EximPe

KYC/Customer Onboarding/AML Policy

EximPe

Document Classification:	**Public**
Version:	**1.0**
Dated:	**27-01-2024**

Revision History

Version	Date	Summary of Changes	Revision Author	Reviewed by	Approved by
1.0	**27-01-2024**	First Release	Syed	Batul	Board of Directors

EximPe

A. INTRODUCTION

A.1 Les Amis Private Limited ("EximPe") is committed to combating money laundering, financial fraud, and other financial crimes (collectively "Money Laundering") and complying fully with all applicable laws and regulations relating to combating money laundering. EximPe is also committed to complying with economic and trade sanctions administered and enforced by the government and supranational bodies, including, among others, the sanctions programs and designated sanctions lists administered by our supervisory.

A.2 In accordance with the Reserve Bank of India's ("RBI") "Regulation of Payment Aggregator – Cross Border" issued vide CO.DPSS.POLC.No.S-786/02-14-008/2023-24 dated October 31, 2023 ("PA-CB Guidelines") read with the "Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2020" issued vide DPSS.CO.PD.No.1810/02.14.008/2019-20, dated March 17, 2020, (the "PA Guidelines"), the Know Your Customer ("KYC")/Anti-Money Laundering ("AML")/ Combating Financing of Terrorism ("CFT") guidelines issued by the Department of Regulation, RBI, in the "Master Direction - Know Your Customer Directions, 2016" ("KYC Master Directions") is applicable to all cross border payment aggregators ("PA-CB"). Provisions of Prevention of Money Laundering Act, 2002 and Prevention of Money Laundering (Maintenance of Records) Rules, 2005 framed thereunder, as amended from time to time, are also applicable. PA-CBs are also required to have a board of directors ("Board") approved policy for Customer onboarding.

A.3 The clarifications to the PA Guidelines, issued vide RBI/2020-21/117, dated March 31, 2021, further clarify that there would not be a requirement to carry-out the entire KYC process (in accordance with the KYC Master Directions), in cases where the Customer already has a bank account which is being used for transaction settlement purpose.

A.4 EximPe intends to apply strict guidelines for onboarding its Customers and in relation to undertaking business with its partners or merchants, in compliance with applicable regulations mentioned above.

A.5 RBI mandates PA-CBs to ensure that a proper policy framework on "Know Your Customer" and "Anti-Money Laundering" measures with the approval of the Board be formulated and put in place.

A.6 The information contained in this guide will provide you with an understanding of our KYC Policy and AML Compliance Program (the 'KYC/AML Policy') that meets the requirements of our local supervisory authority. This guide is designed to help -

(a) Understand our responsibility as an RBI regulated entity;

(b) Comply with the RBI's policies and applicable AML regulations;

(c) Identify suspicious activity and transactions; and

(d) Document protocols and principles for Customer acceptance, Customer identification, transaction monitoring, and risk management.

This policy must be read in line with the relevant guidelines issued by the RBI, as amended from time to time and in case of any conflicts/clarification, applicable RBI guidelines shall be referred and followed.

B. OBJECTIVE

B.1 The aim of this KYC/AML Policy is:

(a) To determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business;
(b) To prepare and implement globally accepted standards/policies, Customer risk scoring, onboarding, and maintenance of Customer data with EximPe;
(c) To prepare and implement globally accepted standards/policies for monitoring and identifying unusual or suspicious transactions or patterns of suspicious activities;
(d) To prevent all types of criminal elements from dealing with EximPe for any money laundering activities;
(e) Organize systems for suspicious activity reports, suspicious transaction reports and currency transaction reports and submitting the same with regulators and law enforcement agencies including the Financial Intelligence Unit – India ("FIU-IND").

B.2 More specifically, EximPe shall undertake the following:

(a) Comply with applicable KYC & AML regulations;
(b) Establish standard operating procedures for customer acceptance;
(c) Customer identification & agreements;
(d) Transaction monitoring reporting and AML risk monitoring.

B.3 The policy is applicable to all the branches, shareholders, board of directors, employees, Customers, business correspondents/agents/ sales executives of entities doing business with EximPe and any other person involved with any process envisaged under this KYC/AML Policy ("Obligated Persons").

B.4 In the event, an employee fails to comply with this KYC/AML Policy, such an employee will be subject to disciplinary proceedings which may lead to dismissal of such an employee. Any act of disobeying this policy will be reported to the relevant regulatory authorities (as applicable) who may also take criminal action against such an employee.

C. APPLICABLE REGULATIONS

C.1 EximPe has considered the following legislations, regulations, guidelines to prepare this policy:

(a) Payments & Settlement Systems Act, 2007;
(b) Prevention of Money Laundering Act, 2002 and Prevention of Money Laundering (Maintenance of Records), Rules, 2005;
(c) Aadhaar (Target Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 and related regulations;
(d) RBI Master Directions on Know Your Customer (KYC) Direction, 2016;
(e) RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2020 dated March 17, 2020 read with clarifications to these Guidelines dated March 31, 2021; and
(f) RBI Regulation of Payment Aggregator – Cross Border (PA - Cross Border) dated October 2023.

D. SUPERVISORY FRAMEWORK

D.1 EximPe shall supervise the implementation of this KYC/AML Policy in-house and such supervisory function shall not be outsourced to any consultant or third-party vendor. The supervisory framework is as outlined below:

(a) The Board of EximPe has identified Arjun Abraham Zachariah as the Designated Director and Deepak Chandel as the Principal Officer, who shall primarily be responsible for the implementation of this KYC/ AML Policy. EximPe shall inform the details of the Designated Director and Principal Officer to the FIU-IND.
(b) The Operations team of EximPe shall be responsible for ensuring the effective implementation of this policy and the procedures laid down therein.
(c) The Board or any other committee to whom the power has been delegated shall carry out the internal audit on periodical basis to verify compliance with this policy.

D.2 The role of the Designated Director shall be to oversee compliance as per the obligations imposed by the PML Act and PML Rules.

D.3 The Principal Officer shall render the following services:

(a) To ensure compliance with the Prevention of Money Laundering Act, 2009 and amendment thereof;
(b) To provide updates to business units about the updated money laundering laws;
(c) To identify gaps from and propose changes in the product/processes/systems;
(d) To conduct training of the business units and other related verticals about the KYC/ AML Policy.
(e) To issue guidelines, procedures to the various department for implementation of this KYC/ AML Policy.

(f) Implement and manage generation of the alerts for suspicious transactions and reporting such transactions to the Director - FIU-India;
(g) Review periodically, the effectiveness of the implementation of procedures with respect to KYC and AML guidelines and provide updates and recommendations to the Board of Directors.

Note: For ease of reference, this KYC/ AML policy has been broadly categorized into 2 parts:
- Customer On-boarding Policy & KYC (outlines pre-onboarding checks) specified and detailed in paragraph E below; and
- AML Policy & Post On-Boarding Checks (outlines post-onboarding checks) specified and detailed in paragraph F below.

E. CUSTOMER ON-BOARDING AND KYC POLICY

E.1 EximPe's Customer On-Boarding and KYC Policy includes following four key elements:

(a) Customer Acceptance
(b) Risk Management
(c) Customer Identification Procedures ("CIP"); and
(d) Monitoring of Transactions

Note: Monitoring of Transactions is covered under "AML Policy and Post On Boarding Checks" provided under Paragraph F of this KYC/AML Policy.

E.2 For the purpose of this policy, "Customer" refers to the exporters or importers who approach the EximPe platform for cross border transaction facilitation and "account" refers to the EximPe dashboard account created on the EximPe platform for the services that the Customer has opted for.

E.3 Customer Acceptance

(a) EximPe shall ensure the following:

(i) No account is opened in an anonymous or fictitious/benami name.
(ii) A standard Customer identification procedure to be put in place and the same should be adhered to before opening an account.
(iii) No account is opened where EximPe is unable to apply appropriate 'Customer Due Diligence' ("CDD") measures as described herein.
(iv) No transaction is undertaken without following the CDD procedures as described herein.
(v) Optional/additional information may be obtained with the explicit consent of the Customer after the account is opened.
(vi) The Customer shall not ordinarily be permitted to act on behalf of another person/entity. If permitted, then the specific circumstances in which a Customer is

permitted to act on behalf of another person/entity must be clearly specified in the terms and conditions of usage of the EximPe platform.

(vii) A suitable system is put in place to ensure that the identity of the Customer does not match with any person or entity whose name appears in the sanctions lists circulated by the RBI and .

(viii) There can be no business relations with any Customer whose name appears in the sanctions lists or who is suspected of having terrorist links.

(ix) At the time of onboarding, EximPe must require the Customers to disclose the exact business category/business sub-category for which such Customer will be using the EximPe Services.

(x) EximPe must verify to its fullest capacity that entities are duly constituted in accordance with the law and operate the bonafide business by checking the product listing, terms & conditions, refund policy, etc.

(xi) EximPe will accept new Customer relationships & extend existing relationships in all products of EximPe only after evaluating regulatory as well as internal guidelines.

(xii) EximPe will ensure that these policies are detailed in the form of operational guidelines/procedures/instructions & these would be widely circulated to all staff to ensure satisfactory services to the Customer. The EximPe will ensure the implementation of well-laid guidelines and processes.

(b) EximPe will put in place the following requirements for Customer acceptance and severance:

(i) For any new or existing relationship, KYC information will be verified as defined herein under the “Customer due diligence (CDD) & periodic review” section of the policy provided under paragraph E.6 below. No transaction or relationship is undertaken without following the CDD procedure.

(ii) CDD process will be applied at the Customer level across EximPe. Thus, if an existing compliant Customer desires to engage in another relationship, there shall be no need for a fresh CDD exercise.

(iii) PAN number obtained from the Customer will be verified through the issuing authority: When an e-document is obtained from the Customer, the digital signature on the document will be verified.

(iv) ‘Beneficial owner’ shall be identified & verified necessarily while initiating a relationship with a non-individual.

(v) EximPe will conduct a review of the Customer at a regular frequency. In the event behavior of the Customer is in contravention to the extant regulatory guidelines e.g. AML or transaction pattern not matching with the profile or non-compliance to periodic review requirements by the Customer, etc. (list is not exhaustive), EximPe shall take necessary steps to intimate the Customer with a request to provide relevant responses/documents. In the event that the Customer is unable to provide appropriate evidence, or the Customer is not traceable beyond a reasonable period, EximPe will follow a risk-based approach to cease the relationship after issuing notice.

(vi) EximPe shall perform checks with regards to the line of business and industry before on-boarding a Customer.

(vii) EximPe will not accept any Customer who participates in illegal business/Industry or pose an extremely high risk that cannot be mitigated with available measures in place. An indicative list of such businesses and industries are listed down in 'Annexure II - Unqualified/Unacceptable Businesses' and will be updated by the Principal Officer from time to time.

(viii) EximPe shall not onboard any Customer who participates in export or import of any prohibited items as stated in Annexure 6.

(ix) EximPe may accept Customers who participate in relatively high-risk business/industries. However, EximPe will make sure to apply elevated/enhanced due diligence measures to mitigate ML/FT risks. These businesses and industries are listed down in 'Annexure 2 - High-Risk Businesses' and will be updated by the Principal Officer from time to time.

E.4 Risk Management

(a) EximPe has a risk-based approach for risk management that seeks to identify, manage, and analyze AML/CFT risk to design and effectively implement appropriate controls. As such, it is critical that risk ratings accurately reflect the risks present; provide meaningful assessments that lead to practical steps to mitigate the risks; are periodically reviewed and, when necessary, are updated.

(b) A risk-based analysis includes appropriate inherent and residual risks at the country, sectoral, legal entity, and business relationship level, among others. As a result of this analysis, EximPe develop a thorough understanding of the inherent risks in its Customer base, products, delivery channels, and services offered (including proposed new services) and the jurisdictions within which it or its Customers do business. Risks arising from the deficiencies in the AML/CFT regime of the jurisdictions included in the FATF Statement are also considered.

(c) This understanding should be based on operational, transaction and other internal information collected by the institution, as well as external sources.

(d) AML/CFT risk categories shall be broken down into the following levels:

(i) Prohibited - EximPe will not tolerate any dealings of any kind in this category given the risk. This category could include transactions with countries subject to economic sanctions or designated as state sponsors of terrorism, such as those on the United Nations or Office of Foreign Assets Control lists.

- High Risk - The risks here are significant but are not necessarily prohibited. To mitigate the heightened risk presented, EximPe should apply more stringent controls to reduce the ML/CFT risk, such as conducting enhanced due diligence and more rigorous

transaction monitoring. Countries that maintain a reputation for corruption or drug trafficking are generally considered high-risk. High-risk Customers may include politically exposed persons or certain types of money services businesses or cash-intensive businesses; high-risk products and services may include correspondent banking and private banking.

(ii) Medium Risk - Medium risks require additional scrutiny, but do not rise to the level of high risk. For example, a retail business accepts low to moderate levels of cash but is not considered cash Intensive.

(iii) Low Risk - This represents the baseline risk of money laundering. Typically, low risk indicates normal, expected activity.

Customer rating guidelines based on risk framework used at the time of onboarding and as a part of subsequent due diligence is detailed in Annexure 5

E.5 Customer Identification Procedures

(a) For Customer identification, EximPe verifies KYC documents as outlined herein based on the type of Customer entity. This also includes beneficial owner checks, name screening and enhanced due diligence for high-risk Customer categories. EximPe also has a right to obtain additional documents and details if required.

(b) As per the PA-CB Guidelines read with the PA Guidelines, PA-CBs are required to have a Board approved policy for Customer on-boarding. Further, PA-CBs are not required to carry-out the entire process of KYC (in accordance with the KYC guidelines), in cases where the Customer already has a bank account which is being used for transaction settlement purposes. In view of this stance, this section outlines a non-exhaustive list of additional Customer checks and due diligence measures conducted by EximPe. These are carried out in addition to reliance placed on the documentation verification already carried out by the banks for the Customers at the time of establishing an account-based relationship.

(c) The nature of information/documents required would depend on the type of Customer. For Customers who are natural persons, EximPe shall obtain sufficient identification data to verify the identity of the Customer, the address/ location.

(d) If the Customer is a legal person or entity EximPe shall verify the legal status of the person or entity through the documents that are relevant and are submitted by them and verify that any person purporting to act on behalf of the legal person or entity is so authorised and identify and verify the identity of that person

E.6 Customer Due Diligence

(a) Customer due diligence ("CDD") means:

(i) identifying the Customer and verifying the identity on the basis of documents, data or information obtained from the Customer and cross checking the same, where relevant, from a reliable and independent source;
(ii) identifying the Customer's beneficial owner and taking reasonable measures to verify their identity and that of the authorized signatories so that it is known who the beneficial owner is;
(iii) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
(iv) conducting ongoing monitoring of the business relationship. This includes transaction monitoring and keeping the underlying information up to date.

(b) EximPe shall apply any one or combination of below-mentioned verification processes for any Customer on boarded

(i) KYC documentation and verification - A standard process to collect and verify the officially valid documents ("OVDs") or constitutional documents of Customers as per KYC checklist below.

(ii) System-level checks - Which includes verification of documents through government sources like, PAN from NSDL, Documents/Information for Corporates from MCA website, documents/information from regulatory or government website/database like GST, etc;

(c) The verifications carried out are outlined below. Additional verifications may also be carried out based on Customer risk levels, etc.

(i) Entity Wise Documentation

The Customer identification requirements as mentioned in Annexure 1 may be relied upon for Customer Identification.

(ii) Standard Due Diligence ("SDD")

SDD is applicable to low/medium risk Customers, those who are permanent residents of India with a transparent source of income and simple legal structure. KYC information may vary based on the type of legal structure of the Customer, for example, company, partnership, trust, etc.

Actual checks conducted vary based on the specific Customer, his constitution type, etc. More details on due diligence checks conducted, including enhanced due diligence for high-risk Customers to be conducted both pre and post onboarding are listed in "AML

Policy and Post On Boarding Checks" provided under Paragraph F of this KYC/AML Policy.

(iii) Other Measures

 Politically Exposed Persons ("PEP")

- To establish a PEP relationship for individuals or beneficial owners of legal entities: information about the sources of funds, accounts of family members and close relatives will be gathered;
- The identity of the person will be verified before accepting the PEP as a Customer;
- The decision to open an account for a PEP is taken at a senior level in accordance with EximPe's Customer Acceptance Policy;
- These accounts will be subjected to enhance monitoring on an on-going basis;
- In the event of an existing Customer or the beneficial owner of an existing account subsequently becoming a PEP, Enhanced Due Diligence is performed, and senior management's approval is obtained to continue the business relationship.

 Adverse Media

Customers with a negative reputation as per public information available or commercially available watch lists (not part of sanction or terrorist lists such as UN/MHA, where Customer risk is high). will be on-boarded post obtaining enhanced due diligence information as outlined in "AML Policy and Post On Boarding Checks" provided under Paragraph F of this KYC/AML Policy.

 Accounts Opened Through Professional Intermediaries

EximPe may also on-board the Customer through professional intermediaries, with the below conditions:

- Customers shall be identified when a Customer account is opened by a professional intermediary on behalf of a single Customer.
- All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of EximPe, and there are 'sub-accounts, each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of EximPe, the EximPe shall look for the beneficial owners.
- EximPe shall, at their discretion, rely on the 'Customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the Customers.
- The ultimate responsibility for knowing the Customer lies with EximPe.

(iv) Screening

EximPe will conduct name screening against watch lists for all existing Customers and their beneficial owners and key controllers at least once on a daily basis against the incremental watchlist database, regardless of the due diligence cycle. For name screening, EximPe will use the list of FATF, UK HMT/UN/ SDN/EU/ OFAC. FATF statements circulated by RBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, is also considered for screening purposes.

In addition to sanctions, EximPe also expands the search for other risk categories such as PEPs, counterfeit, copyright infringement, money laundering, tax offenses, fraud, identity thefts, etc. in accordance with KYC Master Directions, Reserve Bank of India rhat requires financial institutions, as well as certain non-financial institutions, to have internal systems in place to control account opening and ongoing transactions with PEPs (including their related persons).

F. **AML Policy and Post On-Boarding Checks**

F.1 Money Laundering

(a) Money laundering involves taking criminal proceeds and disguising their illegal sources in order to use the funds to perform legal or illegal activities. When a criminal activity generates substantial profits, the individual or group involved must find a way to use the funds without drawing attention to the underlying activity or persons involved in generating such profits. Criminals achieve this goal by disguising the source of funds, changing the form, or moving the money to a place where it is less likely to attract attention.

(b) Formed in 1989, the Financial Action Task Force ("FATF") is an inter-governmental body comprising the group of seven industrialized nations to set standards and foster international action against money laundering. One of FATF's early accomplishments was to dispel the notion that money laundering is only about cash transactions. Through several money laundering "typologies" exercises, FATF demonstrated that money laundering can be achieved through every medium, financial institution, or business.

(c) Money Laundering can involve any of the following:

(i) The conversion or transfer of property, knowing it is derived from a criminal offense, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his or her actions.

(ii) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property knowing that it is derived from a criminal offense.

(iii) The acquisition, possession, or use of property, knowing at the time of its receipt that it was derived from a criminal offense or from participation in a crime.

(d) Money laundering often involves a complex series of transactions that are difficult to separate. However, it is common to think of money laundering as occurring in three stages:

(i) Stage One: Placement – The physical disposal of cash or other assets derived from criminal activity. During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos, and other legitimate businesses, both domestic and international.

Examples of placement transactions include:

- Blending of funds: Commingling of illegitimate funds with legitimate funds such as placing the cash from illegal narcotics sales into cash-intensive locally owned restaurant.
- Foreign exchange: Purchasing of foreign exchange with illegal funds.
- Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade reporting requirements.
- Currency smuggling: Cross-border physical movement of cash or monetary instruments.
- Loans: Repayment of legitimate loans using laundered cash.

(ii) Stage Two: Layering – The separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds.

This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and ownership of funds.

Examples of layering transactions include:

- Electronically moving funds from one country to another and dividing them into advanced financial options and or markets
- Moving funds from one financial institution to another or within accounts at the same
- institution
- Converting the cash placed into monetary instruments
- Reselling high value goods and prepaid access/stored value products
- Investing in real estate and other legitimate businesses
- Placing money in stocks, bonds, or life insurance products
- Using shell companies to obscure the ultimate beneficial owner and assets

(iii) Stage Three: Integration – Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions.

This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures, or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth. This stage provides a launderer the opportunity to increase his wealth with the proceeds of crime. Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate employment, business or investment ventures and a person's wealth or a company's income or assets.

Examples of integration transactions include:

- Purchasing luxury assets like property, artwork, jewellery, or high-end automobiles
- Getting into financial arrangements or other ventures where investments can be made in business enterprises

F.2 Anti-money Laundering Compliance Program

(a) An anti-money laundering/counter-terrorist financing program (AML/CFT program) is an essential component of a financial institution's compliance regime. The primary goal of an AML/CFT program is to protect the organization against money laundering, terrorist financing and other financial crimes and to ensure that the organization is in full compliance with relevant laws and regulations. For that reason, designing, structuring, and implementing these programs should be the top priorities of any financial institution

(b) An AML/CFT program should be risk-based:

- Flexible as money laundering and terrorist financing risks vary across jurisdictions, Customers, products, and delivery channels, and over time.

- Effective as companies are better equipped than legislators to effectively assess and mitigate the particular money laundering and terrorist financing risks they face.

- Proportionate because a risk-based approach promotes a common sense and intelligent approach to fighting money laundering and terrorist financing as opposed to a "check-the- box approach. It also allows firms to minimize the adverse impact of anti-money laundering procedures on their low-risk Customers.

(c) EximPe adopts an AML Compliance Program designed to ensure proper record keeping and reporting of certain transactions and to prevent any Customer from using our platform to launder money.

(d) Our AML Compliance Program includes the following:

- Adoption of a written AML program with internal policies, procedures, and controls for:

  - Verifying Customer identification
  - Compliance with regulatory requirements
  - Filing reports as required by our local regulations, as required under law
  - Creating and retaining records
  - Responding to law enforcement requests
  - Employee's Compliance training

- An ongoing employee training program that:

  - Explains policies and procedures
  - Teaches how to identify suspicious activity
  - Trains and educates employees around ways to identify such activity
  - Trains on filing reports as required by regulations

F.3 On-going Diligence and Transaction Monitoring

(a) EximPe shall, on an ongoing basis, undertake due diligence of Customers to ensure that their transactions are consistent with their knowledge about the Customers, Customers' business and risk profile, and the source of funds.

(b) EximPe shall implement numerous velocity checks.

(c) EximPe's risk team shall be very vigilant and shall constantly be watching transactions where any seems unusual or suspicious. If found suspicious, EximPe shall reach out to the Customer for an explanation. If the Customer can provide valid explanations along with documentary evidence, EximPe shall evaluate those.

(d) Close monitoring of the following types of transactions shall necessarily be done:

(i) Large and complex transactions and those with unusual patterns, inconsistent with the normal and expected activity of the Customer, which have no apparent economic rationale or legitimate purpose.

(ii) Transactions that exceed the thresholds prescribed for specific categories of accounts.

(iii) High account turnover inconsistent with the size of the balance maintained.

(iv) High-Volume Frequency: Scrutinize accounts with frequent high-value transactions within short periods.

(v) High-Risk Country Transactions: Flag transactions involving countries known for higher money laundering risks.

(vi) Politically Exposed Persons (PEPs): Enhanced monitoring for transactions involving PEPs.

(vii) Structuring/Layering Behaviors: Monitor for small, frequent transactions that cumulatively amount to large sums. This includes repetitive deposits or transfers below the reporting threshold and rapid fund movements across accounts, suggesting attempts to avoid detection. Such activities often require closer scrutiny to ensure they aren't part of a money laundering scheme.

(e) The extent of monitoring shall be aligned with the risk category of the Customer. High-risk accounts will be subjected to enhanced monitoring.

F.4 Enhanced Due Diligence Procedure

(a) EximPe shall perform due diligence which may differ from category to category, depending upon the Money Laundering/Terrorist Financing risks posed by different categories of Customers:

Risk categorization	Type of due diligence
Low risk	Standard due diligence ("SDD")
Medium risk	Standard due diligence ("SDD")
High risk	Enhanced due diligence ("EDD")

SDD has been discussed previously in Paragraph E of this KYC/AML Policy. EDD is applied on higher risk Customers, those who have a complex legal structure. Additional KYC & business information is required to verify the identity of the Customer and the services rendered. This activity is performed, pre and post onboarding of the Customers and it's ongoing in nature subject to risk existing or updated triggers.

(b) Examples of enhanced due diligence checks that shall be conducted are as follows: EximPe's understanding on performing EDD is divided into two parts "ie Pre & Post":

(i) Pre Onboarding EDD:

- Financial stability & compliance status of the Customer shall be evaluated for specific businesses and to support the investigation, EximPe shall seek submission of the TDS & GST filing documented proof for the current & previous financial years, in addition the company's standing will also be collected.

- Adverse media screening shall be performed for all the Customers under this queue. Tools used to support the investigation is [●] and the information available in the public registry i.e. Gst.gov, MHA updates, MCA master data & annual filing details, RBI updated list of NBFCs, SEBI, IRDA notifications and so on, also screening of the credentials in the public domain is conducted "i.e. social media and Google keywords".

(ii) Post Onboarding EDD

- Ongoing due diligence is performed for the Customer accounts triggered due to various parameters built on inhouse risk tools, some of these are as follows:

- International Transaction Monitoring: Focus on the patterns and volumes of cross-border transactions for both buyers and sellers.
- Buyer/Seller based AML alerts from AML Screening tools
- Cross-Border High-Value Transaction Tracking: Monitor for transactions that have significantly high values, as they may indicate unusual or potentially risky activities in international trade.
- Surge in International Transactions: Alert systems for accounts showing an unexpected increase in cross-border transaction activity.
- Global Account Dormancy Analysis: Monitor accounts that have been inactive but suddenly initiate or receive international transactions.

F.5 Periodic Updation

(a) Periodic updation shall be conducted at pre-defined periodic intervals, which preferably is, at least once a year for high-risk Customers, once in every eight years for medium-risk Customers, and once in every ten years for low-risk Customers.

(b) Customers other than individuals

(i) No change in KYC information: In case of no change in the KYC information of the Customer, a self-declaration in this regard shall be obtained from the Customer through its registered email id, digital channels (such as online website access/

mobile application), a letter from an official authorized by EximPe in this regard, board resolution, etc. Further, EximPe shall ensure during this process that beneficial ownership information available with them is accurate and shall update the same, if required, to keep it as up to date as possible.

(ii) Change in KYC information: In case of change in KYC information or in cases where any of the CDD documents have expired at the time of updation, EximPe shall undertake the KYC process equivalent to that applicable for onboarding a new Customer.

F.6 Transaction Monitoring:

(a) The purpose of transaction monitoring is to ensure that transactions are consistent with the Customers' profile and source of funds and alert any proceeds of crime and a risk of funds being used for criminal activities related to money laundering/terrorist financing. The main focus of the transaction monitoring process will be on AML, sanctions, due diligence, alert analysis, and fraud control.

(b) While there is no exhaustive list of tried-and-true suspicious activity indicators for businesses, there are many common indicators of financial crime, money laundering and terrorist financing activity. Methods of money laundering have become more sophisticated as the complexity of financial relationships has grown and paths through which funds move worldwide through financial institutions have multiplied. There is also a concern over worldwide terrorist threats.

(c) Financial Institutions and NBFCs play a critical part in efforts to disrupt movement of funds used to support and carry out terrorist attacks. Although it may be difficult to detect terrorist financing transactions, there is guidance available from a variety of authoritative sources. Red flag indicator guidance should be used when building out or refining transaction monitoring programs.

(d) EximPe shall continuously monitor all the Customers' transactions for any abnormal or suspicious Customer behaviour or transaction patterns, bypassing transactions through a transaction monitoring tool.

(e) Transaction Monitoring rules will be customized based on patterns observed for the Customer and all the red flag indicators/criteria all the rules will be reviewed on an ongoing basis to reduce false - positive alerts & implement new areas of risk. All suspicious cases shall be reported as per the FIU-IND guidelines. The rules will be approved by Principal Officer (Head, Compliance).

(f) For export and Import transactions, it shall be carried out after collecting relevant documents based on the purpose code for which the export import transaction is made.

The checks for trade transactions performed is listed under Annexure 4.

F.7 Rejecting/Terminating Business Relationship

(a) Customer relationships may be rejected in case of a suspicion that the aim of establishing the relationship was ML/TF.

(b) A Customer relationship may be rejected or terminated on the occurrence of the following events, including but not limited to:

(i) Where CDD measures are not possible to be performed on a Customer.
(ii) Positive hit against applicable sanctions watchlist.
(iii) Where documentation or identity is identified as potentially counterfeit or forged.
(iv) Where a Customer is identified as being directly or indirectly associated with terrorists or terrorist activity.
(v) Where a Customer is identified as directly or indirectly involved in corruption, crime, or tax evasion.
(vi) If during the CDD process, & turns out that the Customer is having exposure to any sanctioned countries, transactions should not be processed, and the agreement may be terminated with immediate effect.
(vii) Record the reason and the rationale for declining or terminating an existing relationship.

(c) All exit decisions taken by the Risk Monitoring team will be notified to the Principal Officer along with the detailed rationale and screening reports. In instances where a relationship is being exited because of ML/TF or sanctions suspicions, the Onboarding team along with the Principal Officer should consider informing the relevant authorities via a Suspicious Activity Report (SAR).

(d) All declined/terminated Customers will be added to the internal blacklist to avoid any future relationships.

F.8 Partial Freezing and Closure of Accounts

(a) Partial freezing and closure of accounts are mandated under certain conditions such as follows:

(i) Where EximPe is unable to comply with the CDD requirements mentioned above, EximPe shall not open accounts, commence business relations or perform transactions.

(ii) As an exception to the rule, EximPe shall have an option to choose not to terminate the business relationship straight away and instead opt for a phased closure of operations in this account as explained below:

- The option of partial freezing shall be exercised after giving due notice to Customers to comply with KYC requirements/other regulations.
- A reminder giving a further period may also be given.
- Thereafter, partial freezing shall be imposed by allowing all credits and disallowing all debits with the freedom to close the accounts in case of the account being KYC non-compliant after six months of issuing the first notice.
- All debits and credits from/to the accounts shall be disallowed, in case of the account being KYC non-compliant after six months of imposing 'partial freezing'.
- The account holders shall have the option to revive their accounts by submitting the KYC documents.

F.9 Record Management

(a) The following steps shall be taken by EximPe regarding maintenance, preservation, and reporting of Customer account information, with reference to provisions of the PML Act and Rules.

(i) maintain all necessary records of transactions between EximPe and the Customer, both domestic and international, for at least five years from the date of the transaction.

(ii) preserve the records pertaining to the following, for at least five years after the business relationship is ended

- identification of the Customers or their business and their addresses obtained while opening the account and during the course of the business relationship; and
- written findings together with all documents related to the background and purpose of transactions with Customers from jurisdictions included in FATF statements and that do not or insufficiently apply the FATF recommendations.

(iii) make available the following records to the competent authorities upon request:

- identification records;
- transaction data; and
- findings related to the background and purpose of transactions with Customers from jurisdictions included in FATF Statements and that do not or insufficiently apply the FATF Recommendations.

(iv) maintain all necessary information in respect of transactions proscribed under PML Rule 3 to permit reconstruction of an individual transaction, including the amount of the transaction and the currency in which it was denominated and the date on which the transaction was conducted.

(v) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

(vi) maintain records of the identity and address of their Customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

F.10 REGULATORY REPORTING

(a) FIU-IND

(i) As required by Section 12 of the PMLA, the EximPe shall report information of transactions referred to in clause (a) of sub-section (1) of section 12 of the PMLA read with Rule 3 of the PMLA Rules relating to cash and suspicious transactions, etc. to the Director, FIU-IND.

(ii) The provision to the said section also provides that where the Principal Officer has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value to defeat the provisions of the section, information in respect of such transactions will also be provided to the FIU-IND within the prescribed time.

(iii) If any suspicious activity is noticed for a Customer, Suspicious Transaction Report (STR) /Suspicious Activity Report (SAR) shall be filed with FIU-IND for the transaction settlement related to that particular Customer. Furthermore, the assets on the account are to be frozen in the case Customer has Sanctions exposure.

(iv) EximPe will keep a register of suspicious transactions related to its businesses. Principal Officer/Legal & Compliance department on being satisfied that the transaction is suspicious will have the same reported within 7 working days to the FIU-IND. In the case of transactions concerning frauds, EximPe will also inform the relevant police units and other (law enforcement) units.

(v) EximPe will not inform the Customer or any other unauthorized persons that a transaction has been reported as a suspicious transaction or that FIU-IND and/or RBI have been informed about a suspicious transaction. EximPe should block funds and transactions whenever:

- A transaction is deemed suspicious.
- Customer is having a positive Sanctions match or has Sanctions exposure; or
- A request to block Customer funds is made by any regulatory body or law enforcement agency.

(b) Reporting to Other Agencies

Reporting to other criminal investigations, tax authorities, government bodies, enforcement agencies and judicial bodies will be done as and when asked for, on need basis.

(i) Reporting Requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

EximPe shall ensure process to be implemented in place for undertaking reporting under FATCA and CRS as prescribed under RBI KYC Master Directions

(ii) Reporting Requirements Obligations Under International Agreements and Communications from International Agencies

- A suitable mechanism through appropriate policy framework is developed for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit - India (FIU-IND) on priority.
- The EximPe will ensure to update the consolidated list of individuals and entities approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRS) circulated by the Reserve Bank.
- The ISIL (Da'esh) & Al-Qaida Sanctions List and '1988 Sanctions List will be considered for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967. The EximPe will update the lists of individuals/ entities as circulated by Reserve Bank and before opening any new account will ensure that the name/s of the proposed Customer does not appear in either list.
- Further all existing accounts are scanned to ensure that no account is held by or linked to any of the entities or individuals included in the two lists as mentioned above. Full details of accounts bearing resemblance with any of the individuals/ entities in the list will immediately be intimated to the RBI and FIU-IND.

F.11 Escalation and Reporting to Senior Management

(a) This process shall be triggered by any findings made during the execution of the CDD process, which raises suspicion or gives reasonable grounds to suspect that EximPe may be intended to be used as a medium for offenses related to ML/TF.

(b) In the event of rejecting/terminating any Customer relationship, the Risk Monitoring team will escalate all cases to the Principal Officer and the Designated Director for approval.

(c) The Onboarding team is responsible to document the rationale for escalating any relationships/cases.

(d) The Principal Officer is responsible for presenting these cases to the senior management or the Board on a quarterly basis. These cases include, but are not limited to:

- All SARS filed, along with Customer details.
- Customer relationships rejected/terminated on the grounds of ML/TF or financial crime suspicion
- Customers having true match against sanctions or other watch lists
- Customers for whom KYC checks could not be completed

F.12 Training

(a) As EximPe operates in a highly modulated environment, training and educating employees plays a key role for an effective AML program. Employees involved in the AML process shall be trained appropriately on the relevant ML/TF legislation, risks, and mitigation methodologies.

(b) EximPe shall ensure that AML related training is provided to all employees (old/ new) and associates including but not limited to all the new contractors, business partners, third parties, within six months of commencing their employment or association with EximPe.

(c) Continuous training shall be based on the roles and responsibilities of the employees.

(d) Training will be updated and refreshed periodically, reflecting the actual AML requirements, and should be executed with appropriate regularity.

F.13 Obligation of Secrecy

(a) The company shall maintain secrecy regarding the Customer information which arises out of the contractual relationship between EximPe and Customer.

(b) While considering the requests for data/information from Government and other agencies, EximPe shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.

(c) Exceptions to the said rule shall be as under:
  (i) Where disclosure is under compulsion of law,
  (ii) Where there is a duty to the public to disclose
  (iii) the interest of bank requires disclosure; and
  (iv) Where the disclosure is made with the express or implied consent of the Customer.

EximPe shall maintain the confidentiality of information as provided in Section 45NB of RBI Act 1934.

F.14 Audit and Review

(a) The audit team should report to the audit committee of the Board (or similar oversight body) and independently evaluate the risk management and controls of the EximPe through periodic assessments, including: the adequacy of the EximPe's controls to mitigate the identified risks, the effectiveness of the EximPe's staff's execution of the controls, the effectiveness of the compliance oversight and quality controls, and the effectiveness of the training.

(b) The audit function must have knowledgeable employees with sufficient audit expertise. Audits should be conducted on a risk-based frequency, periodically, a EximPe-wide audit should be conducted. Audits should be properly scoped to evaluate the effectiveness of the program, including where external auditors are used. Auditors should proactively follow up on their findings and recommendations.

F.15 AML Committee

(a) EximPe shall form an AML Committee, with Arjun Zachariah, the Director, EximPe as a Chairperson within 30 days from the date of approval of this policy.

(b) The role of the AML Committee shall be to ensure the implementation of this policy and monitor its adherence to this policy.

(c) The AML committee shall include: Designated Director of EximPe, Head of Operations, Head of Legal, CFO, Head of Risk/MLRO.

(d) The AML Committee shall meet at least once every 3 months. The quorum of the AML Committee shall be the presence of at least two members of the AML Committee. The agenda for the AML Committee shall be circulated 7 days before the meeting. The AML Committee may meet in person or undertake a video conference. The minutes of the meeting will be prepared by the Head of Legal. The minutes will be circulated for

confirmation by all the members of the Committee. The Principal Officer shall maintain the record of the minutes.

(e) The Principal Officer shall provide a report to the AML Committee on the following issues:

- Status as to the implementation of the policy.
- Any new developments in respect of regulations that impact this policy.
- Number of suspicious transaction reports filed;
- Number of Customers blocked due to sanction list;
- Status regarding the training of employees on AML & KYC;
- Any other matter that Principal Officer deems fit:
- Any other matter that the Committee may request the Principal Officer to address after due notice.

(f) If there are grounds to believe that Customer activity or transactions on Customer websites are suspicious, then on the basis of these grounds of suspicion, a decision may be taken by the Principal Officer to block funds, terminate the Customer, collate data, and report it to the FIU, Provided that in case the Principal Officer requires an urgent consultation with the AML Committee, such consultation can be done with any two available members of the AML Committee.

F.16 Periodic Review of AML Program

(a) EximPe shall conduct Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for Customers, countries or geographic areas, products, services, transactions, or delivery channels, etc. The assessment process will consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied.

(b) The risk assessment by EximPe shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of EximPe.

(c) The Board shall determine the periodicity of the risk assessment, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually. The outcome of the exercise shall be put up to the Board or any committee of

the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies.

(d) EximPe shall apply a Risk-Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls, and procedures in this regard. Further, EximPe shall monitor the implementation of the controls and enhance them if necessary.

EximPe

Annexure 1

Customer Due Diligence (CDD) - PAN details, officially valid document of the proprietor (passport, driver's license, voter's ID card) and photograph.

In the case of foreign national, the passport and the photograph will be collected.

For Institutional Beneficial Owners, the registration certificate and the address proof of the principal place of operation will be collected.

Entity Wise Documentation

Org Type	Documents Collected	Checks
Proprietorship	• Business proof (Any two of below) - Registration certificate from ROC -Certificate/ license issued by the appropriate authorities under Shops & Establishment Act and/or any other Acts as applicable to the firm -Sales tax & income tax return MSME -GST certificate or details • CDD of proprietor • Bank details or cancelled cheque or attested account statement	• To verify firms legal existence a proprietor needs to upload the GST certificate and Udhyog Aadhar Certificate or Udyam Registration in its dashboard. (self attested). These details are cross verified in Surepass, KSCAN and Comply Advantage. • Proprietor's PAN, voter Id, driving license, passport (any -one) of the proprietor and passport size photograph. • Match all the shared documents and the

		information with our tools. (self-attested) ● Udhyog Aadhar certificate or Udyam Registration or any of the Utility bill on proprietor's name can be collected as address proof.
LLP	● Certificate of incorporation ● LLP Agreement ● List of all designated directors ● GST certificate or details (if applicable) ● PAN ● Bank details or cancelled cheque or attested account statement - In case settlement to own account ● CDD of authorised signatory ● CDD of beneficial owners ● Address proof of principal place of its operation if its different from registered address .	● Authorized signatory (KYC- ID and address proof) (official valid document) ● LLP documents such as Certificate of incorporation and partnership deed are uploaded by the client in their dashboard, these documents are to be verified through KSCAN and Comply Advantage. ● **Important checks** i) LLPIN number has to be the same as provided in customer dashboard and COI. ii) All the mentioned partners PAN details have to be correct as provided in the dashboard iii) Director Identification number has to be active. iv) Legal risks and the cases will be highlighted (if any)
Partnership	● Partnership Deed ● Registration Certificate ● PAN ● Bank details or cancelled cheque or attested account statement ● List of all partners	● Authorized signatory (KYC- ID and address proof) (official valid document) ● Registration Certificate and partnership deed are uploaded by the client in their dashboard, these

	• CDD of Authorised Signatory • CDD of Beneficial Owners • Address proof of principal place of operation if it's different from registered address	documents are to be verified through KSCAN and Comply Advantage. • **Important checks** i) All the mentioned partners PAN details have to be correct as provided in the dashboard, these details are matched with the information shown in KSCAN. ii) Legal risks and the cases will be highlighted (if any)
Private Limited | Public Limited	Certified copy or e-document of: • Certificate of incorporation • memorandum and articles of association • GST certificate • PAN of the company • Resolution from the board of directors and power of attorney granted to its manager, officers or employees to be the authorised signatory • List of directors • CDD of Beneficial Owners for Private Limited companies and authorised signatory • Address proof of principal place of operation if its different from registered address. • Bank details or cancelled cheque or attested account statement	• Authorized signatory (KYC- ID and address proof) (official valid document) • Company documents such as certificate of incorporation, memorandum of association, articles of association and PAN of the company are to be uploaded by the client in their dashboard, these documents have to be verified through KSCAN, Surepass and comply advantage. • **Important checks** i) DIN number has to be the same as provided in customer dashboard. ii) All the mentioned directors PAN details have to be matched as provided in the dashboard iii) Director Identification number has to be active.

		iv) Legal risks and the cases will be highlighted (if any)

Annexure 2

UNQUALIFIED/UNACCEPTABLE BUSINESSES

Any services or products which are purchased/ offered for sale by a user to third parties from time to time, using these services. products shall not include those banned products and services that are listed below:

.

- Adult Goods and Services Which Includes Pornography and Other Sexually Suggestive Materials (Including Literature, Imagery and Other Media); Escort or Prostitution Services
- Alcohol Which Includes Alcohol or Alcoholic Beverages Such as Boer, Liquor, Wine, Or Champagne.
- Body Parts Which Include Organs or Other Body Parts
- Bulk Marketing Tools Which Include Email Lists, Software, Or Other Products Enabling Unsolicited Email Messages (Spam).
- Cable Descramblers and Black Boxes Which Includes Devices Intended to Obtain Cable and Satellite Signals for Free.
- Child Pornography Which includes Pornographic Materials Involving Minors.
- Copyright Unlocking Devices Which Include Mod Chips or Other Devices Designed to Circumvent Copyright Protection. 8) Copyrighted Media Which includes Unauthorized Copies of Books, Music, Movies, And Other Licensed or Protected Materials.
- Copyrighted Software Which Includes Unauthorized Copies of Software, Video Games and Other Licensed or Protected Materials, Including OEM Or Bundled Software.
- Counterfeit And Unauthorized Goods Which Includes Replicas or Imitations of Designer Goods; Items Without a Celebrity Endorsement That Would Normally Require Such an Association, Fake Autographs, Counterfeit Stamps, And Other Potentially Unauthorized Goods
- Cryptocurrency Exchanges, platforms dealing in cryptocurrency trading
- Drugs And Drug Paraphernalia Which Includes Illegal Drugs and Drug Accessories, Including Herbal Drugs Like Salvia and Magic Mushrooms.
- Drug Test Circumvention Aids Which Include Drug Cleansing Shakos, Urine Test Additives, And Related Items.
- Endangered Species Which Includes Plants, Animals or Other Organisms (Including Product Derivatives) In Danger of Extinction.
- Gaming (predominantly game of chance)/Gambling Which Includes Lottery Tickets, Sports Bets, Memberships/ Enrolment in Online Gambling Sites. And Related Content.
- Government IDs or Documents Which Includes Fake IDs, Passports, Diplomas, And Noble Titles.
- Hacking And Cracking Materials Which Includes Manuals, How-To Guides, Information, Or Equipment Enabling Illegal Access to Software, Servers, Watomites, Or Other Protected Property.
- Illegal Goods Which Include Materials, Products Or Information Promoting Illegal Goods or Enabling Illegal Acts.
- Miracle Cures Which Include Unsubstantiated Cures, Remedies or Other Items Marketed as Quick Health Fixes.

- Offensive Goods Which Include Literature, Products or Other Materials That: A) Defame or Slander Any Person or Groups of People Based on Race, Ethnicity, National Origin, Religion, Sex, Or Other Factors B) Encourage or Incite Violent Acts C) Promote Intolerance or Hatred.
- Offensive Goods, Crime Which Includes Crime Scene Photos or Items, Such as Personal Belongings, Associated with Criminals.
- Prescription Drugs or Herbal Drugs which Includes Drugs or Other Products Requiring a Prescription by A Licensed Medical Practitioner.
- Pyrotechnic Devices and Hazardous Materials Which Includes Fireworks and Related Goods; Toxic, Flammable, And Radioactive Materials and Substances. Regulated Goods Which Include Air Bags: Batteries Containing Mercury; Freon or Similar Substances/Refrigerants, Chemical/Industrial Solvents, Government Uniforms, Car Titles or Logos, License Plates, Police Badges and Law Enforcement Equipment, Lock Picking Devices, Pesticides; Postage Meters, Recalled Items, Slot Machines, Surveillance Equipment, Goods Regulated by Government or Other Agency Specifications.
- Securities, Which Includes Stocks, Bonds, Or Related Financial Products
- Tobacco And Cigarettes Which Includes Cigarettes, Cigars, Chewing Tobacco, And Related Products.
- Traffic Devices Which Include Radar Detectors/ Jammers, License Plate Covers, Traffic Signal Changers, And Related Products.
- Weapons Which Include Firearms, Ammunition, Knives, Brass Knuckles, Gun Parts, And Other Armaments.
- Wholesale Currency Who Includes Discounted Currencies or Currency Exchanges. Live Animals or Hides/Skins/Teeth, Nails and Other Parts Etc of Animals. Multi-Level Marketing Collection Fees.
- Matrix Sites or Sites Using a Matrix Scheme Approach.
- Drop-Shipped Merchandise.
- Any Product or Service Which Is Not in Compliance with All Applicable Laws and Regulations Whether Federal, State, Local or International Including the Laws of India The Customer Shall Not Sell, Purchase, Provide or Exchange A Cardholder's Name or MasterCard / Visa Account Number Information in Any Form Obtained by Reason of a MasterCard/ Visa Card Transaction to Any Third Party Other Than Its MasterCard Visa Acquiring Member-Citrus Pay, Or Pursuant to A Government /Statutory or Competent Body's Request.
- Pyrotechnic Devices, Combustibles, Corrosives and Hazardous Materials Which Includes Explosives, Fireworks and Related Goods; Toxic, Flammable, And Radioactive Materials and Substances
- Regulated Goods Which Include Air Bags: Batteries Containing Mercury; Freon or Similar Substances/Refrigerants: Chemical/Industrial Solvents; Government Uniforms: Car Titles: License Plates; Police Badges and Law Enforcement Equipment; Lock-Picking Devices; Pesticides; Postage Meters; Recalled Items: Slot Machines; Surveillance Equipment Goods Regulated by Government or Other Agency Specifications

EximPe

Annexure 3

BANK ACCOUNT CHECK (PENNY DROP TESTING)

Details Requested:

- Bank Account Number
- IFSC code
- Bank Account Name

Objective: To verify the bank account where payments accepted by the Customer are to be settled.

Penny Drop Testing Pass

- The Digital KYC system does a penny drop into the account details checks for two things:
- Is the bank account correct?
- Is the bank account operational?
- Name of the Bank account is pulled from Bank records. This information is used for the three-way checks for Proof of Address (Unreg) and Proof of Business (Reg) verification.
- The system throws an alert if there is either a mismatch with Bank account name entered or with Proof of Identity (POI), Proof of address (POA) or Proof of Business submitted by the Customer.

Penny Drop Testing Fail

In case of a mismatch or if the system is down, the system automatically prompts the Customer to submit either canceled cheque! Bank statement/ Passbook/ Bank verification letter

- The agent performs the same three-way check manually as the automated Digital KYC does with the details mentioned in the uploaded document
- If the three-way check returns a satisfactory outcome, the form is forwarded for Maker-checker review
- If a mismatch is found, the Onboarding agent should mandatorily forward the case to the Risk team for review and further action.
- Additionally, if the document submitted looks forged/tampered or is a VA number (e.g.. PAYTM0123456), the Onboarding agent must refer the case to the Risk team.
- Risk team is required to take a decision considering any supporting Bank letters provided with Bank VA by the Customer.

Appendix

https://www.dgft.gov.in/CP/?opt=itchs-import-export

EximPe

Annexure 4

Checks performed on Import Transactions

Customer Related Checks:

1. Customer is KYC, AML compliant with valid IE Code and not on Caution list;
2. Request letter with debit authority submitted by Customer is duly filled, stamped, signed by authorized signatories;
3. Submission of the FEMA, OG and Bill of entry declaration;
4. Sufficient balance in INR/EEFC Account as the case may be;
5. Details of concessional charges to be levied if any, as per master tariff required;
6. Confirmation on not more than 3 overdue ORMs are outstanding at the time of remittance.
7. Checks on the name of EximPe to which funds are being transferred against Sanctions, Warnings, Fitness & Probity, PEP, Adverse Media. If featured in any of these lists, explanation shall sought from the Customer.

Transaction Related Checks:

Advance Payments Checks

1. Payment request matches with Invoice payment terms;
2. Details of part advance payment done, if any, are provided mentioning our transaction reference number;
3. Transaction does not involve parties from OFAC, US,UK, UN,EU sanctions, etc. ;
4. If transaction involves Iranian parties or Iran nexus, to check if Iran guidelines are adhered
5. If transaction involves Russia/Ukraine parties or nexus, to check with Sanction team before proceeding;
6. For merchanting trade transaction, Merchant Trading Transactions (MTT) – Revised Guidelines dated January 23, 2020 (MTT Guidelines) issued by the RBI should be followed;
7. If more than 2 transactions close to 1 lakh USD are sent for processing on the same day, genuineness of the transaction to be checked
8. Dual use goods check for goods above USD 5 lacs to be done;
9. Military goods check to be done;
10. If advance payment amount exceeds USD 200k, bank has to be notified for separate approvals from business/sales teams;
11. In case commodity is Rough/Semi precious/Precious stones, etc - Kimberley Process Certificate required; latest credit report of beneficiary required and BU approval on case to case basis;

Direct Payments

1. Payment request matches with invoice payment terms;
2. Details of part advance payments done or any previous remittance if any, are provided mentioning our transaction reference number;
3. Bill of entry and IDPMS confirmation required;
4. Delay reason and no interest declaration - for more than 6 six months up to 3 years;
5. Transaction does not involve parties from OFAC,US,UK, UN,EU sanctions, etc. ;
6. If transaction involves Iranian parties or Iran nexus, to check if IRAN guidelines are adhered;
7. If transaction involves Russia/Ukraine parties or nexus, to check with Sanction team before proceeding;
8. For merchanting trade transaction, MTT Guidelines should be followed;
9. If more than 2 transactions close to 1 lakh are send for processing on the same day, genuineness of the transaction to be checked
10. Dual use goods check for goods above USD 5 lacs to be done;
11. Military goods check to be done;
12. If 3rd party payment, then tripartite agreement, satisfactory documentary evidence and/or BU/GTS/branch approval required.
13. If Sole Proprietor/Partnership Firm, direct import remittance limit of USD 3 lakhs to be checked
14. In case of non-physical Imports such as import of software, data through internet etc., CA certificate in lieu of Bill of entry evidencing import required.
15. In case of high sea sales transaction, high seas sale agreement to be verified.
16. For remittances against replacement imports, RBI guidelines to be followed.
17. In case of Import of equipment by Business Process Outsourcing (BPO) Companies for their Overseas Sites, RBI guidelines to be followed.
18. In case of receipt of import documents by the importer directly from overseas suppliers, RBI guidelines to be followed.
19. In case receipt of import documents by the AD Category – I bank directly from overseas suppliers, RBI guidelines to be followed.
20. In case commodity is rough/semi-precious/precious stones, etc: Kimberley Process Certificate required; latest credit report of beneficiary required and BU approval on case to case basis.

EximPe

Annexure 5

Indicative List for Risk Categorization

Low Risk

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorised as low risk.

1. **Business Stability:** Companies with over 5 years of consistent international trading history.
2. **Transaction Limits:** Regular transactions typically do not exceed $50,000.
3. **Transaction Nature:** Consistent and predictable transaction patterns, aligned with the customer's business profile.
4. **Geographical Considerations:** Engagements primarily with countries recognized for robust anti-money laundering (AML) and counter-terrorism financing (CFT) measures.
5. **Compliance History:** A clean record with no previous instances of non-compliance or suspicious activities.
6. **PEPs:** Minimal exposure to PEPs, with no direct relationships.
7. **Adverse Media/Sanction Lists:** No flags in adverse media checks or on sanction lists.

Medium Risk

Customers that are likely to pose a higher than average risk may be categorized as medium depending on Customer's background, nature and location of activity, country of origin, sources of funds and their Customer profile etc.

1. **Variable Transaction Volumes**: Transactions generally range between $50,000 to $500,000.
2. **Business Longevity**: Firms with 2-5 years of experience in international trading.
3. **Diverse Transaction Patterns**: Occasional deviations from typical transaction patterns, requiring additional scrutiny.
4. **Moderate-Risk Geographies**: Business dealings with countries that have moderate risk profiles regarding AML/CFT.
5. **Occasional Compliance Concerns**: Previous instances of minor non-compliance or irregularities that have been resolved.
6. **PEPs:** Occasional dealings with PEPs, requiring enhanced scrutiny but no direct red flags.
7. **Adverse Media/Sanction Lists:** Occasional mentions in media that may require further clarification, but no active listings on sanction lists.

High Risk

High risk Customers are the ones who are very likely to be involved in money laundering. Additional information shall be collected to provide a deeper understanding of Customer activity and to mitigate associated risks. Illustrative examples of high-risk category Customers are:

1. **High-Value Transactions:** Regular transactions exceeding $1,000,000.
2. **New Entrants:** Businesses with less than 1 year of international trading history.
3. **Complex Business Models:** Involvement with NGOs, trusts, shell companies, or having opaque ownership structures.
4. **High-Risk Geographies:** Frequent trading with countries on high-risk lists for money laundering and terrorist financing.http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)
5. **Unexplained Wealth or Turnover:** Significant, unexplained fluctuations in net worth or business turnover.
6. **Regulatory Red Flags:** History of significant non-compliance issues, investigations, or sanctions related to financial dealings.
7. **PEPs**: Regular interactions with PEPs or immediate family/close associates of PEPs.
8. **Adverse Media/Sanction Lists:** Appearances on sanction lists or frequent, significant negative media coverage indicating potential risks.

Annexure 6

Refer the latest list based on the Schedule 1 of ITC(HS) Classifications of Export & Import Items. This list may be cross checked with the actual Schedule 1 of ITC(HS) Classifications of Export & Import Items and Notifications thereof.