2020-21

Anti-Money Laundering (AML) & Combating the Financing of Terrorism (CFT) Policy document

Union Bank of India (UK) Ltd

TREATING CUSTOMERS FAIRLY POLICY

DOCUMENT MANAGEMENT

Document ID / Version	V2.0
Owner	MLRO
Initial Creation Date	21/08/2014
Last Reviewed	25/07/2020
Next Review Date	1 year from the date of approval
Status	Current version approved by RCC on 28.07.2020, and placed for Board approval (Board meeting - 20.08.2020)

VERSION CONTROL

Date	Version	Author	Description
April 2015 (Updated Nov 2015)	1.2	Compliance Department	Third Release of AML-CFT Policy
May 2016	1.3	Compliance Department	GT Amendments
Nov 2017	1.4	Compliance Department	• Amendments to policy to incorporate changes in regulation – The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 • Clause 4.3.4 – Immigration Checks on new accounts Amended • Clause 4.3.5 Business wide risk assessment, Geography included in the risk factors • Clause 4.4.1 Simplified Due diligence amended • Clause 4.4.2 – Inclusion of domestic PEP • Clause 4.5: Treatment of Staff Accounts • Clause 4.6: Ultimate Beneficial Owners defined

			• Clause of 8.1: Review of accounts • Appendix 2 – Change Suspicious Activity form • Appendix 3 – Country Risk Classification
April 2019	1.5	Compliance Department	• General formatting and amendments • Board Statement Amended • Sec 4.1 FATF High Risk Jurisdictions • Sec 11: Inclusion of AML Risk Mitigation Programme • Sec 12: Inclusion of Enhanced Due Diligence (EDD) for high risk customers • Sec 13 Record keeping period from Six to Seven years • Annexure 3 – Country Risk Classification – updated • Annexure 4 Abbreviations
July 2020	2	Compliance Department	• General Amendments including Reformatting to align with the policies suite of the Bank • Sec 4.1 FATF High Risk Jurisdictions • Sec 11 5th Anti-Money Laundering Directive • Sec 12 6th Anti-Money Laundering Directive • Annexure 3 – Country Risk Classification – updated

1 CONTENTS

2 INTRODUCTION

Board Statement:

In the present day's globalised business environment, money laundering and the inherent risks that flow from it affect the banking industry greatly. Union Bank of India (UK) Ltd (the Bank) recognizes that Anti-Money laundering (AML) and combating financing of terrorism (CFT) are an essential pre-requisite for ethical banking and good governance.

The board of Union bank of India UK fully appreciates the potential reputational damage, whether intentional or unintentional that would cause to the bank and therefore will not tolerate any involvement in money laundering activity.

In keeping with UK regulations, Union Bank of India UK Ltd maintains appropriate customer screening, monitoring and related due diligence procedures that are designed to prevent the bank from doing business with entities which engage in money laundering practices or illegal activity. In relation to incorporated entities, these processes extend to the individuals that control such corporations.

It is the policy of Union Bank of India UK Ltd that statutory and regulatory obligations are to be met in full and the UK criminal laws are not violated.

The nature of services provided by banks is such that, they are exposed to being used for money laundering and terrorist financing, which may render them liable for criminal prosecution, regulatory censure or civil proceedings. The Bank aims to prevent its services being used for such activities, while offering ethical banking services.

The object of this policy is to minimize the risk of the Bank's services being abused for the purposes of money laundering and/or terrorist financing, by positive management action involving all employees, officers and directors, to comply with all regulatory requirements in this regard. It is the Bank's policy to remain compliant with all statutory and regulatory requirements relating to AML and CFT.

This policy is applicable to all employees of the Bank as appropriate to their role and position. Officers and relevant staff members of the Bank are made aware of policies, procedures and processes which are mandated to be adhered by them. Written records documenting compliance with such policies , procedure and processes are maintained.

3 BACKGROUND

3.1 AML Regulatory Framework in the UK

The Anti-Money laundering regime in the UK is governed by legislation, regulations, rules and guidance notes as below:

i. **Primary legislation:** The act / law that defines the criminal offence of Money laundering, the offence of failure to make a report of the knowledge or suspicion of the offence, the offence of tipping –off and /or prejudicing an investigation is the *Proceeds of crime act 2002 (POCA)(as amended).*

ii. **Secondary legislation:** These are a set of codes, regulations or orders, which are expected to be adhered to by all financial services businesses including banks to prevent / reduce money laundering, and this legislation is referred to as *The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.* MLR 2017 also incorporates the international regulatory standards prescribed by the *Financial Action Task Force (FATF) and the European Union (EU) directives including MLD 4 and MLD5.* The standards for customer due diligence, record keeping, procedures, training of staff on AML, reporting procedures and exceptions are described in detail in the MLR.

iii. **Tertiary level industry guidance:** Anti-Money laundering guidance notes are issued in the UK by the regulators or trade associations. These guidance notes are to communicate and educate the financial service businesses about how the regulators expect the financial service businesses to comply with the detailed requirements of the primary and secondary legislation. For the financial sector the guidance notes are issued by the *Joint Money Laundering Steering Group* (JMLSG) and the *FCA rule as contained in the Systems and Controls sourcebook (SYSC 3 & 6)*.

The content of the manual has also been benchmarked against the industry guidance published by the Wolfsberg Group and with reference to the Wolfsberg Anti-Money Laundering Questionnaire to check for completeness.if you may mention also as updated in the year 17/18 pl. check.

iv. In addition, key elements of UK's AML / CFT framework includes:

- Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001);
- Counter-terrorism Act 2008, Schedule 7
- HM Treasury Sanctions Notices and News Releases; and
- FCA Handbook and FCA Financial Crime Guides.

3.2 Combating Financing of Terrorism in the UK

The legislation to combat terrorism in the UK is governed by the Terrorism Act 2000 and as later amended by the Anti-terrorism, Crime and Security Act 2001. As per the above acts, a suspicious transaction should include inter alia transactions which give rise to reasonable grounds for suspicion that they may involve financing of activities relating to terrorism. The Bank will ensure enhanced monitoring of accounts suspected of having terrorist links and if found suspicious must report to the National Crime Agency (NCA). Other legislation for CFT which the Bank needs to comply is the Counter-Terrorism Act (CTA) 2008. The Bank will comply with directions issued by HM Treasury under the terms of Schedule 7, of the

CTA Act to conduct enhance due diligence (EDD) and on-going monitoring, systematically report on or limit or cease business with parties that it, reasonably believes, to be involved in money laundering, terrorist financing or facilitating the development or production of nuclear, radiological, biological or chemical weapons that poses a significant risk to the national interest of the UK.

Appendix 1 to this policy contains the details of the web links/ addresses of the above said acts and institutions.

4 MONEY LAUNDERING AND TERRORIST FINANCING

4.1 MONEY LAUNDERING

Money laundering in simple terms is the process of turning dirty money into clean money. However, the definition of Money Laundering will include not only money, it could be any form of property or relationship and hence a more proper definition would be "A transaction or a relationship that involves any form of property that has been derived from or associated with crime". Common examples of money laundering are property derived from bribes, robbery, deceit or money gained by drug trafficking, narcotics trade, illegitimate arms trade and money earned by other malpractices.

The activity of sanitising such money to appear as legitimate money is money laundering. An employee will be committing an offence of money laundering by failing to report knowledge or suspicion of Money Laundering or the offence of tipping off by informing the customer or the money launderers of the investigation or intended investigation, which may prejudice the investigation. As per provisions of law, money laundering is defined as below:

a) *The substantive offences of money laundering*

As per POCA 2002 Sections 327, 328 and 329 define the substantive money-laundering offences, which apply to all, as follows:

i. S.327 – concealing, disguising, converting, transferring or removing criminal property;

ii. S.328 – entering into or becoming concerned with an arrangement which one knows or suspects facilitates the acquisition, retention, use or control of criminal property;

iii. S.329 – acquisition, use and having possession of criminal property.

b) *Failing to report*

As per POCA sections 330, 331 and 332 "A person (employed in the regulated sector) commits an offence if each of the following three conditions is satisfied:

i. they know or suspect, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering.

ii. information or other considerations on which the knowledge or suspicion is based came to him in the course of a business in the regulated sector.

iii. they do not make the required disclosure as soon as they are able after the information or other considerations comes to their attention.

c) *Tipping off and prejudicing an investigation*

Section 333A creates an offence covering the regulated sector (as defined in Schedule 9) of disclosing to the customer concerned or to other third persons the fact that information about known or suspected money laundering has been disclosed (s.333A(1)) or that a money laundering investigation is being, or may be,
carried out (s.333A(3)); it must be proved that the disclosure was likely to be prejudicial.

d) *Money is generally laundered for the purposes as detailed below but not limited to them*

i. To disguise the fact that the money has come from crime.

ii. To put a safe distance between the actual criminal or launderer and the investigating agencies.

iii. To have effective control over the money.

iv. For benefits from the proceeds of crime.

e) *Money is traditionally laundered by a three stage process*

i. Placement: This involves placing the cash generated from crime in a disguised form. This is the point when the proceeds of crime are most apparent and risk detection is easiest. Common forms are depositing a small amount of money into many bank accounts to avoid detection, investing in insurance policies or term deposits or bonds, intermingling with the trade proceeds or business proceeds to avoid detection and asset purchase.

ii. Layering: This is process of putting a safe distance between the perpetrator of the crime, by moving it to other countries to keep it away from the local law or by placing it in a trust run by someone else to avoid detection. Layering obscures the origins of criminal money through complex transactions, often involving different entities like companies and trusts and can take place in multiple jurisdictions. Banks may be targeted at this stage and detection can be difficult.

iii. Integration: Once the origin of the funds has been obscured, the criminal proceeds reappear as from a legitimate source, the money is brought back closer to the launderer or perpetrator of the crime by way of a maze of transactions. They will invest funds in legitimate businesses or other forms of investment, often using banking services to invest, set up a trust or acquire a company, among other activities. This is the most difficult stage of money laundering to detect.

4.2 TERRORIST FINANCING

Terrorist financing is the use of the services of financial institutions to maintain and move money from one location or one account to another for the purpose of committing and abetting terrorist activities. Terrorist financing differs from Money Laundering in certain ways, here the source of money being used may be lawful, but it is the destination of the funds that banks have to be careful about. The funds for terrorist activities need to be disguised, nevertheless an attempt to disguise the intended terrorist financing is a criminal act.

The Counter terrorism Act 2008 (schedule 7, part 1) defines terrorist financing as below:

"Terrorist financing" means—

a) the use of funds, or the making available of funds, for the purposes of terrorism, or

b) the acquisition, possession, concealment, conversion or transfer of funds that are (directly or indirectly) to be used or made available for those purposes.

If in the course of business , if a staff suspects, or have reasonable grounds to do so, that any activity or a specific transaction is related to criminal conduct or terrorist financing, the staff must promptly report it to the MLRO to provide a defence against a possible charge of assisting a criminal to launder the proceeds of their crime or assisting terrorism.

4.3 KYC PRINCIPLES FOR AML AND CFT

4.3.1 Customer Due Diligence

The AML framework primarily rests on conduct of proper Customer Due Diligence (CDD) and Monitoring/Reporting of Suspicious Transactions in accordance with regulation 5 of MLR 2007. The Bank has adopted a risk-based approach for implementing its AML framework, as follows:

a) Customer Acceptance Policy (CAP)

b) Customer Identification Procedures (CIP)

c) Risk Categorization of Customers

The Bank carries out the Customer Identification Procedure at the following stages:

i. While establishing a banking relationship;

ii. Carrying out a financial transaction or

iii. When the Bank has a doubt about the authenticity / veracity or the adequacy of previously obtained customer identification data.

iv. While updating identification data of an existing customer at prescribed intervals.

4.3.2 Customer Acceptance Policy (CAP):

The Bank's CAP sets out criteria for acceptance of customers in such a way as to ensure that its procedures do not result in denial of banking services to the general public. The Bank's "Customer Acceptance Policy" is detailed below:

1. An account will be opened only when the identity of the person or entity has been properly verified.

2. The Bank will not open an account until it has ascertained that the individual or entity does not figure in the list of proscribed individuals and entities published by HM Treasury and the Financial Action Task Force (FATF). If the applicant is identified on this list, the Bank will immediately notify the HM Treasury and NCA that the applicant has attempted to open an account.

3. The Bank will only accept a customer after verifying their identity as laid down in its Customer Identification Procedures (CIP).

4. The Bank has a list of documents and other information to be collected in respect of identification of different types of customers depending on the perceived risk and in accordance with best

banking practices set out in Joint Money Laundering Steering Group Guidance for the UK Financial Sector.

5. The Bank will not open an account where the Bank is unable to apply appropriate CIP or Customer Due Diligence (CDD) measures, such as: inability to verify the identity, inability to obtain documents required as per the risk categorization due to non-cooperation of the customer, or unreliability of the data / information provided to the Bank.

6. When a customer is permitted to act on behalf of another person / entity, the Bank will ensure that its CDD procedures are applied in respect of both the account holder and intermediary and in compliance with established laws and best banking practice.

7. The Bank will only open accounts for customers with outstanding County Court Judgement (CCJ) very selectively and based on the individual merits of the customer. Such accounts may only be opened with the approval of the CEO.

8. The Bank will only open accounts of Money Services Business (MSB) / Bureau de Change on a very selective basis after:

    a. satisfying itself as to the genuineness and competence of the principals;

    b. upon completion of an onsite visit by the ED and MLRO of the Bank and,

    c. Subject to approval by the CEO.

    d. Regular monitoring of the client's AML procedures.

    e. Seek evidence as to the Money Services Business (MSB) / Bureau de Change regulated status by checking with the regulator or through the receipt of other independently obtained evidence

    f. Such companies will be considered under a High risk category and Enhanced Due diligence (EDD) procedures will be carried out.

    g. The account will be subject to detailed monitoring by the MLRO during the initial 6-month period.

4.3.3 Customer Identification Procedures (CIP):

i. Establishing Identity:

Identification is an act of establishing beyond doubt who a person is and who a person purports to be. It involves identifying the customer, by using reliable and independent sources, documents, data or information.
The Bank will obtain sufficient information, to its satisfaction as is necessary, to establish the identity of each new customer, whether regular or occasional in the context of the purpose of the banking relationship.
The Bank has set standards for obtaining comprehensive information from a new customer at the initial stage and from existing customers at the time of updating their identification data.

ii. Verifying Identity:

Where the identity of a customer is to be verified electronically, this will be done by the Bank using as its basis the customer's full name, address and date of birth. Electronic checks either

direct or through a supplier which meets criteria set out by the JMLSG guidance notes, to provide reasonable assurance that the customer is who, they say, they are. Verification of identity must be in conformity with the Bank's AML procedures manual for account opening procedures. The Bank will ensure that process of electronic verification meets standard level of conformation before it will be relied upon. Standard level of conformation, in circumstances that do not give rise to concern or uncertainty, will be:

- First match on individual's full name and current address;
- Second match on individual's full name and either his current address or his date of birth. The address proof obtained from a customer should not be older than 3 months; and
- In certain cases as a matter of financial inclusivity, the Bank may waive the condition for address proof of the applicant and rely on other sources to serve the purpose especially in the following two cases:
    - Overseas students who come to the UK for pursuing their studies and who do not have proof; in such circumstances a certificate from the university or college concerned of their admission to the course and their passport and VISA will be sufficient – copies must be taken for the Bank's records.
    - Similarly spouses and family members of officers or employees on secondment to the UK may not be employed or have proof of address, as the housing accommodation, utility or council tax bills may be in the spouse's name; in such cases the Bank may rely on other sources of identification such as a marriage certificate and the address proof of the working spouse.

In addition to establishing the identity of the applicant, the Bank will collect additional information while opening new account for the purpose of further due diligence measures on the customer, such as:.

- the purpose and reason for opening the account or establishing banking relationship;
- the anticipated level and nature of the activity that is to be undertaken;
- the expected origin of the funds/Source of Funds to be used within the relationship; and
- details of occupation / employment and sources of wealth or income required for banking relationships

All new accounts will be monitored for at least six months by the Branch Head or Relationship Manager to observe whether the activities in the account conform to the KYC information given by the account holder.

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 Bank. The Bank will ensure that staff so authorised receive appropriate training. The staff member conducting verification of identity will complete the process by checking that the client is not the subject of sanctions or other statutory measures or a Politically Exposed Person (PEP), using screening methods set out by MLRO in the Bank's AML procedures manual.

4.3.4 Immigration Checks on New Accounts:

The Immigration Act 2014 was passed into law on 14 May 2014. It prohibits banks and building societies from opening new current accounts (or granting access to existing) current accounts

unless they have performed a 'check' on the applicant and confirmed that they are not a known 'immigration offender'. A bank current account is not defined in the legislation. HM Treasury has stated that the primary test will be the primary purpose of the account being used as a current account. The prohibition does not therefore apply to savings accounts or Notice accounts. The prohibition covers opening an account in relation to which a disqualified person is a signatory or is identified as a beneficiary as well as adding a disqualified person as an account holder or as a signatory or identified beneficiary in relation to an account. The implementation of the current account provisions in the Act will be 12 December 2014.

Banks and building societies are required to perform a check on the applicant and confirm that they are not a known "immigration offender". The check is required to be made with a specified anti-fraud agency i.e. CIFAS. If the check reveals that an applicant is disqualified by virtue of not having the appropriate permission to live in the UK, the bank will be obliged to refuse the application.

4.3.5 Business Wide Risk Assessment and Risk Categorization of Customers

As prescribed by the FCA in its Thematic Review published in November 2014, and the *Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017*, bank is required to evidence that they have taken appropriate steps to identify, assess, understand, and mitigate AML/CTF risk including giving consideration to risk factors such as customer, product, geography, and channel.

Union Bank of India (UK) Ltd carries out a business wide risk assessment, at least annually, which is presented to the Risk and Compliance Committee (RCC) of the Board for their review and approval.

The Bank uses a risk based approach to categorise its customers and has put in place a system that classifies risks as follows:

i. By Customer type

ii. By Product

iii. By Delivery channel

iv. By Geography

i. By Customer Type:

While opening an account, the Bank obtains all the information necessary to satisfy its due diligence requirements, in so doing due care is taken to request only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein are not allowed to be divulged by the Bank for cross selling or any other purposes.

The customer profile mainly contains details relating to customers identity, and the following information:

a) **Nationality**

Date of birth
Anticipated / Actual Annual Turnover
Nature of occupation/business activity

Information about the clients' business/ employment and their location
Place of incorporation of the Company/ business or trust

ii. By Product:

The risk classification will also take into account, the choice of product by the customer. Product types are classified as Low, Medium and High. As an example, remittances are considered high risk as the remitted funds could be used to fund a terrorist activity, hence the Bank needs to monitor the geographic destination of funds and because of this the product is rated high risk; while current accounts and retail loans are assigned medium risk and term deposits, SME loans and corporate credit are rated as low risk.

iii. By Delivery Channel

The Bank has two main delivery channels for providing products to its customers as detailed below:

a) Branch banking (face to face customers)

b) Internet banking (e-banking)

While branch banking is a low risk delivery channel, internet banking poses a higher risk than branch banking and is, therefore, assigned as high risk.

Staff allocate each customer an overall risk categorization of high medium or low derived from a combination of customer type risk, product risk and delivery channel risk. For low and medium and risk customers the account opening decision is made by the Branch Head and for high risk customers the decision is made by the MLRO. For high risk customers the Bank may at its discretion ask for more documents or information to satisfy themselves on the customer due diligence as appropriate to the level of risk, including but limited to:

- obtaining details of the source of the customer's funds and the purpose of the transactions
- obtaining additional evidence of identity
- applying supplementary measures to verify or certify documents supplied or requiring certification by a credit or financial institution
- ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

iv. By Geography

A risk-based approach must be undertaken at all times, the higher the risk, greater due diligence measures should be applied when undertaking business with a customer from the country concerned. Customer's geographical area of operation is also considered in the overall risk assessment. The money laundering risk of countries where customers reside/carry out business and with which transactions are carried out and compared against the 'Know Your Country' and Basel AML Index country list ranking.

'Know your country' risk rating is based upon data collected from many international and government agencies, which are subjectively weighted to provide a free rating tool that is predominantly focused on money laundering and sanctions issues. Whereas Basel's overall score is based on a new FATF evaluation, which includes an effectiveness assessment. Bank refers to the country risk rating published by both these agencies.

These agencies publish an annual report on Country Risk ratings, mentioned below.

- Low risk: with scores 80-100
- Lower Medium: with scores 70-80
- Medium risk: with scores 60 - 70
- Medium Higher: with scores 50 - 60
- High risk: with scores less than 50

Complete list of countries and their scoring has been included in Appendix 3

v. FATF High-risk and other monitored jurisdictions:

The FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing (AML/CFT). The FATF's process to publicly list countries with weak AML/CFT regimes has proved effective. As of February 2020, the FATF has reviewed over 100 countries and publicly identified 80 of them. Of these 80, 60 have since made the necessary reforms to address their AML/CFT weaknesses and have been removed from the process, however with regards to countries considered as substantial AML risks, below countries are classified as:

"High-Risk Jurisdictions subject to a Call for Action".

- Democratic People's Republic of Korea (DPRK)
- Iran

Jurisdictions under Increased Monitoring – 30 June 2020

- Albania
- The Bahamas
- Barbados
- Botswana
- Cambodia
- Ghana
- Jamaica
- Mauritius
- Myanmar
- Nicaragua
- Pakistan
- Panama
- Syria
- Uganda
- Yemen
- Zimbabwe

- As a policy Bank will not provide any banking service to customer based in Democratic People's Republic of Korea (DPRK) & Iran. However, follow high level of due diligence and also seek senior management approval before entering into any new business arrangements with customers based in above mentioned High-Risk Jurisdictions.

Companies registered in offshore tax havens and free trade zones: these jurisdictions frequently present difficulties in verifying beneficial ownership and control because of lack of publicly-available information. The company registration process in some offshore jurisdictions is very lax and permits nominee directors and shareholders, trust structures and, in some cases, bearer shares. The Bank should establish the reason for the choice of jurisdiction and categorize these companies under High Risk accounts and hence Enhanced Due Diligence measures to be applied.

Staff should assess the risk posed by the customer on each parameter as Low, Medium or High based on the above information, for example if the nationality of the applicant is from a FATF jurisdiction it should be high risk whereas for a UK national it would be low risk. The procedures are made available to all staff through the Bank's intranet.

Staff allocate each customer an overall risk categorization of high medium or low derived from a combination of customer type risk, product risk, delivery channel risk and geography risk. For low and medium and risk customers the account opening decision is made by the Branch Head and for high risk customers the decision is made by the MLRO.

For high risk customers the Bank may at its discretion ask for more documents or information to satisfy themselves on the customer due diligence as appropriate to the level of risk, including but limited to:

- obtaining details of the source of the customer's funds and the purpose of the transactions
- obtaining additional evidence of identity
- applying supplementary measures to verify or certify documents supplied or requiring certification by a credit or financial institution
- ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

4.4 TYPES OF CUSTOMER DUE DILIGENCE:

The extent of due diligence undertaken by the Bank when opening an account or processing high value transactions through existing accounts is dependent on the perceived Money Laundering Risk. The Bank applies a "Simple Due Diligence" process for Low Risk accounts and" Enhanced Due Diligence" measures for High / Medium Risk Customers as per JMLSG guidance notes, including those for whom the sources of funds are not clear. The Bank's Risk Based Approach doesn't obviate the need for Enhanced Due Diligence when a higher risk scenario is identified. Separate customer identification is required for non - account holder customers, for any one-off transactions.

4.4.1 Simplified Due Diligence:

Simplified due diligence is permitted where bank determines that the business relationship or transaction presents a low risk of money laundering or terrorist financing, taking into account bank's risk assessment. This is a change from the Money Laundering Regulations 2007, under which SDD was the default option for a defined list of entities.

Regulation 37(3) of the MLR 2017 sets out a list of factors to be taken into account in determining whether a situation poses a lower risk of money laundering or terrorist financing, such that SDD measures can be applied. However, bank should be aware that the presence of one or more of the below factors as stated in 37(3) is not necessarily indicative that a given situation is lower risk.

- ✓ customer risk factors, including whether the customer
    - is a public administration, or a publicly owned enterprise;
    - is an individual resident in a geographical area of lower risk
    - is a company whose securities are listed on a regulated market, and the location of the regulated market;
- ✓ product, service, transaction or delivery channel risk factors,
- ✓ geographical risk factors, including whether the country where the customer is resident, established or registered or in which it operates is
    - o an EEA state;
    - o a third country which has effective systems to counter money laundering and terrorist financing;
    - o a third country identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism (within the meaning of section 1 of the Terrorism Act 2000(**c**)), money laundering, and the production and supply of illicit drugs;
    - o a third country which, on the basis of credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or nongovernmental organisations

In making the risk assessment relevant staff must bear in mind that the presence of one or more risk factors may not always indicate that there is a low risk of money laundering and terrorist financing in a particular situation.

4.4.2 Enhanced Due Diligence:

It is the Bank's policy to undertake Enhanced Due Diligence for the following types of customers.

i. Non-face to face customers and
ii. High net worth individuals (HNI)*;
iii. Trusts, charities, NGOs and organizations receiving donations**;
iv. Politically exposed persons (PEPS) of domestic and foreign origin / resident outside UK;
v. Correspondent banking relationships.

vi. Individuals, legal persons and financial institutions from high risk countries as called for by FATF

*Customers who are expected to hold or holding deposits of more than £1 Million across all accounts.
** Only registered entities.

A. **Accounts of Politically Exposed Persons (PEPs)** A PEP is defined as "an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such person." The EU 4th Money Laundering Directive widened the definition of PEPs to include domestic individuals occupying prominent public functions, in addition to those from abroad. A prominent function could be a prime minister or minister or senior politician, Head of Judiciary or Police or other Public sector undertakings or their immediate family members, or known close associates.

The Bank has put in place procedures through an AML online application system to identify such individuals at account opening and at transaction stage. The Bank generally does not open accounts or establish relationships by accepting deposits from persons holding high profile public office or positions of substantial influence where the level of funds expected to be deposited are far in excess of the declared source of income/remuneration or when there is lack of transparency over the source of funds. Funds of the above nature cannot be accepted as it may result in reputational risk for the Bank. The Bank shall not ordinarily open an account or establish relationship with politically exposed persons and their connected persons/associates' account until such time it is fully satisfied with the background, provenance of wealth that will be used to support the business and the purpose of opening the account is clear. Such accounts will not be opened without the specific approval of the MD & CEO and ED (in the absence of CEO).

B. CORRESPONDENT BANKING:

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc.

The Bank will gather sufficient information to understand fully the nature of the business of the correspondent / respondent bank. Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's / respondent's country will be of special relevance to the Bank.

Similarly, the Bank will also try to ascertain from publicly available information whether the other bank has been subjected to any Money Laundering or Terrorist financing investigation or Regulatory action.

Such relationships will only be established by the Bank with the approval of the MD & CEO or ED (in the absence of CEO).

The responsibilities of each bank with whom a correspondent banking relationship is established will be clearly documented by the Bank. In the case of payable-through-accounts, the correspondent bank will satisfy itself that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank will also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

The Bank should be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against Money Laundering and Terrorist financing.

The Bank will ensure that its respondent banks have Anti Money Laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

Correspondent Relationship with a "Shell Bank"

The Bank will refuse to enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group).

As shell banks are not permitted to operate in UK, the Bank will also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks.

C. NON FACE TO FACE CUSTOMERS:

i. Accounts of companies and firms:

a. The Bank will remain vigilant against business entities being used by individuals as a `front' for maintaining accounts with the Bank. The Bank will therefore examine the control structure of the entity, determine / ascertain the source of funds and identify the persons who have a controlling interest and who comprise the management.

b. These requirements will be moderated by the Bank according to the Money Laundering Risk Perception e.g. in the case of a Public Ltd. Company it will not be necessary to identify all the shareholders.

ii. Client accounts opened by professional intermediaries:

a. When the Bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a third-party client, that client must be identified.

b. The Bank will hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. The Bank will also maintain 'pooled' accounts managed by lawyers / chartered accountants or stockbrokers for funds held on deposit' or 'in Clients Account ' for a range of clients.

c. Where funds held by the intermediaries are not co-mingled at the Bank and there are 'sub-accounts', each of which are attributable to a beneficial owner, all the beneficial owners will be identified. Where such funds are co-mingled at the Bank, the Bank will still look through to the beneficial owners.

d. Where the Bank relies on the 'Customer Due Diligence' (CDD) undertaken by an intermediary, the Bank will satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements.

iii. Syndicated Lending

Syndicated loans are usually loans to large, often multi-national companies, many of which may have their shares listed, or are parts of corporate groups whose shares are listed, on EU regulated or comparable regulated markets. As such, the money laundering risk relating to syndicated loans for this type of customer is regarded as low.

The features of all lending are generally that the initial monies advanced are paid into a bank account. In syndicated lending the monies are usually handled by the Agent making it unlikely that the loan proceeds will be used by money launderers in the placement stage of money laundering. Syndicated facilities could, however, be used to layer and integrate criminal proceeds. Repayments are usually made from the Borrower's bank account to the Agent who administers the repayment from its bank accounts to the Lenders. Repayments in cash are unlikely.

Given that a syndicated loan results in the Borrower receiving funds from the Lender, the initial transaction is not very susceptible to money laundering. The main money laundering risk arises through variations in the loan arrangements such as the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination without a good commercial explanation. When these circumstances occur the source of the money used to accelerate the repayment schedule, or terminate the loan early should be identified.

In circumstances where the Bank participates in Syndicated Lending through a Lead Bank, Arranger or Agent, such Agents have an obligation to verify the identity of the borrower, the Bank may, taking a risk based approach, accept the due diligence carried out by the mandated Lead Manager/Arranger and /or Agent on the borrower where they are in comparable jurisdictions. In such circumstances, the Bank may rely on the certificate stating that the CDD has been undertaken and document is available on request.

Where the Mandated Lead Manager/Arranger and /or Agent are not in comparable jurisdiction, the Bank will carry out appropriate CDD independently taking a risk based approach on the borrower including, where appropriate, taking account of the due diligence carried out by the mandated Lead Manager/Arranger/Book-runner.

4.4.3 Identification Procedure for non-account holding customers for one-off transactions:

The Bank will only provide remittance facilities for customers who hold accounts with the Bank. Where, in exceptional circumstances, a remittance for non-account holder (“remitter”) is considered, customer Identification procedures and transaction monitoring must be carried out on the remitter.
If the funds for a remittance are received by cheque, it is the Bank’s practise to require that the cheque be drawn on the remitters’ account with a FCA regulated financial institution.

4.5 STAFF ACCOUNTS:

There are occasions where the Bank will receive applications to open accounts for employees of Union Bank of India UK Ltd who are either recruited directly in the UK or have been deputed

from the parent bank. In these circumstances the following documents are required for account opening:

- Fully completed application form
- Evidence of identity (usually current Passport and Biometric card)
- Proof of address* – Utility bill, lease agreement, bank statement.

*Address proof waiver – accounts for staff members (i.e. India Based Officers) may be opened without a proof of address only as an exception after obtaining approval from competent authority (MLRO), however the account would be initially opened with Bank's address details. The address would be updated to personal residence address as soon as the staff member provides one of the above mentioned documents, usually within 60 days. Branch head to monitor the exception accounts and report to MLRO on a monthly basis.

4.6 Ultimate Beneficial Owners (UBOs)

Bank should always establish the underlying beneficial ownership of all companies and other legal entities with which the bank conducts business and the beneficial ownership of all funds or other properties that are handled by the Bank.

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 so that the relevant person is satisfied that he knows who the beneficial owner is, including,
in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and obtaining information on the purpose and intended nature of the business relationship.

The beneficial ownership of the company must be independently verified at Companies House

Offshore companies and trusts may be operated from jurisdictions which are inherently high risk and where it may be difficult to confirm the true nature of beneficial ownership.

5 AML MANAGEMENT STRUCTURE

It is the Bank's policy to remain compliant with all AML and CTF rules and regulations issued from time to time by the regulators.

In line with this policy, the Bank has appointed a Money Laundering Reporting Officer (MLRO) as per SYSC 3.2.6JG. The MLRO assesses all aspects of compliance with FCA's requirements on prevention of money laundering /combating of financing of terrorism.

The Bank provides the MLRO with the necessary authority and resources for the on-going implementation of a compliant AML regime, as per JMLSG guidelines. In particular, the Board of Directors and the CEO ensure that the MLRO is provided with the following:

- active support of the Board, the CEO and all department heads and branch head;
- adequate resources and support staff for imparting training, preparation of training material,

conducting awareness workshops and for the monitoring, adherence of AML-CFT procedures and effective discharge of responsibilities;

- independence of action of the MLRO to ensure that there is no pressure on the MLRO to perform their duties contrary to the provisions of this policy;
- access to information at all times to monitor high value transactions, suspicious transactions or any other activity of the Bank as may be required;

The MLRO will monitor all aspects of AML policy and procedures continuously. In addition to the above, the MLRO will ensure continuing competence and monitor the effectiveness of systems and controls. Any deficiencies in AML compliance requiring urgent rectification will be dealt with immediately by the MLRO, who will report such incidents to the relevant Senior Management when appropriate and request any support that may be required.

The MLRO will prepare an annual AML monitoring report, and submit the report firstly to the Risk & Compliance Committee and then to the CEO / Board for their consideration. The report will cover the following issues:

- a summary of the firm's money laundering risk profile and vulnerabilities, together with information on ways in which these are changing and evolving
- a summary of any changes in the regulatory environment(s) in which the firm operates
- a summary of AML activities within the firm, including the number of internal suspicion reports received by the MLRO and the number of disclosures made to the authorities
- details of any compliance deficiencies on which action has already been taken, together with reports of the outcomes
- details of any compliance deficiencies on which action needs to be taken, together with recommended actions and management support required
- an outline of plans for the continuous development of the AML regime, including on-going training and awareness raising activities for all relevant staff.

Where management action is indicated, the Board / CEO will respond to the report with details of appropriate action to be taken. Should the MLRO of the Bank be temporarily unavailable (as per the SUP 10.5.5R) for a period of 12 weeks in any consecutive 12 month, pre-approval for a deputy from the FCA will not be required. However, where it is foreseeable that the deputy will be performing as MLRO for more than 12 weeks, then the Bank shall apply to FCA for approval in advance for the appointed deputy to manage this controlled function.

Management Controls

As part of on-going monitoring the MLRO will submit a monthly report to the Executive Management Committee of the Board giving status of consent for applications submitted and Suspicious Activity Reports lodged with NCA.

The MLRO is required to submit an annual report on the changes in the risk profile of the Bank's AML–CFT prevention regime and suggest changes in approach required arising from new products or changes in the banking environment.

Internal Audit

It is the responsibility of the Bank's Internal Auditor to check on the following aspects of AML and CFT during the course of their audit:

- Whether procedures are followed for account opening including KYC.
- Whether enhanced due diligence is done in case of accounts where it is required.
- Whether the operations and nature of credits are being monitored and
- Whether credits or payments not conforming to the CDD are reported to the managers and whether the issues are resolved in a proper manner.

6 WIRE TRANSFERS

Banks use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

FATF issued Special Recommendation VII, with the objective of enhancing the transparency of electronic payment transfers ("wire transfers") of all types, domestic and cross border, thereby making it easier for law enforcement agencies to track funds transferred electronically by terrorists and criminals. This was implemented in member states of the European Union, including the UK, through Regulation 1781/2006.

The Bank is subject to the obligations of the Wire Transfer Regulation in its role as a Payment Service Provider (PSP) for the payee and an intermediary PSP. An overview of these obligations is provided below for adherence.

i. Transactions below EUR 1000 in value will not require the collection or sending of Complete Information on the Payer ("CIP") as these transactions are subject to the exemption provided by the Wire Transfer Regulation.

ii. Transactions exceeding EUR 1000 in value require the collection and verification of CIP on a risk based approach as set out in the JMLSG guidance.

iii. Where a wire transfer is funded through a card payment exceeding £800, as it would be treated for practical purposes as a transaction for payment of goods and services and consequently satisfies the requirement for a unique identifier to accompany the transfer of funds.

iv. When funding transactions exceeding EUR 1000 are made from a bank account or other financial institution account in the EU, then CIP can be substituted with an account number or a unique identifier enabling the transaction to be traced back to the payer.

Regulation requires the ordering financial institution to ensure that all wire transfers carry specific information about the originator (Payer) who gives the instruction for payment to be made. The core requirement is that information consists of name, address and account number although there are a number of permitted variations and concessions.

The Bank must comply with the regulations at all times and ensure that all wire transfers are accompanied by information about the remitter and the receiver with their respective bank details. All wire transfers are subject to screening of sanctions lists and The Bank employs an alert management system to check names against such lists which are updated regularly. Notwithstanding the provision of 5 (i), the Bank will only process transactions of exempt value after conducting proper customer due diligence.

6.1 Cross-Border Wire Transfers

a) All cross-border wire transfers must be accompanied by accurate and meaningful originator information.

Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, will be included.

Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (b) above.

6.2 Transfers within the European Union

Where both payer and payee are located within the European Union, wire transfers must be accompanied, where complete payer information cannot be given, by the payer's account number or by a unique identifier which enables the transaction to be tracked back to the payer.

6.3 Role of Ordering, Intermediary and Beneficiary Banks

Ordering bank

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. When acting as an ordering bank, the Bank will ensure that qualifying wire transfers contain complete originator information. The Bank will also verify and preserve the information for a period of at least six years.

Intermediary bank

For both cross-border and domestic wire transfers, when the Bank processes an intermediary element of a chain of wire transfers it will ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record of all the information received from the ordering bank will be kept by the Bank for at least ten years.

Beneficiary bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. Accordingly, when acting as a beneficiary bank, the lack of complete originator information will be considered by the Bank as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the NCA. The Bank will also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter.

If the ordering bank fails to furnish information on the remitter, the Bank will consider restricting or even terminating its business relationship with the ordering bank.

The Bank will list check both incoming and out-going wire transfers using online AML checks to ensure that none of the parties to the transfer are on any Sanction List.

7 TRADE FINANCE

7.1 MONEY LAUNDERING RISK IN TRADE FINANCE

In the context of JMLSG guidance, the term 'Trade Finance' is used to refer to the financial component of an international trade transaction, i.e., managing the payment for goods and/or related services being imported or exported. Trade finance activities may include issuing letters of credit, standby letters of credit, and bills for collection or guarantees. Trade Finance operations are often considered in a cross-border context but can also relate to domestic trade.

The Financial Action Task Force (FATF), regulators and others have identified misuse of the trade system as one of the methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the legitimate economy. FATF typologies' studies indicate that criminal organisations and terrorist groups exploit vulnerabilities in the international trade system to move value for illegal purposes. Cases identified included: illicit trafficking in narcotic drugs; illicit trafficking in stolen or other goods; corruption and bribery; fraud; counterfeiting/piracy of products; and smuggling. More complicated schemes integrate these fraudulent practices into a complex web of transactions and movements of goods and money.

Given the nature of the business, there is little likelihood that trade finance will be used by money launderers in the placement stage of money laundering. However, trade finance can be used in the layering and integration stages of money laundering as the enormous volume of trade flows obscure individual transactions and the complexities associated with the use of multiple foreign exchange transactions and diverse trade financing arrangements permit the commingling of legitimate and illicit funds

FATF's study notes that the basic techniques of trade-based money laundering include:

9. **Over Invoicing**: by misrepresenting the price of the goods in the invoice and other documentation (stating it at above the true value) the seller gains excess value as a result of the payment.
10. **Under invoicing**: by misrepresenting the price of the goods in the invoice and other documentation (stating it at below the true value) the buyer gains excess value when the payment is made.
11. **Multiple invoicing**: by issuing more than one invoice for the same goods a seller can justify the receipt of multiple payments. This will be harder to detect if the colluding parties use more than one financial institution to facilitate the payments/transactions.
12. **Short shipping**: the seller ships less than the invoiced quantity or quality of goods thereby misrepresenting the true value of goods in the documents. The effect is similar to over invoicing
13. **Over shipping**: the seller ships more than the invoiced quantity or quality of goods thereby misrepresenting the true value of goods in the documents. The effect is similar to under invoicing.

14. **Deliberate obfuscation of the type of goods**: parties may structure a transaction in a way to avoid alerting any suspicion to financial institutions or to other third parties which become involved. This may simply involve omitting information from the relevant documentation or deliberately disguising or falsifying it. This activity may or may not involve a degree of collusion between the parties involved and may be for a variety of reasons or purposes.
15. **Phantom Shipping**: no goods are shipped and all documentation is completely falsified.

7.2 Risk of Dual-Use Goods in Trade Finance

Dual-use goods are items that have both commercial and military or proliferation applications. This can include goods that are components of a weapon, or those that would be used in the manufacture of a weapon (e.g., certain machine tools that are used for repairing automobiles can also be used to manufacture certain component parts of missiles)

Dual-use goods destined for proliferation use are difficult to identify, even when detailed information on a particular good is available. Regardless of the amount of information provided for a particular good, highly specialised knowledge and experience is often needed to determine if a good may be used for proliferation. Dual-use items can be described in common terms with many uses – such as "pumps" – or in very specific terms with more specific proliferation uses – such as metals with certain characteristics. Further, many goods are only regarded as dual-use if they measure-up to very precise performance specifications

7.3 Handling the AML Risks Arising from Trade Finance Transactions

The FCA's thematic Review TR13/3 (July 2013) on banks' control of financial crime risks in trade finance highlights the facts that the majority of banks are not taking adequate measures to mitigate the risk of money laundering and terrorist financing in their trade finance business and asks banks to conduct significant work to ensure that all financial crime risks are routinely considered when processing trade finance transactions.

The Bank takes a variety of risk-based approaches to mitigate the money laundering and terrorist financing risks arising from its trade finance business, mainly through considering the details of the transaction such as;

1. the amount of information available such as the size/type of the firm and the volume of business that it is handling, parties involved in the transaction and the countries where they are based, as well as the nature of any goods forming the basis of an underlying commercial transaction.
2. Bank has registered with International Maritime Bureau (IMB) for verification of Bill of Lading, MLRO will perform necessary checks in addition to the IMB report.
3. The Bank is not expected to investigate commercial transactions outside their knowledge, although naturally if documentation they see as part of a banking transaction gives rise to suspicion, the Bank is obligated to report the transaction.

   Apart from, in certain specific highly structured transactions The Bank shall exercise reasonable judgement and consider whether additional investigation should be undertaken. Such investigation may include determining whether over-invoicing or under-invoicing, or any other misrepresentation of value, may be involved, which cannot usually be based solely on the trade documentation itself. Based on the normal course of the business, where the unit price of goods

appears to be materially different from the current market value, The Bank shall consider whether they have a suspicion and whether they should accordingly submit a Suspicious Activity Report ("SAR") to the NCA.

8 NEW PRODUCTS

As the banking industry evolves rapidly with technology and new products, it also gives rise to new risks. Hence all new products being introduced by the Bank whether deposit products, loan products or payment service products require mitigation strategies for these new risks. Accordingly, all new deposit products and payment services/ electronic money products must be evaluated by the Risk and Compliance Committee and loan/ credit products by the Credit Committee and will be implemented only if approved by the respective committees.

When new products are presented to the respective committees for approval the MLRO will be invited to the meetings and requested to provide an assessment of the money laundering and terrorist financing risks arising from the new product being considered and to make recommendations as to the appropriate risk mitigation procedures that should be implemented.

9 MONITORING AND REPORTING

9.1 MONITORING OF HIGH RISK ACCOUNTS

On-going monitoring is an essential part of the Bank's AML framework. The Bank can effectively control and minimise the risk only if it understands the normal and reasonable activity of the customer, so that it has means to identify transactions that fall outside the regular pattern of activity.

Transaction monitoring is the daily act of screening transactions of all types that occur in any account managed by the Bank. The main objective of this procedure is for the timely identification of significant changes in patterns or unusual account behaviour. This would also enable further investigation that would ascertain whether or not such accounts can be classified as 'suspicious' and disclosed to the relevant authorities.

However, the extent of monitoring depends on the Money Laundering Risk sensitivity of the account. The Bank pays special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

All significant client instructions and transactions receive the attention of the Branch Manager/ Department Head who will consider whether they are consistent with those anticipated.

.

If a client's instruction or transaction is not consistent with what is anticipated the following actions will be taken:

4. an explanation will be sought, if appropriate, by contacting the client
5. the involvement of unexpected jurisdictions or organisations will be checked with the Bank's MLRO for possible alerts or sanctions
6. if a satisfactory explanation is found, the client file will be updated to reflect the change in anticipated client activities

7. if no satisfactory explanation is found, the MLRO will consider whether there are grounds to suspect money laundering
8. Branch will maintain a register for recording the nature and purpose queries raised along with customer responses.
9. the MLRO will consider whether there is cause to carry out a re-assessment of money laundering risk, and, if so, carry this out
10. Irrespective of whether specific incidents have caused a re-assessment of ML risk, every client file will be reviewed periodically to check that
11. the information held is still adequate, correct and up to date
12. the level of client due diligence being applied is still appropriate

Periodic review of client files for AML due diligence purposes is conducted at the same time as business development reviews.

The Bank prescribes / defines various threshold limits for transactions through accounts of counterparties in the AML Software which will generate alerts for those transactions that exceed the limits set and thereby enable monitoring of such transactions in the accounts.

Transactions involving large amounts of cash, inconsistent with normally expected activity of the customer will attract the attention of the Bank.

Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account.

The Bank identifies and monitors high risk accounts based on certain transaction characteristics, such as:

13. unusually large or abnormal transactions or a high frequency of transactions over a customer's account as compared to his peer group;
14. the nature of a series of transactions: for example, a number of cash credits into their account, which was not a normal feature hitherto;
15. the geographic destination or origin of a payment: for example, to or from a high-risk country such as FATF countries, or countries with a weak AML jurisdiction; and
16. the parties concerned: for example, a request to make a payment to or from a person on a sanctions list.
17. obtaining details of the source of the customer's funds and the purpose

High and Medium Risk Categorized accounts will be subjected to greater monitoring. For this purpose, the Bank will consider the background of the customer, i.e. country of origin, sources of funds, the type of transactions involved and other risk factors. Accounts in which suspicious transactions are reported will also be subjected to further monitoring.

Dormant accounts:

An account shall be classified as 'Dormant' where there has been no customer activity for a period of two years or where an account has been flagged as 'Dormant' by virtue of failure to provide data in accordance with any periodic review process.

There is potential for a Dormant Account to be used for fraud or money laundering. To limit this risk an account identified as Dormant or closed shall be designated as such on the computer systems and the customer file. Accounts on the computer system shall be blocked and no customer transactions or entries (other than internal system generated entries or charges) shall be allowed without the specific written authorization of the CEO.

The Identification of Dormant Accounts is on a system run basis, conducted once every half year by the IT Department. On identification of an account where there have been no customer induced operations for over 18 months, the relationship manager will endeavour to re-establish contact with the customer to update the KYC/KYB information and ascertain the reasons for the inactivity and customer's need for the account. If this cannot be determined or where the KYC/KYB information cannot be updated within a period of six months, the account shall be blocked and annotated as Dormant.

Dormant Accounts can only be reactivated by completion of all Account Opening/Periodic Review procedures, including such KYC/KYB, as are appropriate.

Review of accounts:

The Fourth ML Directive is more prescriptive with respect to the ongoing monitoring of customers, and more specific in outlining factors for consideration/evidencing in conducting risk assessments for each customer, and how these risk assessments must be kept up to date. This reinforces the requirement to undertake a risk based approach, and from a practical perspective, which means that the bank must be able to evidence the rationale behind the risk rating applied to each customer.

The Bank will review all accounts on a regular basis and all transactions will be authorised by a manager of the Bank who holds the appropriate delegated authority.

Review of accounts will be carried out based on the risk profile of the customers. The accounts of those customers falling in the high risk categorisation will get closer attention, reviewing them every 6 months for Politically Exposed Persons (PEPs), 12 months for high risk categorisation whereas customers account with medium and low risk categorisation will be reviewed once in 18 months and once in 24 months respectively.

9.2 Reporting of Suspicious Transactions

9.2.1 Internal Reporting

It is the policy of the Bank that all staff members shall remain alert to the possibility of money laundering and shall report any knowledge or any suspicion for which they believe there are reasonable grounds, following the Bank's procedures.

Definitions of Knowledge and Suspicion:

Having Knowledge means knowing something is true, while Suspicion is a degree of satisfaction not necessarily amounting to belief but at least extending beyond speculation as to whether an event has

occurred or not. Although creation of suspicion requires a lesser factual basis than the creation of belief, it must be nonetheless built up on some foundation.

For the purposes of the POCA 2002 and the Terrorism Act, knowledge means knowledge of money laundering activity based on information that became known to the member of staff or MLRO in the course of the business in the regulated sector.

Suspicion is an opinion held that is based on information or circumstances but without certainty or proof.

Employees should note that unusual transactions are not necessarily suspicious. However, the Money Laundering Regulations 2007 regulation 20 requires that unusual transactions and any other activity that is regarded as particularly likely by its nature to be related to money laundering or terrorist funding must be identified and scrutinised. This could result in a suspicion requiring disclosure. Reasonable grounds for knowledge or suspicion arise where the facts or circumstances, if viewed objectively, would lead to an expectation that a reasonable person working in the Bank would know or suspect that someone was engaged in money laundering or terrorist financing. The response of each staff to possible suspicions shall be appropriate to their role and position in the Bank. No one other than the concerned employee is expected to have a greater knowledge and understanding of clients' affairs than the employee performing that role.

Procedure

i. Every member of staff must be alert for the possibility that the Bank's services could be used for money laundering purposes, or that in the course of their work they could become aware of criminal or terrorist property.

ii. Alertness to the possibility of money laundering must be combined with an appropriate knowledge of clients' normal arrangements so that members of staff become aware of possible causes of suspicion.

iii. A member of staff becoming aware of a possible suspicion shall gather relevant information that is routinely available to them and decide whether there are reasonable grounds to suspect money laundering.

iv. The requirement to gather relevant information does not extend to undertaking research or investigation, beyond using readily available information from the account and files of the Bank. Clients may be asked for relevant information but only in the context of routine client contact relevant to the business.

v. If after gathering and considering routinely available information, the member of staff is entirely satisfied that there are no grounds for suspicion, no further action should be taken.

vi. A member of staff who considers that there may be grounds for suspicion, shall raise the matter with the Branch Manager/Department Head. If after a discussion they both agree that there are no grounds for suspicion, no further action should be taken.

vii. If, following the raising of a possible suspicion by a member of staff, or resulting from their own observations, Branch Manager/ Department Head decides that there are reasonable grounds to suspect money laundering, he or she must submit a suspicion report to the MLRO, in the format specified by the MLRO for that purpose. Failure to make a report of a suspicion or knowledge of money laundering is an offence

viii. An internal suspicion report does not breach client confidentiality /professional privilege and no member of staff shall fail to make an internal report on those grounds.

ix. In the circumstance where any member of staff forms a suspicion of money laundering but the responsible Branch Manager/Department Head does not agree that there are reasonable grounds for suspicion, the member of staff forming the suspicion must fulfil their legal obligation by submitting a money laundering suspicion report directly to the MLRO, in the format specified by the MLRO for that purpose.

x. Where it is felt that the report that is being made by the staff member is not suitable for reporting, Branch/Departmental Head must give his/her reasons in support of their findings for consideration by the MLRO. Under no circumstances should a SAR submitted by a member of staff must be blocked/ suppressed. The Branch Manager/Department Head must recognise this legal requirement and assist the staff member in fulfilling it in light of the JMLSG guidelines.

9.2.2 External Reporting

1. It is the policy of the Bank that the Money Laundering Reporting Officer or in his absence his deputy shall receive and evaluate internal suspicion reports, and decide whether a formal disclosure is to be made to the authorities. If so deciding, the MLRO will make the formal disclosure on behalf of the Bank, using the appropriate mechanism.

2. On receiving a money laundering report or money laundering suspicion report or an attempted money laundering report from a member of staff, the MLRO should acknowledge in writing, referring to the report by its date, without including the name of the person(s) suspected. This confirms to the member of staff that their legal obligation to report has been fulfilled.

3. Following receipt of a SAR, the MLRO shall gather all appropriate information held within the Bank, and make all appropriate enquiries of members of staff anywhere in the Bank, in order to properly evaluate the report and reach a decision about the Bank's obligation to make a formal disclosure to NCA.

4. All members of staff shall respond in full to all enquiries made by the MLRO for the purposes of evaluating a suspicion report. Information provided to the MLRO in response to such enquiries does not breach client confidentiality/professional privilege, and no member of staff shall withhold information on those grounds.

   On deciding that a formal disclosure to the authorities is required, the MLRO shall make such disclosure by the appropriate means. The SAR should be made to the NCA online via secure internet. Guidance is available on the website.

   https://www.ukciu.gov.uk/(hgj04b55bkzuwo45b2r5st55)/Information/info.aspx?InfoSection=Submission

5. The MLRO shall document in the report log the reasons for deciding to make or not to make a formal disclosure.

6. Following a formal disclosure the MLRO shall take such actions as required by the authorities in connection with the disclosure.

7. The MLRO is the nominated officer to handle all communications with the various law enforcement agencies regarding the SAR. The MLRO should hold on record in hard copy and soft

copy forms containing all particulars of the transactions reported so that the information can be provided to the law enforcement agencies as and when required.

8. SARs should contain as much detail as possible, such as the occupation/ activity of the client, the nature of business, details of their company or entity, NI number etc, as it will assist the enforcement agencies in their enquiries. However, it may also be noted that the Bank is not under any obligation to collect these details but to only provide all details held on record.

9. There is no obligation to make a report to NCA where:

   i. the identity of the person who is engaged in money laundering is unknown;

   ii. the whereabouts of any of the laundered property is unknown;

   iii. the information that is available would not assist in identifying that person, or the whereabouts of the laundered property.

   An example of such circumstances would be the theft of a cheque book which can lead to multiple low-value fraudulent transactions over a short, medium, or long term period of time.

10. The MLRO should also consider whether to report to HM Treasury when funds are frozen under financial sanctions legislation or if knowledge or suspicion of a listed person or entity or a person acting on behalf of a listed person or entity is involved in the transaction.

The reporting to various law enforcement agencies will have to be made by the MLRO as follows.

Type of reporting	**Address for reporting**
For seeking NCA consent to proceed with a suspicious transaction	UKFIU, PO Box 8000, London, SE11 5EN Phone02072388282 Website: http://www.nationalcrimeagency.gov.uk/ E-mail: ukfiusars@nca.x.gsi.gov.uk
Report under financial sanctions legislation	Asset Freezing Unit, HM Treasury, 1 Horse Guards Road, London SW1A 2HQ. Phone- 02072705454, Website: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets E-mail: financialsanctions@hmtreasury.gsi.gov.uk
SAR to NCA	UKFIU, PO Box 8000, London, SE11 5EN Phone02072388282 Website: https://www.ukciu.gov.uk/(kdckpz5543gddwa1kraq4l45)/saronline.aspx

1. All staff should note that under English Law they are obliged to report knowledge or suspicion of Money laundering and terrorist financing to the MLRO under the POCA and Terrorism Act. Failure

to report will render the staff liable for prosecution or regulatory censure. The maximum punishment for failure to report could be a 5 year imprisonment and/ or a fine.

2. Failure of the Bank to comply with the obligation to freeze funds and not to make funds or economic resources available for suspected terrorists and not to make available financial services to listed persons or entities or to report knowledge or suspicion will render the Bank liable for prosecution. Hence all staff members are cautioned to report such knowledge or suspicions to the MLRO.
3. At times the Bank may receive instructions from a customer to carry out a transaction and if you suspect that it could be linked to Money Laundering the matter should be reported to the MLRO. The MLRO will then decide whether to permit the activity or refer it to the UK Financial Intelligence Unit ("UKFIU" - an arm of the NCA) for their consent. If UKFIU permit the transaction or if there is no reply from them within 7 working days the transaction can be effected. If they do not permit staff must not carry out the instruction. Care should be taken by the MLRO to report (preferably electronically via secure internet for a speedy resolution to the web link as stated in the table in point 11 above) and seek consent from the UKFIU at the earliest opportunity so as to avoid undue delay for the customer.

9.3 Tipping Off

Tipping Off is an offence committed when a person (staff member) discloses the information contained in a report either made internally to the MLRO or externally to the NCA to any other person, which is likely to prejudice any on-going investigation or an investigation that might be conducted following the report.
JMLSG guidance notes to prevent tipping-off place certain obligations on staff that must be adhered to and other points of note are as below:

a) Staff should be aware that under the POCA and Terrorism Act there are two separate offences of tipping off and prejudicing an investigation:
   i. disclosing that an internal or external report has been made;
   ii. the second relates to disclosing that an investigation is being contemplated or is being carried out.

b) Once an internal or external suspicion report has been made, it is a criminal offence for the staff including the MLRO to disclose information about that report which is likely to prejudice an investigation that might be conducted following that disclosure.

c) However, staff may note that reasonable enquiries of a customer made regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is considered as a prudent practice, forms an integral part of CDD measures, and will not be deemed as tipping off.

d) An offence is not committed if the disclosure is made to the FCA (or other relevant supervisor) for the purpose of:
   i. detection, investigation or prosecution of a criminal offence (in UK or elsewhere);
   ii. an investigation under POCA; or
   iii. the enforcement of any order of a court under POCA.

e) Employees are further cautioned that, the Bank cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting consent from the NCA; neither can they

tell them subsequently unless the law enforcement agency /NCA agrees, or a court order is obtained permitting disclosure; nor can they tell a customer that a transaction or activity was delayed because a report had been made under POCA or the Terrorism Act; and cannot tell the customer that law enforcement is conducting an investigation.

f) The Bank does not commit an offence under POCA 2002, or the Terrorism Act if the disclosure is from one credit institution to another, or from one financial institution to another, relating to:

i. A customer or former customer of the Bank making the disclosure and of the institution to which the disclosure is made; or if the disclosure is for the purpose only of preventing an offence under Part 7 of POCA or under Part III of the Terrorism Act; or if the institution to which the disclosure is made is situated in an EEA State or in a country imposing equivalent money laundering requirements; and

ii. The Bank and the institution to which it is made are subject to equivalent duties of protection of personal data (within the meaning of the Data Protection Act 1998).

It is the Bank's policy to make all employees aware of their obligations and the offence of tipping-off. The Bank advises staff to maintain all information on internal or external reporting or a likely report strictly confidential.

10 FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA) & UK FATCA

1. *The Foreign Account Tax Compliance Act (FATCA)* is a regulatory legislation from the United States of America (USA) which is designed to encourage enhanced tax compliance and transparency with respect to US persons who may be investing and earning income through financial institutions or entities outside of the USA. In particular, FATCA seeks to prevent US persons from avoiding US taxation on their income and assets.

   FATCA became effective from 1 July 2014 and Foreign Financial Institutions (FFIs) are required to classify all account holders and to report to HMRC on an annual basis. HMRC will then forward that information to the US Internal Revenue Service (IRS). Currently such information as of each year-end is required to be submitted to HMRC by 31 May the following year (information for 31st December 2014 was required to be submitted by 31st May 2015), along with the following information:

   Name
   Address
   US TIN (where applicable or DoB for Pre-existing Accounts)
   Account number or functional equivalent
   Name and identifying number of Reporting Financial Institution
   Account balance or value
   The total amount of gross interest paid or credited to the account in the calendar year or other reporting period

   The Bank has registered with IRS, US and the Bank's name is listed on the IRS website along with the Global Intermediary Identification Number (GIIN) assigned to the Bank.
   In order to comply with the provisions of the regulations, the Bank has the responsibility to classify its customers (Each Specified US Person either holding a Reportable Account or as a

Controlling Person of an Entity Account) whether a US person or non-US person. Accordingly, the Bank has appropriately revised the account opening form to obtain a suitable declaration from customers.

2. The Crown Dependencies and Overseas Territories(CDOT) and Common Reporting Standards (CRS):

   The Crown Dependencies of Guernsey, the Isle of Man and Jersey and the UK Overseas Territories of Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Gibraltar, Montserrat and the Turks & Caicos Islands have all entered into agreements with the UK to automatically exchange information on financial accounts.

   Of these, the agreements with the three Crown Dependencies and with Gibraltar are reciprocal thus imposing obligations on UK Financial Institutions to collect, maintain and report information to HMRC on financial accounts held by individuals and entities resident for tax purposes in those territories:
   All new accounts opened after 1 July 2014.

   Pre-existing accounts as the due diligence for such accounts must have been completed by 30 June 2015.

   Once identified as reportable accounts, these accounts continue to be reported annually thereafter, subject to account closure or a change of circumstance making them non-reportable.

   The following information is required by HMRC under UK FATCA:
   Name
   Date of Birth
   Social Security Number/National Insurance Number
   Account Number
   Account balance or value
   The total amount of gross interest paid or credited to the account in the calendar year or other reporting period.

11 5TH ANTI-MONEY LAUNDERING DIRECTIVE (5AMLD)

The Fifth Money Laundering Directive (5AMLD) came into force on January 10, 2020. Building on the regulatory regime applied under its predecessor, 4AMLD, 5AMLD reinforces the European Union's AML/CFT regime to address a number of emergent and ongoing issues with the aim to strengthen the barriers in the battle against money laundering and terrorist financing. The directive notes that this new legislation is, in part, a response to the terror attacks that have happened within EU member states over the past few years namely in Britain, France and Belgium. It is worth noting that the 5AMLD has not made any changes to penalties that are in place for breaches, however, the scope of firms/individuals who will be caught by the regulation has widened.

5 key elements of this new Anti-Money Laundering (AML) legislation are:

1. Beneficial Ownership

The new regulation imposes greater transparency on the financial sector regarding beneficial ownership with a focus on the beneficial ownership of trusts. A firms data on beneficial owners will be made

accessible to competent authorities (i.e. the FCA), and professional sector service providers, such as banks and others who can demonstrate a legitimate interest. The same information can be accessed by any member of the public without the need to demonstrate a legitimate interest. This puts further obstacles on a preferred method of money laundering globally as part of the Client Due Diligence process.

- *Bank will continue to record all relevant information at the time of On-boarding, necessary KYC checks are performed and information on UBO's are clearly captured in Bank's KYC DMS – AML-Trac.*

2. Extending the Scope

5AMLD extends AML/CFT obligations to new assets being managed such as:

- Virtual Currencies: increasing the scrutiny on virtual currencies and extending the scope of AML/CTF controls in 4MLD to virtual currency providers, to notably prevent anonymity. Anonymous safe deposit boxes will also no longer be allowed.

- Art Traders: When dealing with high-value artwork that results in a transaction of €10,000 or more, art traders will have to report suspicious activity and perform checks on customers when necessary.

- As a policy, considering bank's risk appetite - Bank will not provide banking service to firms with exposure to Virtual currencies that includes companies dealing with Bitcoin, Ethereum etc
- Any transaction above £5000/$5000 are referred to compliance for review and approval, first line function will continue to seek relevant supporting information and documents for such transactions.

3. PEP (Politically Exposed Persons) Clarification

The Member States must issue a list of specific functions which qualify as "prominent public functions" to make sure individuals who are potential PEPs are identified for monitoring. The EU will then consolidate the lists from the Member States and publish the results keeping the individual's identities anonymous.

4. Enhanced Due Diligence for High-Risk Third Countries

The EU currently maintains a list of High-Risk third countries, and when doing business with clients within these countries, parties are required to undertake enhanced due diligence measures. One of the new updates that the 5AMLD brings, is that any client that is based in a High-Risk country is now subject to compulsory enhanced due diligence measures, of which the 'relevant person' must undertake. These include obtaining information on the source of funds, background checks and beneficial ownership to name just a few. Member States may also prevent firms from opening branches or subsidiaries in high-risk third countries and prevent the opening of a branch or subsidiary of a firm based in a high-risk third country.

- *Bank performs EDD checks on all new accounts taking into account the jurisdiction and ownership structure. These regular AML checks include seeking information on Source of funds, regular background checks and recording UpToDate information on UBOs during Periodic review.*

5. Prepaid Cards

The threshold for prepaid instruments (e-money & prepaid cards) subject to due diligence has been lowered from €250 to €150.

- *Not applicable to our Bank*

12 THE 6TH ANTI-MONEY LAUNDERING DIRECTIVE

On 12 November 2018, approximately 6 months after the adoption of the 5th EU Anti-Money Laundering Directive (5AMLD), the European Parliament published further rules to strengthen the fight against money laundering through the 6th EU Money Laundering Directive (6AMLD). Member States are required to transpose the 6AMLD into national law by 3 December 2020. After which, relevant regulations must be implemented by firms within Member States by **3 June 2021.**

13 AML RISK MITIGATION PROGRAMME

As part of the Bank's risk-based strategy, it is important and a requirement of the FCA and UK AML regulations that the Bank develops and implements a Risk Mitigation Programme (RMP) to prevent and reduce the risk of our products/ services being used for money laundering and /or terrorist financing. Using the UK JMLSG Guidance as a benchmark, the Bank has developed what we believe to be a robust and effective RMP that will address the specific AML risks we face as a business.

The details of our RMP are outlined below:

13.1 CUSTOMER IDENTIFICATION PROGRAMME (CIP)

As mentioned in sec 4.3.1, An effective CIP is the primary defence which the Bank will employ to protect itself and its reputation from the fraudulent use and abuse of its services. The purpose of the CIP is to establish the standards which must be applied to enable the Bank to identify its clients, to meet regulatory and legal obligations, and have effective and robust defence against financial crime.

The identification of a client (and its beneficial owners) involves the collection of necessary identity information and the subsequent verification of the information through the use of appropriate records and/or approved local sources of information (such as a registered list of directors/officers held by the local Companies House). This two-step approach provides the Bank with confidence that it 'knows' the identity of its clients, and ensures that appropriate documentary evidence is available to support this assertion.

13.2 ADEQUATE KNOW YOUR CLIENT (KYC) INFORMATION

- Our standard KYC information will include the following:
- A risk assessment of both the business to be undertaken with the client and the client
- The purpose and reason for opening the account or establishing the relationship
- The anticipated level and nature of the activity that is to be undertaken
- Where applicable, the origin of the funds to be ascertained within the relationship and understanding of the source's of the customer's income pl. redraft-

- Identifying whether the client is a PEP or appears on any other sanctions list including but not necessarily limited to the HM Treasury Consolidated List of Financial Sanctions Target,
- Media search is also done

The above will be documented in a file note which will include a completed account opening form and checklist

13.3 Approval for opening accounts for Politically Exposed Persons (PEPs)

As mentioned in Sec 4.4.2, Bank has put in place procedures through an AML online application system (AML-Trac) to identify individuals as a Politically Exposed Person including Domestic PEPs at account opening and at transaction stage.

The Bank shall not ordinarily open an account or establish relationship with politically exposed persons and their connected persons/associates' account until such time it is fully satisfied with the background, provenance of wealth that will be used to support the business and the purpose of opening the account is clear.

Such accounts will not be opened without the specific approval of the CEO and by ED (in the absence of CEO).

13.4 Transaction monitoring

As mentioned in Sec 9.1. There are three aspects to the Bank's monitoring of transactions for which the Bank has both automated and manual systems and processes;

• Pre-execution transaction monitoring (real time and automated) which is specifically connected with the identification of transactions which would, if executed, result in a breach of applicable sanctions or embargoes. Considering the small quantity of transactions processed by the bank, all transactions above £ 5000 are referred to MLRO for review and approval.
Bank additionally has in place Swift Sanctions screening system, which places transactions on hold for any match against the sanctions list. MLRO reviews the transactions and then seeks additional information before releasing the payment..

• Post-execution transaction monitoring (automated and manual) focuses on the identification of single or multiple transactions which would be considered to be suspicious, AML-Trac generates alerts on daily basis which are allocated to branch by compliance and reviewed by the branch and dealt accordingly either for closure or for further investigation..

• Ad-hoc monitoring focuses on the identification of suspicious activity, it is an activity which is undertaken on a more informal basis. It is a procedure which is undertaken by Branch staff, and is considered one of the most effective means of identifying suspicious activity. Staff who are familiar with individual clients and their expected economic activity, are ideally positioned to identify transactions which are unusual of their client's normal activities

13.5 Trade Finance Checks:

As mentioned in Sec 7.3 Bank has put in place steps to verify the authenticity of the documents provided as part of Transaction. All Bill of ladings are referred to International Maritime Bureau (IMB) for their confirmation.

Compliance additionally performs due diligence including checks for sanctions on the parties involved i.e. Shipper, Manufactures, Shipping Agents and also on the Buyer.

Checks on the Vessel for sanctions, Transhipment are recorded additionally, Compliance also check for Dual usage goods and pricing before approving the transaction.

13.6 SCREENING OF POTENTIAL AND EXISTING CLIENTS AGAINST THE HM TREASURY SANCTIONS LIST AND OTHER OFFICIAL DATABASE

All new/existing clients are screened against the HM Treasury Consolidated List of Financial Sanctions, OFAC, EU Sanctions list and other sanctions database e.g. Dow Jones Existing clients are screened daily using the Bank's automated AMl -Trac system (which also screens for PEP and adverse media information).

If they appear on one of the Financial Sanctions lists an account cannot be opened.

All clients are screened against updates to any applicable lists within 48 hrs of these updates being made available. Any positive match will be immediately notified to the MLRO

13.7 PERIODIC REVIEW OF CLIENT RELATIONSHIPS

Periodic Review of accounts will be carried out based on the risk profile of the customers. The accounts of those customers falling in the high-risk categorisation will get closer attention, reviewing them every 6 months for Politically Exposed Persons (PEPs), 12 months for high risk categorisation whereas customers account with medium and low risk categorisation are reviewed once in 18 months and once in 24 months respectively.

14 ENHANCED DUE DILIGENCE (EDD) FOR HIGH RISK CUSTOMERS

The Bank has implemented an EDD programme for all customers that are classed as high risk following a review of their KYC information by the Branch and MLRO. From our risk assessment, all customers classified as high risk will be subject to EDD. (customers specified in Sec 4.4.2)

EDD procedure includes the following checks:

- Conduct thorough media searches including Google and other media searches. All adverse media information will be referred and reviewed by the competent authority before signing off for account opening.
- Sanctions checks, review all fuzzy matches and record necessary signoffs.
- Source of Funds: Bank will record the source of fund with necessary supporting documents.
- In the cases of HNI or PEP customers, Bank will seek additional information on Wealth by requesting customer to complete Source of Wealth form.

- Verify information provided by customer with the data base available with Chamber of commerce or Company Houses

- Review of ownership structure to clearly identify and record the details of Ultimate Beneficial Owners
- Record KYC information of Settlor, Trustees and beneficiaries in the cases of Trust accounts.
- Seek third party professional confirmation i.e. Incumbency Certificates, certificate of good standing etc issued by Auditors or Solicitors

15 RECORD KEEPING & RECORDS WITHIN THE GROUP

The Bank shall preserve records of customer/ applicant for opening accounts, transactions and remittances for a period, as may be required by the regulatory requirements in a manner that can be easily retrievable and to demonstrate compliance with AML Regulations and to aid resulting investigations. Presently the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the regulations), which transpose the Fourth EU Money Laundering Directive into UK law requires holding and preservation of records of customer/applicant for business for remittances for a period of five years from the date of closure of an account or the last transaction conducted/concluded.

Her Majesty's Revenue & Customs (HMRC) in the UK requires retention and preservation of records for a period of six years for criminal activities relating to tax evasion etc., hence it is the Bank's policy to retain and preserve records for a period of Seven years from the date of closure of a customer account or the last transaction conducted for an applicant for business - remitter.

Such records will be retained either by way of original documents or by way of photocopies of the original documents or in scanned or computerised or electronic form. Records relating to ongoing investigations shall be retained until the relevant Law Enforcement Agency (LEA) has confirmed that the case has been closed.

Where record of the documents provided for verifying the identity of a customer are held by another entity within the Group, the Bank is not required to hold in duplicate copies of such documents. However, the records should be made accessible to the MLRO/CEO on request or should also be provided when they may be called upon by any law enforcement to produce them. Further, in case the relevant entity within the group cease to trade or have a business relationship with such a customer, then the Bank shall ensure that proper handover of the relevant documents is done for its records.

The Bank shall maintain records to cover:

a) Customer information
b) Transactions
c) Internal & external suspicious reports
d) MLRO's annual reports
e) Information not acted upon
f) Training and compliance monitoring
g) Information about the effectiveness of the training

16 TRAINING AND AWARENESS

It is the Bank's policy that all staff members shall receive Anti-Money laundering training as advised in the general guidance on staff awareness, training and alertness as given in Part I, Chapter 7 of JMLSG. In particular:

1. Staff will be made aware of the risks of money laundering and terrorist financing, the relevant legislation and their obligations under that legislation.
2. Staff will be made aware of the identity and responsibilities of the firm's nominated officer and MLRO.
3. Staff will be trained in the Bank's procedures and on how to recognise and deal with potential money laundering or terrorist financing transactions at regular intervals, and details recorded.
4. The MLRO is responsible for oversight of the Bank's compliance with its requirements in respect of staff training, including ensuring that adequate arrangements for awareness and training of employees are in place.
5. All staff members are provided a copy of this policy for reference. The appendix to this policy contains the web links to the various laws and guidance available from the government, Joint Money Laundering Steering Group and the enforcement agencies for further reference.
6. In light of the obligations placed on each individual by the Laws, Regulations and the possible penalties, the MLRO shall ensure that information about these personal obligations is available to all members of staff at all times.

Accordingly the MLRO shall, in co-operation with the Bank's HR department, ensure that training is imparted to members of staff according to their exposure to money laundering risk, at least once a year to maintain awareness and ensure that the Bank's legal obligations are met.

The Bank provides the outsourcing firms used by the Bank awareness training as to their obligations under AML-CFT and Data Protection Act and the same is part of the SLA signed with the outsourcing service provider.

PROCEDURES:

i. The Bank shall run in-house employee training programmes on CDD, so that members of the staff are adequately trained in CDD procedures and in identifying suspicious transactions. The training is also provided to all new employees within one month of joining. Training will be repeated every two years.

ii. In addition the MLRO will, evolve the AML training methods, products and services in order to make suitable training activities available to all members of staff having client contact, or access to client information.

iii. Training will be needs based and take into account:

- the need to achieve a level of knowledge and understanding appropriate to the individual's role in the Bank
- the need to maintain that level through on-going refresher training
- the practicality of assigning different programmes to staff with different roles on a risk-sensitive basis

iv. The training programme will evaluate and confirm that each individual has achieved an appropriate level of knowledge and understanding, either through formal testing, assessment, informal discussion, or other means. The HR department will ensure that all staff members have been trained. The MLRO will keep records of training completed, including the results of tests or other evaluations demonstrating that each individual has achieved an appropriate level of competence. The MLRO shall remind staff of their legal obligations under the law, of their duty to report suspicious transactions /monitoring of transactions and where appropriate impart training on one to one basis or in groups as necessary and invite questions and provide clarifications sought by the staff members in relation to prevention of money laundering.

v. The MLRO will determine the training needs of his own role, and ensure that he/she obtains appropriate knowledge and understanding such as may be required to fulfil the MLRO's obligations.

17 INTERNAL AUDIT

The Bank's internal audit programme is set using a risk based approach and includes periodic audits of the Bank's AML Policies and procedures and adherence thereto.

The Internal Auditor (currently service provided by BDO) will make necessary checks for compliance on Anti-Money Laundering/Combating Terrorist Financing matters and will independently verify against the checklist of various instructions/requirements during the audit.

As part of the internal audit, the internal auditors check for compliance with the MLRO's guidance or instructions on the implementation of AML checks by staff. The internal audit function also contributes towards effective supervision of the proper implementation of AML and CFT procedures, in the following ways:

- Inadequacies if any in the policy and procedures being followed may be observed by the internal audit function. This may be taken up with the MLRO for improving the policy or procedure while review is undertaken.
- Deficiencies in the oversight function, which are recurring may require better attention in the policies or procedures and may be intimated to the MLRO by the internal audit.
- Comments of the internal audit function on suspicious transactions and investigations relating thereto will be made available to the MLRO for remedial action, if required.
- If there is evidence of repeated shortcomings in AML-CFT due to the training not providing adequate guidance on certain issues. Internal audit will report such inadequacies in the training material to the MLRO for updating of the training material.
- Whether the internal reporting of suspicious activity report of the transaction is as per the requirements.
- Whether the MIS reports being generated are providing proper data as envisaged by the MLR 2017 and JMLSG.

The Internal Auditor will submit a report of findings to the Audit Committee of the Board.

18 REVIEW AND UPDATING OF POLICY

This policy shall remain in force and cover all transactions of the Bank and shall be reviewed or updated once every year by the Board or as and when required, as advised by the MLRO, based on the changes in legislation, JMLSG guidance notes and/or FCA's regulatory requirements.

The policy will be reviewed annually after the date of final approval by the Board each year, or at earlier intervals, should there be changes in the regulations or guidelines requiring amendments to the policy. In the circumstances where the policy is not approved by the board before the expiry date, the policy may be extended by the Risk and Compliance Committee of the Board for a further six months.

19 APPENDIX - 1

Websites available for further reference on the laws and guidance are as below:

FATF: The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing.
Web link: http://www.fatf-gafi.org/
European Union Directives: The creation of the Single Market and the breaking down of barriers provides increased opportunities for money laundering and financial crime. European legislation has been adopted to protect the financial system and other vulnerable professions and activities from being misused for money laundering and financing of terrorism purposes. At the international level, the Internal Market Directorate General heads European Commission's delegation to the Financial Action Task Force on Money Laundering, the foremost world body in this area.
Web link: http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm
JMLSG: The Joint Money Laundering Steering Group is made up of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. This is primarily achieved by the publication of industry guidance.
Web link: http://www.jmlsg.org.uk/
MLR 2007: Money Laundering Regulations 2007, is the UK legislation.
Web link: http://www.legislation.gov.uk/uksi/2007/2157/contents/made
MLR 2017: The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) is the UK legislation that came into force on 26 June 2017. They implement the EU's 4th Directive on Money Laundering. In doing so, they replace the Money Laundering Regulations 2007 (MLR 2007) and the Transfer of Funds (Information on the Payer) Regulations 2007 which were previously in force.
Web link: http://www.legislation.gov.uk/uksi/2017/692/contents/made
POCA 2002: Prevention of Corruption Act 2002. A UK legislation.
Web link: http://www.legislation.gov.uk/ukpga/2002/29/contents
NCA: National Crime Agency tackles serious organised crime that affects the UK and our citizens. This includes Class A drugs, people smuggling and human trafficking, major gun crime, fraud, computer crime and money laundering.
Website: http://www.nationalcrimeagency.gov.uk/
SYSC: Systems and Controls handbook of Financial Conduct Authority (FCA), the banking, insurance and financial services regulator in UK.
Web link: http://fshandbook.info/FS/html/FCA/SYSC
Terrorism Act 2000: This is UK legislation.
Web link: http://www.legislation.gov.uk/ukpga/2000/11/contents
The Counter Terrorism Act 2008: This is UK legislation.
Web link: http://www.legislation.gov.uk/uksi/2009/58/contents/made

20 APPENDIX – 2 SUSPICIOUS ACTIVITY REPORTING FORM

UNION BANK OF INDIA (UK) LIMITED
SUSPICIOUS ACTIVIITY REPORT (INTERNAL)
(HIGLY CONFIDENTIAL)

Report From:_____ Date:_____

Department: _____

Customer Name and Account Number:_____

Transaction Details/Situation that aroused your suspicions:

Reason for Suspicions:

_____

Signature of Reporting Staff

(***Beware of Tipping off:*** *Do not inform anyone about this report, including staff members from your department. MLRO will provide acknowledgement for your report on the same working day*).

For MLRO Use: Date and Time Received: _____

21 Annexure – 3 COUNTRY RISK CLASSIFICATION

Scores not provided I think only rankings ?

Lower	Lower - Med	Medium	Med - Higher	High
80 - 100	70 - 80	60 - 70	50 - 60	<50

7. Low risk: 0 – 3.3
8. Medium risk: 3.3 – 6.6
9. High risk: 6.6 - 10

*: Country AML Risk classification as per Know your country AML Risk Ratings - June 2020

	Country	Score
1	Norway	**87.49**
2	Svalbard and Mayen	**87.49**
3	Sweden	**87.46**
4	Åland Islands	**86.75**
5	Finland	**86.75**
6	New Zealand	**85.81**
7	Tokelau	**85.81**
8	Denmark	**85.61**
9	Faroe islands	**85.61**
10	Greenland	**85.61**
11	Estonia	**84.48**
12	Slovenia	**83.81**
13	Bermuda	**83.34**
14	Lithuania	**83.22**
15	Andorra	**82.26**
16	Malta	**82.14**
17	San Marino	**81.89**
18	Austria	**80.03**
19	Croatia	**79.92**
20	Namibia	**78.38**
21	Vatican City State (Holy See)	**77.99**
22	Burkina Faso	**77.83**
23	Germany	**77.80**
24	South Korea	**77.60**
25	France	**77.57**
26	French Guiana	**77.57**
27	French Polynesia	**77.57**
28	Guadeloupe	**77.57**
29	Martinique	**77.57**
30	Mayotte	**77.57**

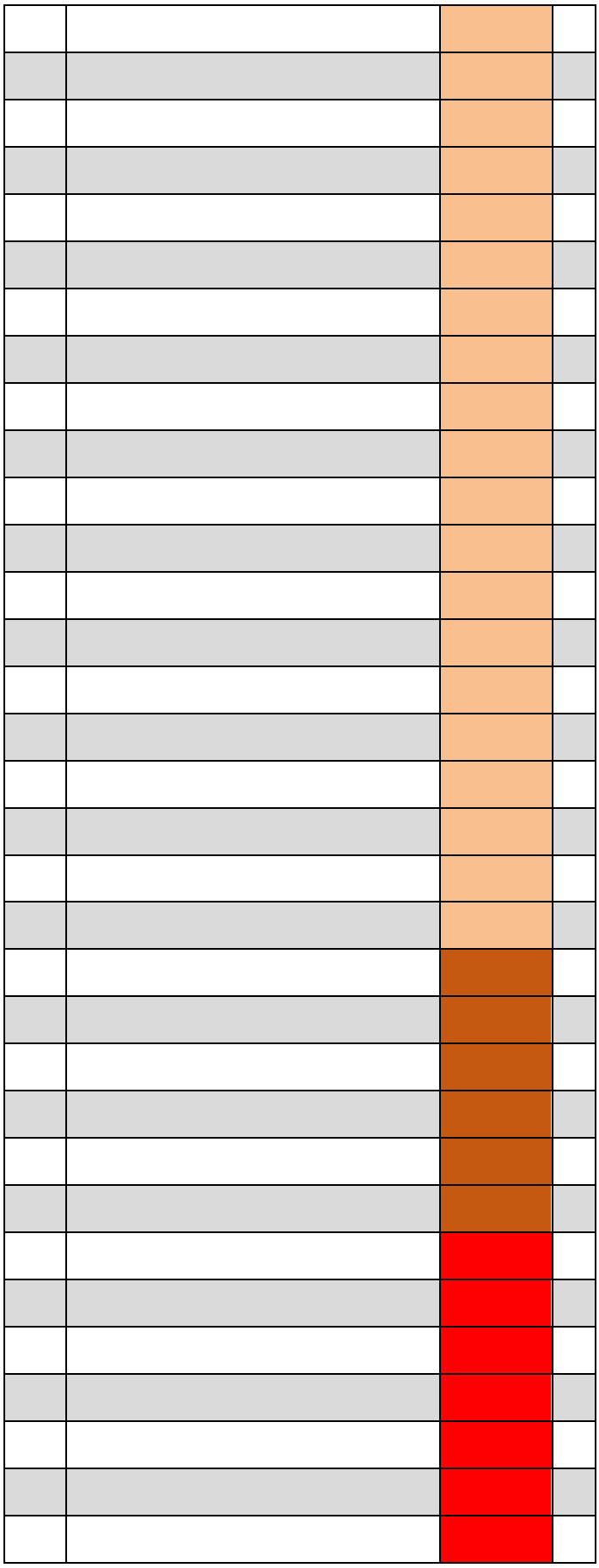
31	New Caledonia	**77.57**
32	Réunion	**77.57**
33	Saint Berthélemy	**77.57**
34	Saint Martin (French part)	**77.57**
35	Saint Pierre and Miquelon	**77.57**
36	Wallis and Futuna	**77.57**
37	Montserrat	**77.55**
38	Anguilla	**77.42**
39	Bhutan	**77.41**
40	Macedonia	**77.24**
41	Rwanda	**77.09**
42	Malawi	**76.94**
43	Brunei Darussalam	**76.91**
44	Singapore	**76.83**
45	Tonga	**76.82**
46	Australia	**76.78**
47	Christmas Island	**76.78**
48	Cocos (Keeling) Islands	**76.78**
49	Norfolk Island	**76.78**
50	Solomon Islands	**76.73**
51	Switzerland	**76.68**
52	Zambia	**76.67**
53	Czech Republic	**76.49**
54	Guernsey	**76.44**
55	Chile	**76.10**
56	Fiji	**76.08**
57	Belgium	**75.90**
58	Latvia	**75.86**
59	Oman	**75.81**
60	Ireland	**75.63**
61	Niue	**75.52**
62	Liechtenstein	**75.43**
63	Greece	**75.38**
64	Jersey	**75.38**
65	Spain	**75.24**
66	Canada	**75.22**
67	Qatar	**75.19**
68	North Mariana Islands	**75.00**
69	United States	**75.00**
70	Luxembourg	**74.78**
71	Poland	**74.74**
72	Taiwan	**74.69**
73	Isle Of Man	**74.65**
74	Portugal	**74.38**

75	British Indian Ocean Territory	**74.29**
76	Falkland Islands (Malvinas)	**74.29**
77	Pitcairn	**74.29**
78	Saint Helena, Ascension and Tristan	**74.29**
79	United Kingdom	**74.29**
80	Hungary	**74.24**
81	Uruguay	**74.10**
82	Lesotho	**73.92**
83	Bulgaria	**73.57**
84	Slovakia	**73.35**
85	Marshall Islands	**73.24**
86	Niger	**73.22**
87	South Africa	**73.17**
88	Micronesia	**73.14**
89	American Samoa	**72.95**
90	Madagascar	**72.91**
91	Togo	**72.84**
92	Nepal	**72.69**
93	Cook Islands	**72.60**
94	Gabon	**72.48**
95	Italy	**72.38**
96	Mauritania	**72.14**
97	Kuwait	**72.14**
98	Gibraltar	**72.02**
99	Bonaire, Sint Eustatius and Saba	**71.92**
100	Netherlands	**71.92**
101	Romania	**71.73**
102	Nauru	**71.65**
103	Papua New Guinea	**71.53**
104	Georgia	**71.52**
105	Sri Lanka	**71.40**
106	Ethiopia	**71.36**
107	Cameroon	**71.35**
108	Monaco	**71.33**
109	United States Virgin Islands	**70.97**
110	Swaziland (Eswatini)	**70.52**
111	Turks & Caicos	**70.41**
112	Congo (Brazzaville)	**70.30**
113	Chad	**70.26**
114	Bahrain	**70.21**
115	Equatorial Guinea	**70.13**
116	Gambia	**70.12**
117	Hong Kong	**70.04**
118	Bangladesh	**69.97**

119	Grenada	**69.92**
120	Iceland	**69.90**
121	Macau	**69.74**
122	Costa Rica	**69.64**
123	Argentina	**69.56**
124	Cyprus	**69.45**
125	Puerto Rico	**69.12**
126	Indonesia	**69.04**
127	Jordan	**68.90**
128	Timor-Leste	**68.88**
129	Saudi Arabia	**68.85**
130	Israel	**68.71**
131	Tuvalu	**68.67**
132	Guyana	**68.66**
133	Aruba	**68.60**
134	United Arab Emirates	**68.38**
135	Maldives	**68.34**
136	Suriname	**68.03**
137	Kiribati	**67.79**
138	Guam	**67.77**
139	Cote D'Ivoire	**67.57**
140	Djibouti	**67.29**
141	Malaysia	**67.23**
142	British Virgin Islands	**67.05**
143	St Kitts & Nevis	**66.85**
144	Sierra Leone	**66.75**
145	Palau	**66.69**
146	Japan	**66.68**
147	Angola	**66.54**
148	Antigua and Barbuda	**66.48**
149	Peru	**66.47**
150	Kazakhstan	**66.32**
151	Sao Tome & Prin.	**66.31**
152	Senegal	**66.02**
153	India	**66.02**
154	Cape Verde	**65.80**
155	Kyrgyzstan	**65.53**
156	St Vincent & Gren	**65.25**
157	Serbia	**65.06**
158	Turkey	**65.04**
159	Seychelles	**64.99**
160	Vanuatu	**64.87**
161	Curacao	**64.80**
162	Algeria	**64.76**

163	Thailand	64.65
164	Dominican Republic	64.63
165	Montenegro	64.62
166	Honduras	64.56
167	Tajikistan	64.46
168	Eritrea	64.42
169	El Salvador	64.39
170	Trinidad & Tobago	64.37
171	Belize	64.17
172	Benin	64.10
173	Uzbekistan	64.03
174	Cayman Islands	63.83
175	Moldova	63.73
176	Mexico	63.72
177	Vietnam	63.46
178	St Lucia	63.44
179	Mauritius	63.39
180	Botswana	63.34
181	Dominica	63.04
182	Colombia	62.99
183	Turkmenistan	62.73
184	Tanzania	62.53
185	Belarus	62.49
186	Kosovo	62.23
187	Paraguay	62.17
188	Armenia	61.50
189	Kenya	61.44
190	Guinea	61.42
191	Mozambique	61.09
192	Mongolia	61.06
193	Samoa	61.05
194	Guatemala	60.50
195	Bolivia	60.17
196	Comoros	60.09
197	Philippines	59.75
198	Tunisia	59.30
199	Morocco	59.30
200	Western Sahara	59.30
201	Cuba	59.27
202	Mali	59.22
203	Lao People's Democratic Republic	59.03
204	Uganda	59.02
205	China	58.61
206	Ecuador	58.35

207	Liberia	56.99
208	Azerbaijan	56.95
209	Egypt	56.75
210	West Bank (Palestinian Territory, Occupied)	56.65
211	Ukraine	56.52
212	Central African Rep	56.51
213	Russian Federation	56.01
214	Brazil	56.00
215	Gaza Strip	55.79
216	Nigeria	55.34
217	St Maarten	54.46
218	Burundi	54.05
219	Albania	53.81
220	Sudan	53.20
221	Cambodia	53.05
222	Barbados	52.20
223	Bahamas	52.17
224	Bosnia-Herzegovina	52.17
225	Jamaica	51.35
226	Ghana	50.65
227	Congo, the Democratic Republic	49.93
228	Guinea Bissau	48.42
229	Haiti	48.09
230	Lebanon	46.31
231	Venezuela	45.83
232	Zimbabwe	44.83
233	Libya	44.68
234	South Sudan	44.52
235	Panama	43.96
236	Iraq	43.57
237	Pakistan	42.74
238	Somalia	37.80
239	Nicaragua	36.79
240	Myanmar	35.94
241	Syria	34.85
242	Yemen	32.84
243	Afghanistan	31.83
244	North Korea	20.80
245	Iran, Islamic Republic of	18.01



22 APPENDIX 4 - Abbreviations

AML	Anti-Money Laundering
CAP	Customer Acceptance Policy
CDD	Customer Due Diligence
CDOT	Crown Dependencies and Overseas Territories
CEO	Chief Executive Officer
CFT	COMBATING THE FINANCING OF TERRORISM
CIP	Customer Identification Procedures
CM	Chief Manager
COO	Chief Operating Officer
CTA	Counter-Terrorism Act
DMS	Data Management System
ED	Executive Director

EDD	Enhanced Due Diligence
EEA	European Economic Area
EU	European Union
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
HMRC	Her Majesty's Revenue & Customs
HMT	Her Majesty's Treasury
HNI	High net worth individuals
JMLSG	Joint Money Laundering Steering Group
KYC	Know Your Customer
LEA	Law Enforcement Agency
MD	Managing Director
MLRO	Money Laundering Reporting Officer
MSB	Money Services Business
NCA	National Crime Agency
PEP	Politically Exposed Person
POCA	Proceeds of crime act
RCC	Risk and Compliance Committee
RMP	Risk Mitigation Programme
SAR	Suspicious Activity Reporting
SME	Small and Medium Size Enterprises
UBO	Ultimate Beneficial Owners