JOY REFINERY (FZC)

SUSPICIOUS TRANSACTIONS REPORTING (PROCEDURES)

TABLE OF CONTENTS

1. OBLIGATION TO REPORT SUSPICIOUS TRANSACTIONS

The Company is obliged to report transactions to the FIU when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing, or benefitting from a crime. There is no minimum reporting threshold, and no statute of limitations with regard to ML/FT crimes or reporting of suspicious transactions.

2. IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

Employee shall remain vigilant to identify possible red flags with the customer transaction/activity such as:

- *The customer has an unusual interest in the internal policies, controls, regulations, and supervisory procedures and unnecessarily elaborates on justifying a transaction.*
- *The customer is reserved or anxious.*
- *The customer requests or seeks to carry out the transactions without disclosing his identity.*
- *The customer refuses to submit original documentation particularly those related to his identification.*
- *The customer intentionally conceals certain valuable information like his address (actual place of residence), telephone number.*
- *Cash transactions where banknotes with unusual denominations are used.*
- *Complex and unusual large transactions.*
- *Unusual pattern in the customer profile and transactions.*
- *Customer reluctant to complete KYC process.*
- *Suspects that a customer is carrying out transactions that are disallowed under Prohibited Activities in **ANNEXURE 1***

3. SUSPICIOUS TRANSACTION REPORTS (STR) TO THE FIU

The Company is obliged to report STRs to the FIU "without any delay." Since it is the responsibility of the CO to "review, scrutinize and study records, receive data concerning suspicious transactions, and take decisions to either notify the FIU or maintain the transaction, it follows that the time period for reporting STRs to the FIU begins at the moment a decision is made by the CO that a transaction (whether pending, in progress, or past) is suspicious.

Notifications (through the Go AML portal or any other means required by the FIU) should include all relevant information, document and records relating to the transaction, customer or account involved.

JOY REFINERY FZC has instituted a system for the mandatory reporting of suspicious transactions pursuant to Federal Law No. 4 of 2002 regarding criminalization of money laundering.

Any suspicious transactions must be reported to Anti-Money Laundering and Suspicious Cases Unit (AMLSCU). Where any employee or personnel, director or officer of **JOY REFINERY FZC** knows that the client has engaged in any of the predicate crimes under the UAE Federal Law,

the matter must be promptly reported to the Compliance Officer within the organization who, in turn, must immediately report the details to the AMLSCU.

If there are reasonable grounds to suspect that the customer has engaged in an unlawful activity, the Compliance Officer, on receiving such a report, must promptly evaluate whether there are reasonable grounds for such belief and must then immediately report the case to the AMLSCU unless the compliance officer/s or unit considers, and records an opinion, that such reasonable grounds do not exist.

COMPANY's directors, officers, and employees shall not warn their customers that information relating to them has been reported or is in the process of being reported to the AMLSCU, or communicate, directly or indirectly, such information to any person other than the AMLSCU. Any violation of this confidentiality provision shall render them liable for criminal, civil and administrative sanctions under the UAE federal law.

JOY REFINERY FZC shall maintain a register of all suspicious transactions that have been brought to the attention of its Compliance Officer, including transactions that are not reported to the AMLSCU. The register shall contain details of the date on which the report is made, the person who made the report to its Compliance Officer and information sufficient to identify the relevant papers related to said reports.

Chapter 3 of the UAE Federal Law No. 4 of 2002 provides penalties for failure to report suspicious activities to the AMLSCU by those who are aware of a suspicious activity or transaction which may be a criminal offense, punishable by a fine or imprisonment or both.

- **JOY REFINERY FZC** (through its Compliance officer (CO)) has an obligation to report suspicious activity to the relevant financial intelligence department.
- Failure to act on or report suspicions where there are reasonable grounds to suspect criminality, is an offence under AML/CFT Law.
- All SARs (Suspicious Activity Reports) or STRs (Suspicious Transactions Reports) must be reported by employees, confidentially, only to the Compliance officer, by filing an Internal SAR/STR.
- The CO has a duty to consider all such internal reports and if the CO also suspects ML/TF, an external SAR/STR must be made to the Financial Intelligence Department.
- The Company will not prejudice an Employee who discloses any information regarding money laundering to the Compliance officer.
- All records of SAR/STR will be kept in a special confidential file and not on the customer's file. The CO may reveal details of STR/SARs to persons only if he is convinced that doing so does not constitute tipping-off.

Following procedures are applied in sequence to figure out suspicious activities :

PART 1 : CUSTOMER DUE DILIGENCE (CDD)

- DEFINITION : CDD is the process where pertinent information of a customer's profile is collected and evaluated for potential money laundering or terrorist financing risks.
- OBJECTIVE : Upon completion of CDD, the customer may be given a risk rating in accordance with the risk he or she may present to the company.

  Risk ratings can be in the form of a category, such as "low risk" or "high risk", or a numeric value derived from a risk matrix based on a pre-defined set of criteria.

  A risk rating helps a company in deciding how and when to apply the appropriate checks, treatment, and controls that commensurate to the level of risk.

  This methodology is also known as the risk-based approach, which allows a company to prioritize resources accordingly to areas that require more attention.

- DATA COLLECTION : The first step of CDD is to obtain information from a customer. The following points outline the general information that should be collected.

- CUSTOMER PROFILE (INDIVIDUAL) :

- Full name, including any alias
- Residential address, mailing address
- Contact numbers, email addresses
- Place of birth, date of birth
- Gender
- Marital status
- Nationality
- Race
- Government-issued identification number
- Government-issued tax identification number
- Occupation
- Specimen signature
- Parental consent form (where the individual is a minor)

- **CUSTOMER PROFILE (ENTITY) :**

- Name of corporation
- Type of corporation
- Date of incorporation
- Place of incorporation
- Board resolution on authorised signatories
- Certificate of Incumbency
- Constitution
- Articles of Association
- Certificate of Incorporation
- Annual report
- Directors
- Shareholders
- Senior Management
- Ultimate Beneficial Owners

- **CUSTOMER PROFILE (TRUST) :**

- Settlor's information
- Trustee's information
- Beneficiaries information
- Protector's information
- Relationship between settlor, trustee, protector and beneficiary
- Ultimate beneficial owner's information

- **WEALTH PROFILE :**

- Source of wealth
- Source of funds
- Annual income

INDEPENDENT VERIFICATION OF COLLECTION :

The second step is to verify the information collected from the customer to ensure accuracy and legitimacy. Majority of the information can be verified by documents that are issued by a government body or an independent reputable agency.

Examples include:

- **Government-issued photo identification card (specimen photos for all ID cards around the world here)**
- **Government-issued passport (specimen photos for all passports here)**
- **Tax bill**
- **Phone/power/water bill to prove residential address**
- **Business profile issued by a government regulator for business entities**
- **Certificate of incorporation from a country's official company register**
- **Articles of association, or memorandum of association**

4. NAME SCREENING :

Name screening is the next step where an analyst performs a check via a name-screening and/or an internal blacklist database to determine if a customer is known to be of heightened risk and thereby posing a risk to the financial institution.

As per Article 21.2 of Cabinet Resolution No.74 of 2020., **JOY REFINERY FZC** regularly screen their databases and transactions against names on official sanction lists issued by UN, Central Bank, OFAC, UAE Local Terrorist List, and other law enforcement agencies and immediately when notified of any changes to any of such lists.

The sanction screening is integrated into the accounting and bookkeeping system. The Company is using **"DIGI Compliance"** as a screening tool.

Screening processes should be conducted at various stages of the customer lifecycle to include:

- **Periodic name screening**: A change to either the customer identifying information or UN Consolidated List/Local Terrorist List should trigger an automatic screening.
- **Ad hoc name screening**: Such screening is triggered by a specific business need or to comply with a request by a competent authority, or in the case of feedback from a downstream financial institution.
- **Re-screening**: A specific scenario in the transaction monitoring system identifies a high-risk jurisdiction in updated customer information.

Typically, the objective is to ascertain if the customer is known to have any of the following profiles:

- **Politically Exposed Persons (PEPs)**
- **Criminals**
- **Terrorist**
- **Sanctioned individual/entity**
- **Reported in media to be involved in any activity that is adverse in nature**

PART 2 : ENHANCED DUE DILIGENCE

WHEN : EDD is conducted where the customer has been evaluated to be at a heightened risk to the company.

Part of the Financial Action Task Force (FATF) Recommendations suggests that companies adopt a risk management system to determine if the customer presents a higher risk.

The main process of conducting EDD is to obtain senior management approval before establishing a relationship and to take reasonable measures to establish the source of wealth and the source of funds.

Examples of higher risk customers/transactions include but not limited to:

- **Politically Exposed Person (PEP)**
- **Customer who are positively identified to have adverse profiles on watchlists**
- **Terrorists**
- **Non-face to face account opening**
- **Correspondent accounts**
- **Customers located in high-risk locations**

5. STR Procedures

As a primary requirement of submitting Suspicious Transaction Reports (STR), **JOY REFINERY FZC** has obtained access to goAML, the online STR reporting portal of the Central Bank. The Licensed Person may contact the FIU or the AML Department at Ministry of Economy for appropriate guidance to obtain access to the STR reporting portal.

All employees of the **JOY REFINERY FZC** are obliged personally to report, when there are reasonable grounds to suspect that the funds are proceeds from criminal activity or to be used for money laundering, terrorism or terrorist act or terrorist financing, to the compliance officer. The compliance officer will conduct proper investigations and update the highest authority and raise suitable STR/SAR's.

A single Suspicious Transaction Report (STR) can help stop the flow of illegal money and help prevent the repercussions of financial crime. Further, these reports are an essential contribution to the development of the financial intelligence resources that are used by country's law enforcement, revenue, and national security agencies. Thereby, we file STRs to ensure that the **JOY REFINERY FZC** is not used to aid the transfer of illegal money for money laundering and terrorism financing.

- All employees are required to report any potentially suspicious or unusual transactions.
- The reporting must be done with full facts of the case within reasonable time.
- It is company`s obligation to investigate the background and purpose of transactions deemed to be 'unusual' and to set forth our findings in writing, even in the event, it is not considered necessary to report the transactions to FIU as suspicious. As is the case of other documents these findings should also be maintained for inspection by the competent authorities for a period of at least five years.

- The Compliance Officer shall conduct in depth investigation and take an appropriate action before reporting such transactions to Financial Intelligence Unit.
- It is important to note that the "time factor" in reporting suspicious transactions remains crucial; if we are able to retrieve / submit the relevant information, it will help regulatory authority and Law enforcement authorities to effectively review and take effective measures to combat money laundering, terrorism financing or any other illegal activity.
- Attempted Transactions are obliged to report transactions through GoAML system, which appear as an attempt to launder money and/or finance a terrorist organization and/ or a terrorist activity.

In case of doubt that a transaction might be meant for terrorism or terrorist organizations or for terrorist purposes, we should freeze the transaction/account and inform the financial intelligence unit at the in writing immediately.
All Employees should strictly comply with the following if a transaction created at your end/found in the system seems suspicious to you:

- Do not inform the customer of your suspicions about his/her transaction(s), and action being taken by you.
- Hold the transaction and report immediately to your Compliance Officer.
- Forward copy of Customer identity and transaction copy to Compliance Officer
- Do not proceed with a transaction put on hold or block the transaction.

Institutions which fail to report unusual and suspicious transactions shall be penalized in accordance with the prevailing laws and regulations, such incidents should be immediately reported to the authorities through proper system.

6. Tipping Off

- All suspicious transactions must be kept fully confidential, and no one should inform any person or customer that his/her transaction is being reported as a suspicious transaction to the FIU.
- Non-compliance is a criminal offence, and the employee involved shall be terminated, immediately and additionally he/she is personally subject to a fine or imprisonment or both.
- It is a criminal offence for an employee to tip off, tell or inform any person including customers that any of their transactions is being scrutinized for possible involvement in suspicious money laundering operations or terrorist financing.
- Under the AML/CFT Law, 'Tipping Off' is an offence. Once an internal or external suspicious activity report has been made, it is an offence for anyone to tip-off any person, that is, inform any person that his activities are being scrutinized for possible involvement in suspicious money laundering operations, or that any other competent authority is investigating his possible involvement in suspicious money laundering operations.

- Tipping Off risks become real once a suspicious activity report has been made to the Compliance Officer and where the Compliance Officer agrees with the underlying suspicion and submits a report to the Financial Intelligence Department. All communication between staff and the customer(s) from that point on needs to be handled with care, the Compliance Officer will provide advice as to how to handle such situations.
- If **JOY REFINERY FZC** reasonably believes that performing the CDD process will tip-off a customer or potential customer, it may choose not to pursue that process and should file an Internal STR. **JOY REFINERY FZC** will ensure that its Employees are aware of and sensitive to these issues when considering the CDD process.
- According to the Article 25 of the AML/CFT Law, any person violating this prohibition is liable to a penalty of no less than AED 100,000 and no more than AED 500,000 and imprisonment for a term of not less than six months or both.

7. Guidelines for Internal Real-Time Reporting of Unusual or Suspicious Transactions

In case of identifying a transaction as unusual or suspicious at the time when the customer is at **JOY REFINERY FZC**, the Reporting Entity should proceed as follows:

- Conceal his suspicions from the customer.
- Hold the transaction if it is related to TF and freeze the funds.
- Report your Internal STR through automated System to The Compliance Officer in confidence.
- Upload scanned copy of the customers' identification document and any document relating to the transaction for the Compliance Officer review.
- Proceed as instructed by the Compliance Officer.
- Do not inform the customer that his transaction is being investigated or reported as a suspicious transaction. Such an action constitutes tipping-off and is a criminal offense.

8. Guidelines for External Reporting of Unusual or Suspicious Transactions to the Regulators

- **JOY REFINERY FZC** have procedures, systems, and controls to ensure timely reporting of suspected cases to the FIU.
- **JOY REFINERY FZC** has access to the online STR/SAR reporting portal of the CBUAE and will contact the regulators for assistance.
- The Compliance Officer must promptly report all cases where there are reasonable grounds for suspicion of money laundering or terrorist financing, including attempted transactions that appear to be linked to such criminal activity.

- The Compliance Officer will ensure that appropriate actions are taken to comply with the directions of the FIU upon receipt of acknowledgement of an STR.
- The Compliance Officer will retain records of STRs submitted to the FIU together with all details relating to the investigations performed for a period of at least 5 years.
- In case of a transaction suspected to be associated with terrorist financing, the **JOY REFINERY FZC** employee must inform The Compliance Officer immediately, freeze the account and hold the transaction. The Compliance Officer must in turn submit an STR to the Regulators immediately.

9. ANNEXURE

PROHIBITED CUSTOMER TYPES/BUSINESS RELATIONSHIPS

The Company has categorized various kinds of clients whose commercial dealings call for increased levels of due diligence. This will often be the case in situations in which the company's business activities are anticipated to present a risk that is greater than the company's average risk. Transactions involving restricted customer categories are a type of ML/FT typology that is frequently employed by organizations that participate in the criminal underworld and professional money launderers.

The following are the conditions under which company, will refuse to accept a new business connection or will end an existing one. The following are some examples of such circumstances:

- Persons (natural or legal) who are unable to meet the company's identification and verification requirements or existing customers who no longer fulfil them.
- Shell banks / company
- Persons (natural or legal) or existing customers on sanction lists or lists provided by the EOCN or other regulatory authorities.
- Customers for whom suspicious transaction reports have been repeatedly submitted to the FIU, unless the latter requests the accounts to remain open so as to facilitate the investigation process.
- Prohibited transactions, these are transactions for which the company has assessed that the level of risk is not acceptable to the Company.