with appropriate oversight and support of the Management and Shareholders.

A new risk assessment will be performed in 12 months or as soon as it is practically necessary should business circumstances change.

Annexure 1

Business Risk Assessment

FACTOR	LOW – 1	MEDIUM - 2	HIGH - 3	OUR RISK
1	Business formed or acquired over 1 year ago; experienced management.	Business formed or acquired within 1 year ago; experienced management.	Business recently formed or acquired by new management.	Low
2	Business has provided one or more financial services for a lengthy period; experienced management.	Business has provided financial services for over 1 year.	Business has only recently begun to provide financial products and services.	Low
3	Business carried out through its own premises	Part of the operations are outsourced through other MSBs or third parties	Entire business is operated through other MSBs or third parties	Low
4	Business serves retail customers only	Business has a combined source of business from wholesale and retail	Business serves wholesale customers (i.e. Financial Service Institutions) only	Low
5	All MSB services are provided directly by the business; there is no agent agreement with a registered MSB.	Some MSB services are provided under an agent agreement with a registered MSB providing significant compliance training, tools, technology and oversight.	All MSB services are provided under an agent agreementwith a registered MSB providing significant compliance training, tools, technology and oversight.	Low
6	The business currently deals 100% of its customers face to face.	The business currently deals 50% of its customers face to face.	The business currently deals more than 50% of its customers non-face to face.	Low
7	Highly effective, well trained staff; low employee turnover.	Trained staff; moderate turnover.	Frequent employee turnover and poor/inconsistent training.	Low

8	Effective automation assists in managing customer relationships, conducting transactions, identifying reportable activity, filing regulatory reports and in complying with the law.	Some automation is available to support AML compliance efforts.	No automation supports the AML compliance efforts or transaction processing. The audit trail of transactions is limited and/or difficult to construct.	Low

Business Size, Location and Market Risk Factors

FACTOR	LOW - 1	MEDIUM - 2	HIGH - 3	OUR RISK
9	The business operates from 1-2 locations in which money services are provided. Having no agents.	The business operates in 2 to 5 locations in which money services are provided. Having few agents.	The business operates in more than 5 locations in which money services are provided. Having large numbers of agents.	High
10	Premises have easy access to information and communication through servers / internal communication mechanisms	Branches have limited connectivity of IT systems and communications	Servers are not linked and communications and access to information from one branch to another is slow	Low
11	The business is located low crime area for business robbery as per London metropolitan police	The business is located medium crime area for business robbery as per London metropolitan police	The business is located high crime area for business robbery as per London metropolitan police	Low
12	Most of the customers are regular from the local area market who purchase goods/services; local, stable, generally well-known customer base.	Local area customers along with transient customers passing through the area; little repeat business based on longstanding relationships.	Persons primarily from outside the immediate area who are visiting temporarily or are passing through to another destination; little or no relationship based repeat business.	Low
13	Customers are mainly UK residents providing UK and foreign passports or driving licenses as ID.	Some international customers providing forms of identification not issued in UK.	Many international customers frequently providing forms of identification not in UK	Low
14	Moneys are received through bank transfers and Debit/Credit Cards	Moneys are received in cash and through a combination of bank transfers/cards	The business only operates a cash only service	High
15	Moneys are paid out in bank accounts	Moneys are paid out in cash and through a combination of bank transfers/cards	The business only operates a cash only service	Low

Quantity of PEPs and Sanction List Risk Indicator

FACTOR	LOW – 1	MEDIUM - 2	HIGH - 3	OUR RISK
16	Stable, well-known customer base in a localized environment serving low-risk customers including beneficiary's jurisdiction.	A large, fluctuating client base frequently serving medium-risk customers including resident and non-resident aliens and foreign customers including beneficiary's jurisdiction.	A large, fluctuating client base frequently serving high-risk customers including resident and non-resident aliens and foreign customers including beneficiary's jurisdiction.	Low
17	No history of PEPs and Sanction List actions. No evidence of apparent violation or circumstances that might lead to a violation.	Actions taken other money service business.	Actions taken by law enforcement/regulatory agencies, including notice letters, or civil money penalties.	Low

Quality of AML Management

FACTOR	LOW - 1	MEDIUM - 2	HIGH - 3	OUR RISK
18	Management fully understands the risk and exhibits a strong commitment to compliance.	Management reasonably understands the key aspects of compliance and its commitment is generally clear and satisfactorily communicated.	Management does not understand or has chosen to ignore, key aspects of compliance risk. The importance of compliance is not emphasized or communicated throughout the organization.	Low

19	Compliance considerations are incorporated into all products and areas of the organization.	Compliance considerations were overlooked or weak in one or two areas, but management promised corrective action when it was identified.	Compliance considerationsare not incorporated into numerous areas of the organization.	Low
20	When deficiencies are identified, management promptly implements meaningful corrective action.	Problems can be corrected in the normal course of business without significant investmentof money or management attention. Management is responsive when deficiencies are identified.	Errors and weaknesses are not self-identified. Management may only respond when violations are cited.	Low
21	Authority and accountability for compliance are clearly defined and enforced, including the designation of a qualified AML Officer.	Authority and accountability are defined, but some refinements are needed. A qualified AML Officer has been designated.	Authority and accountability for compliance has not been clearly established. No or unqualified AML Officer may have been appointed. Roleof the AML Officer is unclear.	Low
22	The Board has approved an AML compliance program that includes policies, procedures, controls and information systems that are adequate.	The Board has approved an AML compliance program that addresses most policies, procedures, controls and information systems but some weaknesses are noted.	The Board may not have approved an AML compliance program. Policies, procedures, controls and information systems are significantly deficient. For example, there are substantial failures to file currency transaction reports and/or suspicious activity reports.	Low
23	Training is appropriate, effective, covers applicable personnel, and necessary resources have been provided	Training is conducted and management provides adequate resources given the risk profile of the organization; however, some areas are not	Training is not consistent and does not cover important regulatory and risk areas.	Low

	to ensure compliance.	covered within the training program.		

24	Effective customer identification processes and trusted relationship / membership opening procedures are in place.	Customer identification process and trusted relationship / membership opening procedures are generally in place, but not well applied to all high-risk areas.	Customer identification process and trusted relationship / membership opening procedures are absent or ineffective.	Low
25	Compliance systems and controls quickly adapt to changes in various lists (for example Bank of England, Home Office, and Other Government Provided Lists.)	Compliance systems and controls are generally adequate and adapt to changes in various government lists	Compliance systems and controls are inadequate to comply with and adapt to changes in various government lists.	Low

Conclusion of AML Risk Analysis

It is reasonable to conclude that a business's risk could be categorized according to the total points scored using this model, as follows:

Low Risk: 1 point per factor – range 1-25 Medium Risk: 2 points per factor – range 26 -50 High Risk: 3 points per factor – range 51-75

Risk Level	Factor	Risk value per factor	Total Risk Score
Low Risk	23	1	23
Medium Risk	0	2	0
High Risk	2	3	6
Total	**25**		**29**

The total number of points calculated for the review of the business through this review process is **29**. Thus, our risk is considered as **Medium** for potential money laundering activities, potential terrorist financing activities and Sanction.

Based on risk assessment, we are doing following in relation to transactions or business relationships with a high-risk jurisdictions or customers:

- Enhanced due diligence
- Enhanced ongoing monitoring
- Systematic reporting
- Limiting or ceasing business

Annexure 2

Operational and security risk Analysis & Controls.

S. No	Operational and Security, Regulatory compliance and mitigation of risks	Yes/ No/ N.A
1	The firm has documented AML policies and procedures, which are regularly updated and communicated to all personnel?	YES
2	Firm has documented a list of business functions, supporting processes and information assets supporting payment services provided and classified by their criticality.	YES
3	The firm has robust client acceptance procedures (accelerated to MLRO where appropriate for high risk clients)?	YES
4	Robust client re-acceptance procedures (or ongoing checks on higher risk clients), involving MLRO?	YES
5	Procedures and policies are applied equally by all aspects of the firm?	YES
6	The firm has implemented an appropriate approach to Customer Due Diligence records that is evident on all client files?	YES
7	Enhanced due diligence procedures are applied where appropriate?	YES
8	The firm has an appropriate SARs reporting procedure?	YES
9	The firm has a robust firm-wide risk assessment, with key risks communicated to staff and mitigations in place?	YES
10	The firm carries out an effective annual compliance review, which covers the full business, and also higher risk areas. This includes an action plan and follow up of remedial action, where appropriate?	YES
11	Staff and principals have undertaken appropriate up to date training in AML, including key requirements and how to identify money laundering. Records maintained of training and staff declarations signed?	YES
12	More frequent training for staff in higher risk areas?	YES
13	Screening of staff, including regular screening in higher risk areas?	YES
14	Robust Clients Money procedures, in compliance with the Clients Money Regulations.	YES
15	MLRO keeping up to date on key requirements and emerging risks.	YES
16	Where reports are made to the National Crime Agency these are made in a complete & timely	YES

	manner.	
17	There are no inordinate delays in reporting to the NCA following initial report from staff members. Please report how many SARs reported to the NCA during the year in NOTES.	YES (Zero till now)
18	Additional safeguards, including additional engagement review procedures (e.g. second partner review/external review), for higher risk clients.	YES, MLRO and Director Check

Annexure 3

Risk Analysis					Further Actions(s)	
Ref	Type of Risk	Risk Description	Impact	Existing Controls	Future improvement	Responsible Person
1	Physical Security Risk	Fire damages property/people or terror attack	Fire & Health and Safety Act breach, financial and data loss	To project our premises we have security doors, no one can enter in to the company without verification. Fire and Health and Safety training given to our branch's regularly. Fire emergency signs, first aid available, alarms tested regularly and in the event of terror attack staff must need to call police and related organisation for	Upgrading Fire alarms, camera, insurance policy and cautiously checking latest development to implement in the company. Company will keep update all the emergencies contact number.	MLRO & MD
2	System Security Risk (IT and Data)	Firms must ensure Data Access is granted on a secure environment, satisfying PSD2 requirement and going forward GDPR	Financial Loss, Reputational damage/, Customer Complaints, Data Breach, or fine	The business has implemented PSD2 standards whilst also planning for GDPR.	External testing, reviews and audit are being used to further add MI to Management; this is an ongoing and regular process. Comprehensive IT Security arrangements, with defined access rights, and monitoring arrangements whichare tested internally in an ongoing basis	MLRO & MD

	System Security Risk (IT and Data)	IT system halt or crash down	Disruption of Daily activities/ Business	The online software is also backed up with a secondary back up. In the event of a system halt or crash down, the secondary backup ofthe system kicks in and operation of the system resumes back to normal.	It is very rare that a system crash will occur, Proper procedures are in place to deal withthe issue if it occurs and can keep a closer eye if it happens and improve accordingly	MLRO & M
	System Security Risk (IT and Data)	security also protects data from corruption. Data security is an essential aspect of IT for organizations of every size and type. Data security is also known as information security (IS) or computer security.	Loss of Data	The online application is hosted under secured Socket Layer Protocol (SSL Certification) - web hosting with virus scanner. Server and client communication is done via encrypted data link using SSL Certificate. Sensitive data is encrypted before it's stored in the system. User must be authenticated by providing login details.	System is closely monitored for any external threats; firewalls anti hacking tools will be in place.	MLRO & M
	System Security Risk (IT and Data)	Poor record keeping practices, failure to maintain backups, failure to secure data	Loss of regulatory records, e.g. due diligence documentation	Access controls in place, data archived and backed up electronically	Regular monitoring of IT Control	MLRO & M
	System Security Risk (IT and Data)	Loss of Company records	Loss of financial records. Possible implications for tax audit	Access controls in place, data archived and backed up electronically	Regular monitoring of IT Control	MLRO & M

	System Security Risk (IT and Data)	Host System	If there is a problem between the two companies, or the unlikely event of Intra Data going into administration, the main system will cease to operate.	If there are contract problems with System, or in the unlikely event of software/server provider going into administration, we contact our solicitors in order to release the escrow server, which has the customer transactions and database	Regular monitoring of IT Control	MLRO & M
	Operation al Risk	Operational risk is "the risk of a change in value caused by the fact that actual losses, incurredfor inadequate or failed internal processes, people and systems, or from external events, differ from the expected losses"	Financial Loss / Reputational damage/ Service Delivery/Mista kes and Fraud	Extensive training has been given to all staff, in the context of their duties and company obligations; staff have been given job descriptions and are regularly monitored. External references and checks are in place to check criminal convictions and previous employment	Compliance Monitoring program and external testing are carried out to determine performance of operational processes; employees are subject to ongoing performance reviews to ensure they are adhering to processes	MLRO & M
	Operation al Risk	Telephony Centre/ca ll Centre	If an issue arises that could compromise the telephony system, our customers would not be able to contact us.	The company provides access to mobiles to the employees and redirect the calls to the main number to the mobiles. This can be done within 1 hour.	We would have a secondary telephony system in place on another location ready to take place if we lose connectivity to the internet.	MLRO & M
0	Operation al Risk	Staff	When staff leaves the company, their logins could be left active	There is a procedure for staff leaving the company and fully integrated with IT.	There is formal procedure and we have few employees and managing them successfully.	MLRO & M

1	Operation al Risk	Poor handling of complaints, inability to resolve issues	Ombudsman proceedings against the company, Fines and penalties for non-compliance	Robust complaints policy, staff trained in procedure, management oversight and reporting	Senior management aim is to provide the best services and continuous train staff how to handle customers complaints.	MLRO & M
2	Operation al Risk	Representatives of third parties steal money from the company	Fraud and losses to company, Fines and penalties for non-compliance	Fraud prevention measures in place, IT systems audited for security, due diligence conducted on all clients	Internaland external audit	MLRO & M
3	Business Continuit y and Recovery	Beneficiaries, it is always possible that they may refuse to pay remittances or may be affected by insolvency or other events that may affect contractual fulfilment and deliveryof remittances Arrangements must exist to ensure business is not disrupted by way of external factors that may stop services to clients. Businesses must ensure that their ability to maintain its ability to recover from downtime/	Data Breach, Financial Loss and reputational damage	Business continuity and disaster recovery arrangements are in place to ensure down times and possible effects can be mitigated. Cloud based and external servers being backed up and supported are the key elements of the plans. Furthermore, contingency locations and remote working arrangements are also part of reducing the impact of possible issues affecting operations	Arrangements have been tested to ensure performance andability to operate in "worst case scenario" situations. Minor adjustments are being made to ensure performance remains appropriate to the needs to the business to support services delivery to clients	MLRO & M

		external factors also permits work to be carried out by staff				
4	Operation al Security Risk	Disgruntled Employees	Internal attacks are one of the biggest threats facing your data and systems, especially members of the IT team with knowledge of and access to networks, data Centre's and admin accounts, can cause serious damage	The first step in mitigating the risk of privileged account exploitation is to identify all privilegedaccounts and credentials [and] immediately terminate those that are no longer in use or are connected to employees that are no longer at the company	companies would implement necessary protocols and infrastructure to track, log and record privileged account activity [and create alerts, to] allow for a quick response to malicious activity and mitigate potential damage early in the attack cycle.	MLRO & M

5	Operation al Security Risk	Careless or Uninformed Employees	employees who are not trained in security best practices and have weak passwords, visit unauthorized websites and/ or click on links in suspicio us emails or open email attachments pose an enormous security threat to their employers' systemsand data.	Train employees on cyber security best practices and offer ongoing support, hold training sessions to help employees learn how to manage passwords and avoid hacking through criminal activity like phishing and keylogger scams. Then provide ongoing support to make sure employees have the resources they need	make sure employees use strong passwords on all devices, Passwords are the first line of defence, so make sure employees use passwords that have upper and lowercase letters, numbers and symbols, To be extra safe, "implement multifactor authentication such as One Time Password, RFID, smart card, fingerprint reader or retina scanning [to help ensure] that users are in fact who you believe they are.	MLRO & M
6	IT	Anti-Virus	Loss of data, non- compliance and financial loss.	All computer equipment identified by the scope of the policy shall have anti-virussoftware installed and operational.On first installation of the anti- virus software a full virus scan of all attached storage devices (hard disks) must be completed. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.	Continuous monitoring that Users ensure that anti-virus software is installed and operating on all workstations, personal computers or laptops they have been personally allocated. Administrators shall be responsible for ensuring that anti-virus software is installed	MLRO & M

					and operating on servers or shared computer equipment.	
7	IT	Encryption Policy (Encryption is the process of disguising data to hide its substance from any casual observer gaining access to it. This is done by applying a mathematical function, known as a cryptographic algorithm or cipher, to the data to render it unreadable. A mathematical function that reverses the encryption process is used to decrypt	Unauthorised and leak of sensitive information	Only tools and products based on proven, mathematically sound cryptographic algorithms, subjected to peer review by the cryptographic community, shall be used for encryption. For block ciphers, a minimum symmetric key length of 128 bits should be used. For long term security a symmetric key length of 256 bits is recommended. For public key ciphers, a minimum asymmetric key length of 2048 bits should be used. For long term security an asymmetric key length of 4096 bits is recommended. All keys shall be stored safely. Where a key is secured by use of a pass phrase, the pass phrase shall be at least 12 characters in length. The requirements and recommendations for password selection and password protection described in the Password Policy shall apply for pass phrases.	Some products contain patented algorithms or methods, which may require the purchase of a suitable licence. Company will continuous monitor the effectives and validity of products.	MLRO & M

		the data. One or more unique keys is used in conjunction with the cipher to perform the encryption or decryption.)				
8	IT	Network Monitoring Policy (To establish the requirements for monitoring, logging and retention of traffic on the Company network.)	Unauthorised access to data, viruses, loss of sensitive information and other security of data and system	IT Administrators may intercept network traffic without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime, gross misconduct or unauthorised use, and ensuring the efficient operation of Company communications systems. The primary aims of network monitoring are: • To maintain the integrity and security of the Company network, IT equipment and information assets. • To collect information to be used in network design, engineering,	During the risk assessment and effectiveness of the existing control there is no deficiency. Company will continuously monitor the existing control for further improvement.	MLRO & M

				troubleshooting and usage-based accounting.		