CASSA

Policy Manual for the Prevention of Money Laundering and Countering the Financing of Terrorism

March 2024

CPS/KYCPM/V.2

Document Control Sheet

Document Title:	Policy Manual for the Prevention of Money Laundering and Countering the Financing of Terrorism.
Version:	CPS/KYCPM/V.2
Department Belongs to:	Compliance / Risk Management
Year	March 2024
Reviewed and Recommended by	General Manager
Approved By:	Shareholder

Document Revision History:

Version No.	Date	Sections Changed	Summary of Changes
CPS/KYCPM/V.1	March 2023	New Policy	First Version of Policy
CPS/KYCPM/V.2	March 2024	Revised Policy	Revised in line with the Supplemental Guidance for Payment Services Sector
	Next Review on March 2025	For any Updates and Changes required	

POLICY STATEMENT:

Cassa Payment Services Co. LLC (CPS) is a licensed entity and supervised by Ministry of Economy as its reporting entity and is committed to prevent money laundering and countering the financing of terrorism. The management understands the importance of application of the standards and guidelines issued by Ministry of Economy and the industry best practices while transacting and conducting businesses in the UAE.

The management of Cassa Payment Services Co. LLC (CPS) believes that the best way to fulfill this commitment is to establish effective internal policies and procedures that are conducive to:

- Carrying out the activities and services provided in accordance with strict ethical standards and current laws and regulations.
- The implementation of codes of conduct and monitoring and reporting systems to prevent that, the company is used for money laundering and terrorism financing.
- Ensuring that all the employees of Cassa Payment Services Co. LLC observe this policy manual and performs action to the adherence of the processes mentioned in it.

This Policy Manual is:

Reviewed and recommended by:	Approved by:
General Manager	**Shareholder**

Dated: 31 March 2024

Table of Contents

1. BASIS OF POLICY FORMULATION AND REFERENCES

1.1. The Ministry of Economy

The Ministry of Economy is fully committed to countering money laundering, combating, detecting, and deterring terrorist financing in accordance with legislation, as the relevant authorities in the UAE have established an institutional system of supervision, control and gathering information on all practices that may lead to and respond to financial crimes, including money laundering and terrorist financing. The authorities are aware that the national framework and coordination to address money laundering and combat terrorist financing must continue to be strengthened and developed to improve its effectiveness.

As a reporting entity for Designated Non-Financial Businesses and Professions expects:

- Strict compliance with applicable Anti-Money Laundering and Terrorism Financing Laws - Decree 20 of the Federal Law 2018 on countering money laundering offences, combating terrorist financing and financing illegal organizations and
- As well as with the recommendations and circulars issued on this subject - Regulations 10 of 2019 for a decree of federal law No. 20 of 2018 on countering money laundering crimes, combating terrorist financing and financing illegal organizations
- Cabinet Decision No. (20) of 2019 Terrorism List Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing and proliferation of Weapons of Mass Destruction, and Related Resolutions.
- Cabinet Resolution No. (16) of 2021 on the Consolidated List of Offences and Administrative Fines
- Cabinet Resolution No. (53) for 2021 on administrative sanctions resulting from violators of the provisions of The Council of Ministers Resolution No. (58) for 2020
- Cabinet Resolution No. (58) for 2020 Regulating the Beneficial Owner Procedures
- Cabinet Resolution No. (74) of 2020 on the system of lists of terrorism and the implementation of Security Council resolutions on the prevention, suppression and financing of terrorism, cessation of arms proliferation and financing and relevant resolutions
- Federal Decree Law No (26) of 2021 to amend certain provisions of Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations
- Cabinet Resolution No (24) of 2022 Amending some provisions of Cabinet Resolution No (10) of 2019 On the Executive Regulations

Website: www.economy.gov.ae

1.2. United Nations:

United Nations is an intergovernmental organization to promote international co-operation. It was established on 24th of October 1945. At its founding, United Nations had 51 member states. Currently United Nations has 153 members. The headquarters of the United Nations is in Manhattan, New York, USA. The organization is financed by assessed and voluntary contributions from its member states. Its objectives include maintaining international peace and security, promoting human rights, fostering social and economic development, protecting the environment, and providing humanitarian aid in cases of famine, natural disaster, and armed conflict.

The UN has six principal organs:

- the General Assembly (the main deliberative assembly).
- the Security Council (for deciding certain resolutions for peace and security).
- the Economic and Social Council (ECOSOC) (for promoting international economic and social co-operation and development).
- the Secretariat (for providing studies, information, and facilities needed by the UN).
- International Court of Justice (the primary judicial organ); and
- the United Nations Trusteeship Council (inactive since 1994).

UN System agencies include the World Bank Group, the World Health Organization, the World Food Program, UNESCO, and UNICEF.

United Nations Security Council: The Security Council is charged with maintaining security among countries. While other organs of the United Nations can only make "recommendations" to member states, the Security Council has the power to make binding decisions that member states have agreed to carry out, under the terms of Charter Article 25. The decisions of the Council are known as United Nations Security Council resolutions.

The Security Council is made up of fifteen member states, consisting of five permanent members, China, France, Russia, the United Kingdom, and the United States and ten non- permanent members. The UN Charter is a multilateral treaty. It is the constitutional document that distributes powers and functions among the various UN organs. It authorizes the Security Council to act on behalf of the members, and to make decisions and recommendations. Resolutions by the Security Council are legally binding if they are made under Chapter VII of the Charter.

Websites:

- www.un.org
- www.unscr.com

1.3. Financial Action Task Force (FATF)

The Financial Action Task Force on Money Laundering (FATF) was established in 1989 at G7 Summit in Paris to combat the growing problem of money laundering. The task force was charged with studying money laundering trends, monitoring legislative, financial and law enforcement activities taken at the national and international level, reporting on compliance, and issuing recommendations and standards to combat money laundering.

At the time of its creation, the organization had 16 original members. The FATF Secretariat is housed at the headquarters of the OECD in Paris. In its first year, the FATF issued a report containing forty recommendations to fight money laundering more effectively. These standards were revised in 2003 to reflect evolving patterns and techniques in money laundering. In 2001 the purpose expanded to act on terrorism financing. In February 2012, the FATF codified its recommendations and Interpretive Notes into one document and included new rules on weapons of mass destruction, corruption, and wire transfers.

FATF monitors countries' progress in implementing the FATF Recommendations by 'peer reviews' ('mutual evaluations') of member countries.

Website: http://www.fatf-gafi.org/

2. INTRODUCTION:

The leadership and management team of Cassa Payment Services Co. LLC (CPS) is committed to implement a strict compliance regime across all its services and follow the guidelines, rules and regulations as laid by the regulators and its amendments from time to time, laws of the country and international best practices related to Anti-Money laundering (AML) and Combating Financing of Terrorism (CFT).

CPS maintains high standards of professional, social, business ethics and relationship with regulators, customers, peers, real estate brokers, and other internal and external stakeholders.

In its relentless efforts to exercise caution in all its transactions, the organization has planned to implement policies and procedures, provide suitable trainings to its staff to increase awareness and implement guidelines as issued by the Ministry of Economy on AML/CFT.

This internal policy is based on the guidelines issued by the Ministry of Economy for (Designated Non-Financial Businesses and Professions) DNFPBs and supplementary guidelines for Payment Services Sector in the UAE, and other international recommendations and practices by FATF.

3. GOVERNANCE FRAMEWORK:

3.1. Governance Structure for AML/CFT Compliance – Figure 1

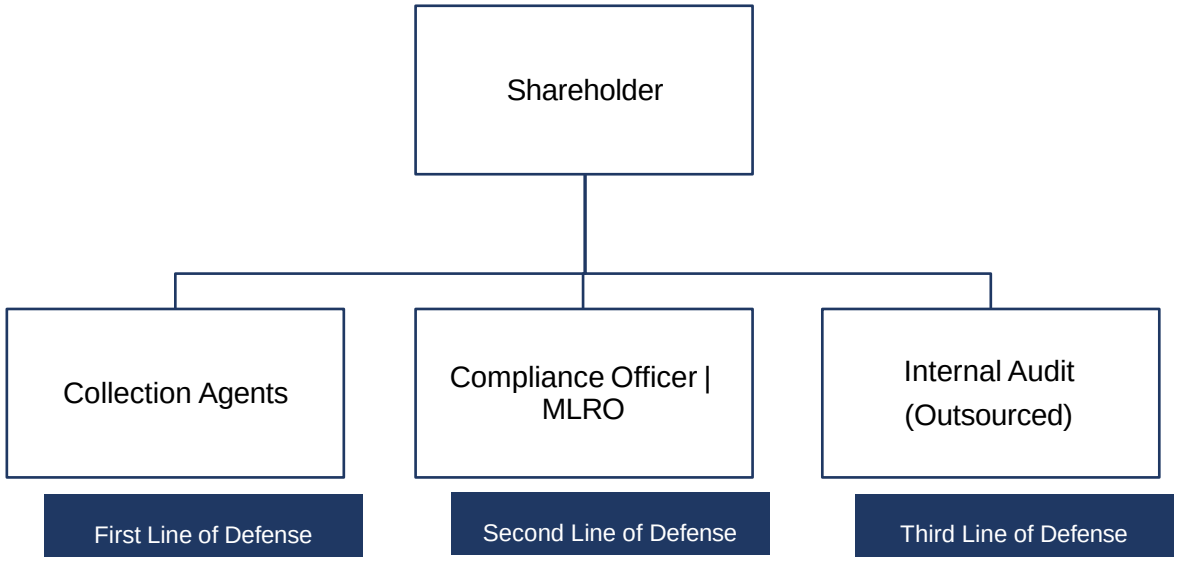


Figure 1: Governance Structure – Cassa Payment Services Co. LLC (CPS), as of March 2024

3.1.1. The First line of Defense: Collection Agents

The Collection agents reporting to the Owner and Partner, is responsible for direct dealing to individuals and legal entities in the UAE and collecting their payments. They shall also ensure that the KYC procedures are followed based on the KYC Guidelines (Reference Point 5.1).

3.1.2. The Second line of Defense: Compliance Function

Compliance Officer as MLRO takes all compliance related decisions jointly with both the Owners. The Compliance functions act as a second line of defense for Cassa Payment Services Co. LLC (CPS) and shall ensure KYC Guidelines / Name Screening / STR are implemented. The detailed responsibilities are mentioned below. (Reference Point 3.2.2)

3.1.3. The Third Line of Defense: Internal Audit Function

The Internal Audit function is outsourced at Cassa Payment Services Co. LLC (CPS) reporting directly to the Owner / Partner is an independent function acting as a third Line of defense. The detailed guidelines pertaining to the functional scope on compliance is mentioned under as Independent Review (Reference Point 6).

3.2. Roles and Responsibilities:

3.2.1. Owner and Partner

3.2.1.1. Minimum requirements:

Owner and Partner must undertake and govern the compliance activities and functions in Cassa Payment Services Co. LLC (CPS).

The following functions shall be undertaken by the senior management:

- Undertake a risk assessment which identifies the vulnerability of the company to be used to launder money or finance terrorists.
- Based on the risk assessment, implement a risk management framework to ensure that the company is not used to launder money or finance terrorists.
- Ensure that the risk management framework is developed, and sufficient resources being devoted to dealing with higher-risk customers and transactions.
- Ensure that the company has appropriate compliance management arrangements, including the appointment of a compliance officer at management level; and
- Devote sufficient resources to deal with money laundering and terrorist financing, including ensuring that the compliance function is adequately resourced, and that staff receive appropriate and adequate training.

3.2.1.2. Actions required.

- Carry out a risk assessment, which should be reviewed and updated on a regular basis, identifying where the business is vulnerable to money laundering and terrorist financing.
- Based on the risk assessment, develop internal policies, procedures, and controls to combat money laundering and the financing of terrorism.
- Ensure staff effectively implement the internal policies, procedures, and controls and receive appropriate training; and
- Monitor the implementation of the company policies, procedures, and controls and make improvements where required based on changes to the company's money laundering and terrorist financing risk assessment or as recommended by the regulatory authority and / or the financial intelligence unit.

3.2.1.3. Responsibilities

The management is responsible for the effective implementation of a risk framework to the management of money laundering and terrorist financing risk.

The management of risk needs to be reviewed and updated from time to time to reflect changes in the company's strategy or other factors such as changes to the law.

Policies and procedures should consider risk factors relating to the customer, product and service, delivery channel, and geographic location of the customer.

Where higher risks are identified, based on the company's risk assessment, the staff must take extra measures and senior management should ensure that the staff fully understand and implement the requirements of the policies and procedures.

3.2.2. Compliance Officer/MLRO

The Compliance Officer (CO) / Money Laundering Reporting Officer (MLRO) is responsible for the following actions:

- Receiving inputs from staff and making suspicious transaction reports to the financial intelligence unit and regulatory authority.
- Developing and maintaining the anti-money laundering and counterterrorist financing policy and internal procedures of the company in line with regulatory requirements.
- Assisting the management in developing and maintaining an effective anti-money laundering and counterterrorist financing compliance culture.
- Ensuring adequate documentation of the Cassa Payment Services Co. LLC (CPS) risk management policies regarding prevention of money laundering and terrorist financing, risk assessments, and their application.
- Determining and updating, in consultation with the senior management, a risk-based approach regarding money laundering and terrorist financing and the risk assessment of the Cassa Payment Services Co. LLC (CPS) customers, products, services, delivery channels, and geographic reach.
- Ensuring that all internal suspicious activity reports received are investigated without delay.
- Submitting suspicious transaction reports to the financial intelligence unit through goAML System.
- Providing initial and updated training for all relevant staff, including all staff who handle transactions, and customer receipts and payments transactions.
- Providing awareness training to the staff and the senior management.
- Ensuring that the staff are aware of and complying with their obligations under the law and the Cassa Payment Services Co. LLC (CPS) policies and procedures and that the basis for the risk-based approach to managing money laundering and terrorist financing risks is understood and applied.
- Presenting reports to the Owner and Partner, and the senior management; making recommendations, if any, for action to remedy any deficiencies in the policies, procedures, systems, or controls and following up on those recommendations.

3.2.3. Front-line staff

- Completing KYC and customer due diligence (CDD) procedures, including verifying customer identity, conducting screening, and assessing potential risks associated with the customers.
- Identifying and reporting any suspicious activity or transactions (Refer Annexure 10.3) to the compliance officer or MLRO.
- Conducting ongoing monitoring of customer accounts and transactions to identify and report any unusual or suspicious activity.
- Keeping accurate records of customer information, transaction details, and relevant AML/CFT documentation, as required by this Policy and regulatory requirements.
- Providing timely and accurate information to the designated compliance officer or MLRO regarding any AML/CFT-related concerns or queries.
- Attending and completing AML/CFT training and awareness programs provided by the company.
- Maintaining confidentiality and professionalism in all interactions with customers and colleagues regarding AML/CFT matters.

4. CUSTOMER RISK ASSESSMENT

Cassa Payment Services Co. LLC (CPS) as Payment Services provider carefully consider following factors while conducting any business relationship with a natural person/Individual, legal entity, or a corporate customer and group them according to the risk levels of High, Medium, and Low (See Annexure 10.4)

4.1. Customer Risk:

- Whether the counterparty or customer is a natural person or a legal entity
- Whether there is an association with a PEP
- Whether the Individual or Legal Entity is Resident or Incorporated within the UAE or Outside the UAE
- Whether the customer in relation to whether the party appears to be acting on their own or at the behest of a third party, and whether their knowledge and experience level regarding the product or service and transaction type is appropriate.

4.2. Product Risk

CPS has following products as part of services offered to its customer and are rated accordingly.

- Payment Services Provider - Treated as Low Risk

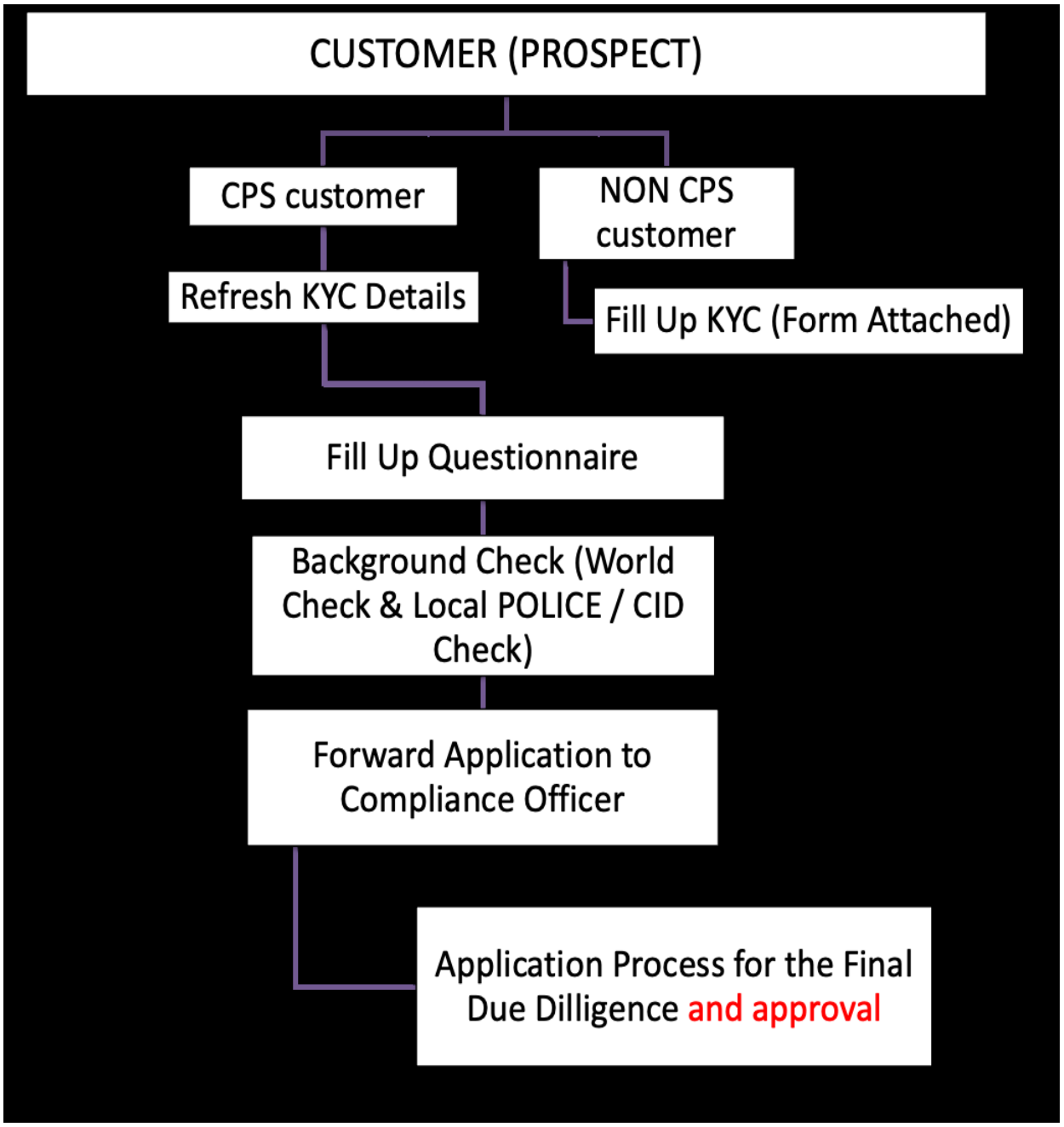
4.3. Geographic Risk:

- Country of origin or residence status of the customer (whether a UAE national or a foreign customer, and in the case of the latter, whether associated with a High-Risk Country)

4.4. Channel Risk:

- Channel by which the counterparty/customer is introduced (e.g., referrals versus walk-in, international versus domestic, in-person or via the internet or other media) and communicates (e.g., remote, or personal contact, direct or indirect through a proxy)
- Mode of Payment if done through Bank Transfer / Cheque or Cash Payments.

5. AML/CFT GUIDELINE AND PROCEDURES:



5.1. KYC

KYC is an acronym for "Know Your Customer". The foremost tool of anti-money laundering/countering financing of terrorism policies and procedures is to know your customers before executing any transactions. It involves making reasonable efforts to determine true identity and beneficial ownership of accounts, source of funds, the nature of customer's business and more. Beyond matching names, a key aspect of KYC controls is to monitor transactions of a customer against their recorded profile, history of the customer transactions and so on.

KYC is not a onetime process; it is an on-going process which continues throughout the business relationship with a customer. KYC is not an option; it is MANDATORY. KYC to be carried by adopting following procedures: KYC process can be carried our performing Customer Simple Due Diligence (SDD) and Enhanced Due Diligence (EDD).

The following are the types of customers onboarded by Cassa Payment Services Co. LLC (CPS) and compliant procedures for onboarding:

5.1.1. Registration Stage

5.1.1.1. Individual or a Natural Person

An Individual customer is considered as a Natural Person either a Resident or a Non-Resident of UAE with a willingness to perform transaction with Cassa Payment Services Co. LLC (CPS) of purchase / sale or leasing of property for his own interest or for the purpose of leasing to the third party.

KYC Process to be adopted for Individual or Natural Person is as follows:

The customer to be registered by collecting following information:

- Full legal name
- Residential status (whether UAE Resident or UAE Non-Resident)
- Address in the UAE with house or apartment number with building name and mentioning proper State / Province or Emirate)
- PO Box Details if available
- Temporary address in the UAE and the permanent address in the home country (for UAE Non-Residents)
- Mobile number
- Email, if available
- Date of Birth
- Nationality
- Country of Birth
- ID type (Emirates ID / Passport Copy with Visa Page / National ID)
- Copy of ID to be retained taken from original document and to be stamped as "Original Sighted and Verified")
- ID number, ID place of issue, ID issue date and ID expiry date
- Profession
- Anticipated Property Investment Value (i.e., expected Investment value and number of units required for future transaction monitoring)

5.1.1.2. Legal Entity or a Corporate Entity

Legal Entity or a Corporate Customer to be registered by collecting following information:

- Full Legal Name
- Legal form
- Date and Place of incorporation
- Registration Number
- Trade License
- Registered Address and Trading address
- Type of Business activity
- Name of the Owners / Partners
- Identification documents of Owners / Partners
- Representative Name
- Identification documents of Representative
- Authorized Signatory letter to perform transaction (for Transaction Purpose)
- Anticipated Property Investment Value (i.e., expected Investment value and number of units required for future transaction monitoring)

5.1.2. Name Screening

At this stage, name screening of all the parties to be done against the UAE Local List and United Sanctions List and PEP List The following categories to be identified for further procedures:

- Positive Match – Implement 'Freeze and Suspend' measures and file FFR
- Partial Match – Suspend all transactions until further instructions and file PNMR
- Negative Match – Approval for onboarding of the Customer
- PEP Match – To be escalated to the senior management for approval and onboarding of the customer and perform adverse media search either on Google or any other reliable database
- Follow Name Screening process. (Refer Point 5.4)

5.1.3. Due Diligence

Due diligence is conducted based on the ML/FT risks posed by a customer. For customers who are assessed to be of Low or Medium risk, a Simplified Due Diligence (Refer point 5.2) may be conducted, whereas for High Risk customers, Enhanced Due Diligence measures (Refer point 5.3) are to be implemented.

5.1.4. Collection Agent or a Broker

For a Payment Service Provider Agent or a Broker all activities to be performed as mentioned in legal or corporate customer on boarding except that of Source of Funds Identification if the agent or broker is performing transaction on behalf of the customer and not for his own entity.

Agent Agreement form and other documentation are to be collected as per the CPS internal policy and Agent onboarding process.

Follow name screening process for Payment Services Provider. (Refer Point 5.1.4)

5.2. Simple Due Diligence (SDD)

The main purpose of Simple Due Diligence (SDD) is to know and understand a client's identity and business activities so that any ML/TF risks can be properly identified and managed. Effective SDD is, therefore, a key part of AML defenses. By knowing the identity of a client, including who owns and controls it, a business not only fulfils its legal and regulatory requirements it equips itself to make informed decisions about the client's standing and acceptability.

SDD also helps the company to construct a better understanding of the client's business activities. By understanding what the normal practice is, it would be easier to detect abnormal events, which, in turn, may point to ML/TF activity.

The company's policy is to conduct SDD for all its new and existing clients, irrespective of the associated risk.

SDD must be carried out based on the following event:

- At the start of a new business relationship (including a company formation),
- When an occasional transaction is to be undertaken,
- When there is any doubt about the reliability of the identity information, or documents obtained previously for verification purposes,
- When the company has a legal duty to contact a client and the duty includes a requirement to review information related to the ownership or control structure of the client or any beneficial owners.
- When there is a change in the ownership or legal structure of a client.

5.2.1. Steps in conducting SDD:

1. Obtaining all critical documents specified in KYC section 5.1.
2. Identification and confirmation of customer information and structure such as:
   - Ultimate Beneficial Owner (UBO) of legal person
   - Documents collected are of customer only
   - In case of third party involved, documents as per the registration stage shall be collected for third party also
   - Customer profile and value of investment – Customer status and ability to invest
   - Collection of sources of funds (for individual with business source and corporate entities)
   - Cash limits as per internal policy
   - Application of Risk Based Approach (RBA) to identify risk level of the customer
   - Memorandum of Association – Detailing Activity of the Business of legal person
   - Follow Transaction Monitoring process. (Refer Point 5.5)
3. Upon compiling all related documentation, the company carries out risk assessment based on the areas such as client risk, product/service risk, geographic risk, and delivery channel risk.

4. In carrying out the risk assessment, risk profiling will be completed, and each risk profile will include the aspects under section 4.
5. Verification of documents obtained will be done via checking original and signing off as the original has been seen & checking with relevant authorities.

In the event the company unable to complete SDD, the company exercises the following:

- Immediately terminate any relationship with the customer
- Consider whether it should make a suspicious transaction report to FIU.

When delays occur – Limited time extensions could be permitted if the customer is deemed to be low risk towards AML/CFT issues and has not shown reluctance to provide documents. Business relationship could be commenced but during the permitted time SDD should be completed - if not, the business relationship should be ceased.

5.2.2. Additional SDD requirements:

a. If there is a change to the signatory or the beneficiary of an existing contract or business relationship.
b. There are material changes in the way the account with the legal person is operated or material changes in the manner of conducting business relationship.
c. A significant transaction is made
d. The company has doubts about the veracity or adequacy of previously obtained SDD information and documents.
e. There is a significant change in the documentation and a vast difference in Business operations.

5.3. Enhanced Due Diligence

Under the AML/CFT Law, the Company is under obligation to conduct Enhanced Due Diligence for the customers who carry high risk levels in terms of ML/TF. EDD takes place where the company conducts an in-depth assessment of the customer, where additional information will be requested from the client and strict verifications will be carried out.

The company carries out EDD on the following events.

a. in cases where it is required to do so under the AML/CFT Law,
b. in any other case that by its nature can present a higher risk of money laundering or terrorism financing,
c. in cases where the regulator makes changes in the required EDD procedures,
d. where a reporting person discovers that a customer has provided false or stolen identification documentation or information and the reporting person proposes to continue to deal with that customer, and
e. In the event of any unusual or suspicious activity.

5.3.1. EDD measures include but are not limited to.

1. Obtaining additional information on the customer through:
   - Occupation
   - Volume of assets
   - Information available through public databases
   - Internet
2. Updating more regularly the identification data of the customer and the beneficial owner.
3. Obtaining additional information on the intended nature of the business relationship.
4. Obtaining information on the source of funds or source of wealth of the customer.
5. Obtaining information on the reasons for intended or performed transactions.
6. Obtaining the approval of senior management to commence or continue the business relationship.
7. Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
8. Where Cassa Payment Services Co. LLC (CPS) determines that the beneficiary who is a legal person or legal arrangement presents a higher risk, enhanced due diligence measures will be taken to identify and verify the identity of the beneficial owner of the beneficiary at the time of payout and those include:
   - assessing the risks posed by a legal person or legal arrangement, obtaining additional information of beneficial owners, officers, shareholders, trustees, settlors, beneficiaries, managers, and other relevant entities.
   - assessing the risks posed by a facility the company would consider of reduction in transparency, or any increased ability to conceal or obscure, and
   - subrules above do not limit the matters to be reflected in the risk profile of a legal person, legal arrangement, or facility.
   - enhanced ongoing monitoring for customers from high-risk jurisdictions whose line of business is more vulnerable to corruption.
   - In the event the company is unable to complete EDD, it will:
     a. not proceed with the business relationship
     b. Submit an STR/SAR as per section 5.6
     c. For existing customers engagement should be limited or ceased with the consent of the authority, where applicable.

5.3.2. Politically exposed person (PEP)

The handling of a client who is no longer entrusted with a prominent public function shall be based on an assessment of their risk. Family members and known close associates of PEPs are treated as High risk on this basis as well.

If the company intends to enter, or continue, a business relationship with PEP it will carry out EDD, which includes:

- senior management approval for the relationship
- adequate measures to establish sources of wealth and fund
- enhanced monitoring of the ongoing relationship and number of transactions performed by the PEP

The nature and extent of EDD measures will vary depending on the levels of ML/TF risk associated with individual PEPs.

5.3.3. Other special risk flags

Irrespective of the risk score otherwise obtained for a customer, the Company will conduct EDD and enhanced ongoing monitoring on that customer if they are flagged as one the below special risk flags:

- legal person, legal arrangements, and facilities with highly complex structures
- has an adverse presence or media reports in connection with money laundering and / or predicate offence
- makes unusual requests of the real estate agency, brokerage, or its employees
- other matches at the time of name screening

A decision to enter into a business relationship with such customers will only be taken with senior management approval after EDD has been conducted.

5.3.4. Ongoing Monitoring of real estate transactions

Due to the transactional nature of the real estate sector, and the limited access to customers' financial transactions in many instances, it may not always be possible for the company to perform ongoing monitoring of their customers' activity. Nevertheless, in circumstances in which High-risk customers have been identified, the Company will make reasonable efforts to monitor activity related to properties with which it has been involved.

- reviewing transactions based on an approved schedule and obtain management approvals.
- developing and reviewing reports of linked high-risk transactions more frequently.
- flagging certain activities or those that deviate from normal expectations and raise concerns, as necessary.
- setting business limits or parameters on accounts or transactions that would trigger early warning signals and require a mandatory review; or
- reviewing transactions more frequently against suspicious transaction indicators relevant to business relationships.

5.4. Name Screening:

Cassa Payment Services Co. LLC (CPS) is registered for the updates at EOCN website for Local Terrorist List and UN Consolidated list.

As a Payment Services provider, Cassa Payment Services Co. LLC (CPS) owes a responsibility towards the screening names and addresses against UN Consolidated Sanctions and UAE Local list which is compiled and updated on a regular basis and kept in records for the purposes of identifying designated and prohibited individuals and entities, PEPs and other high- risk entities who may pose a threat to the international community at large. Name screening should be done for all the customers of the organization and for all the onboarding of the relations and related parties.

5.4.1. Requirements:

- Cassa Payment Services Co. LLC (CPS) should follow the strict adherence to the name screening on each transaction and ensure that no transaction is done with the customer's name that appear in any list (of known specially designated nationals (SDN) or suspected terrorists or terrorist organizations or any blacklist provided by the UAE Regulatory Authorities
- Cassa Payment Services Co. LLC (CPS) ensures that the name screening is done on a regular and transactional basis.
- Cassa Payment Services Co. LLC (CPS) conducts screening of each customer and beneficiary against the mentioned list.
- In the event that there is a possible match of a customer name with that of the blacklist, the transaction is put on hold.
- The details of the name match on the SDN list are checked against details of the customer and beneficiary.
- In the event of an exact match i.e., it is determined that the name is on the blacklist, the transaction is withheld and immediately reported to the Financial Intelligence Unit (FIU) and the regulatory authority.
- Cassa Payment Services Co. LLC (CPS) understand that the failure to report the same could result in fines, penalties, reputational and commercial loss.
- In the event the details of the customer do not match with the SDN list, the transaction and onboarding are released for further processing.
- The blacklists will be updated on a regular basis to avoid omission of names which may be recently added or deleted by the above-mentioned authorities.
- Cassa Payment Services Co. LLC (CPS) maintains its internal watch list for addition and deletion of the persons with whom the company does not want to deal with according to the risk he/she may expose the company to.
- Any customer/UBO that is identified a PEP is escalated for the approval of the Owner and Partner with the detailed EDD on the customer.
- The logs related to the screening should be kept for 5 years from the date of transaction for records.

5.5. Transaction Monitoring:

The Payment Services sector has come under immense regulatory pressure to improve and expand monitoring and surveillance of transactions for the purposes of preventing and detecting money laundering and CTF activities.

A well-defined Transaction Monitoring Program is an important component of an effective AML and CTF program. Transaction monitoring in the simplest form means to collect and analyze the transactions processed by a customer.

5.5.1. Objective:

The primary objective is to concentrate on actual risks, customer, and product classification and to reduce the number of chances of Cassa Payment Services Co. LLC (CPS) from being misused for money laundering and funding of terrorist activities. This can be explained as:

- To ensure that all transactions conducted through Cassa Payment Services Co. LLC (CPS) comply to the laws and regulations both locally and internationally.
- To assess the transactions of all customers, so to see whether they are in line with his profile or known business activity.
- To identify suspicious activity which might lead to money laundering that may ultimately result in the filing of a Suspicious Transaction Report (STR).
- To realign the risks associated to a customer, product, and service.
- To strengthen our KYC and EDD procedures

5.5.2. Rules for Transaction Monitoring – 5W's

The basic rules to be applied while monitoring transactions. Monitoring may be done through automated or a manual process to identify unusual transactions and different trends in a single or set of transactions.
Compliance personnel should always keep in mind the 5 "W" while analyzing transactions,
The 5 W`s are:

- **Who** - is the customer- individual or corporate, what is the profile of the customer?
- **What** - product is the customer availing?
- **Where** - is the customer? Is the country a high-risk jurisdiction? Is there a valid reason for transacting from that country?
- **Why** - is the customer taking property? Does the transaction make economic sense to the nature of business and investment?
- **Whom** – for whom the transaction is being conducted, who will benefit from the transaction? Who is the Ultimate beneficiary?

Transactions should be ideally monitored on the same or successive day to check if there is any breach of rules or suspicion. Certain rules to identify specific patterns of behavior are listed below which may be used in transaction monitoring are given in the table below:

Sr. No	Rule Name
1	High Value - Single transaction (Natural Person)
2	High Value - Single transaction (Legal Entity)
3	High Value transactions – Multiple Booking of Properties (Natural Person)
4	High value transactions – Multiple Booking (Legal Entity)
5	Transaction count – No of Units Booked (Natural Person)
6	Transaction count – No. of Units Booked (Legal Entity)
7	High Risk Country Bank Transfer – Inward or Outward Request
8	Nationality
9	Multiple Location / Broker transactions
10	Cash payments by Natural Person / Legal Entity
11	Beneficiaries name which can be identified as institutions for Charity, Social and
12	Watch List Customer/ Hit on Name Screening
13	Employee transacting beyond his income Limit and behalf of someone else
14	Third Party Payments on behalf of the Customer

5.6. ISTR and STR Procedures:

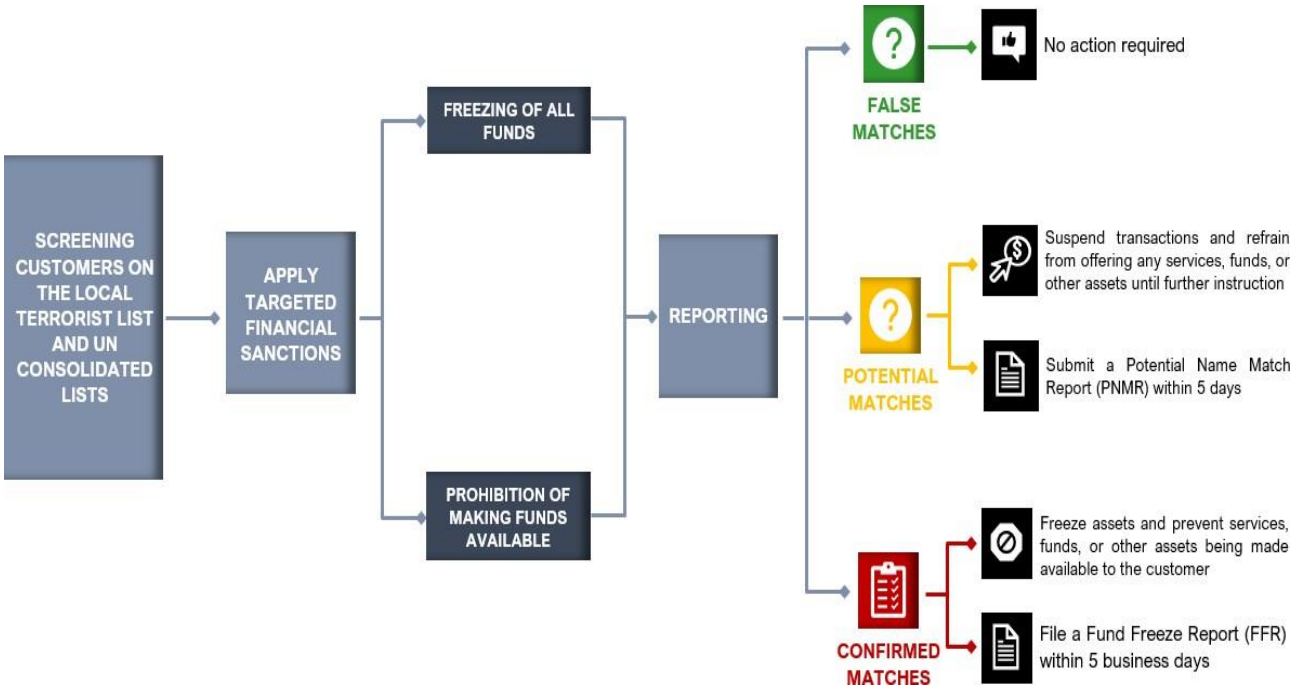
As a primary requirement of submitting Suspicious Transaction Reports (STR), Cassa Payment Services Co. LLC (CPS) has obtained access to goAML, the online STR reporting portal of the Central Bank.

All employees of the Cassa Payment Services Co. LLC (CPS) 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 Cassa Payment Services Co. LLC (CPS) is not used to aid the transfer of illegal money for money laundering and terrorism financing.

DNFPB's 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 Financial Intelligence Unit (FIU).

5.6.1. Procedures:



- All employees are required to report any potentially suspicious or unusual transactions.
- The reporting must be done with full facts of the case within a reasonable time.
- It is the 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 (FIU).
- It is important to note that the "time factor" in reporting suspicious transactions remains crucial; if the company can 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.

5.6.2. Terrorism Financing

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:

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

5.6.3. Other Reporting Requirements

The Compliance Officer is responsible for adhering to additional reporting requirements as applicable to the real estate sector and to DNFBPs in general including filing the below reports via the GoAML portal in the following cases:

- Real Estate Transaction Report (“REAR”) on purchase and sale transactions where any single physical cash transaction or several transactions equal to or exceeding AED 55,000 for the entire, or a portion, of the property value.
- Real Estate Transaction Report (“REAR”) purchase and sale transactions where the method of payment is a virtual asset (or converted from a virtual asset) for a portion or the entire property value.
- High-Risk Country Transaction Report (“HRC”) or High-Risk Country Transaction Report (“HRCA”) upon identification of customer transactions or activities related to high-risk countries.

5.6.4. 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.

5.7. Red Flags, Unusual, Suspicious Customer and Transactions

Few key indicators of suspicious Customers and Transactions are: -

- Reluctant to provide identity Documents – Natural or Legal Entity
- Acting on behalf of the customer and refusing to provide details of the beneficial owner
- Mismatch of the customer profile and proposed investment
- Refusing to provide source of funds
- Booking of Multiple units within short period
- Multiple units booked under family member's name
- Payment arrangements through exchange houses
- Use of complex loans, credit finance, or investment schemes
- Shell Company formation documentation
- Reluctant to provide information on Business Activity
- Is a foreign national with no significant dealings in the country, and no clear economic or other rationale for a real estate transaction in the country
- Is a politically exposed person or has familial or professional associations with a person who is politically exposed
- Non-Availability of social media presence or internet searches

5.7.1. Third party Red Flags:

- Gatekeepers such as accountants, lawyers, or other professionals holding power of attorney, act on behalf of their customers, and where the investment has an unreasonable reliance on the gatekeeper.
- The customer changes the beneficiary clause and nominates an apparently unrelated third party.
- Payments are regularly received from third parties that have no apparent relationship with the beneficiary owners.
- Use of corporate vehicles

5.8. KYE

Know Your Employee policy should be conducted have the following stages.

a. Pre- Employment Stage
b. Course of employment
c. Employee Conduct

5.8.1. Pre – Employment Stage:

Due diligence in KYE starts at the recruitment stage, to know if the promising candidates are telling the truth.

At the initial stage references should be checked; a reference check can be done by the organization or by outsourced agencies.

References of a prospective employee - You can verify if there is any criminal conviction which can be achieved by obtaining:

- A Police Clearance Certificate (PCC) from the police station of the last known residences.
- The relieving letter from the previous employer(s).
- The past employer can be asked to provide details like whether they really worked for the company stated on the CV, other employment credentials such as designation, role, compensation, conduct and reason for leaving etc.

- How was the conduct of the prospective employee?
- References provided by the prospective employee can be requested to provide information.
- The references given by the candidate shall be contacted and affirmed (First degree relations should not be hired).
- In case the verification or background check services are provided by a vendor, the company must ensure the standards and procedures the organization applies while conducting the check - Are their standards comparable to yours? Are their procedures reviewed by an independent firm?
- Screening of Employee names against the sanctions list.

5.8.2. Course of Employment:

Even though the reference checks have been applied, it is advisable to have random checks to ensure that the employee maintains its responsibility to be a trustee of the organization. It is good management practice to monitor your employees' performance and understand what makes them stick, but this routine procedure can also unearth internal threats to your business.

5.8.3. Employee Conduct:

Signs which could raise a signal for verifying the employees conduct and behavior:

- Staff Behavior: A change in the employee's lifestyle, especially when spending by an employee sees a drastic change than what an employee at the same level could afford.
- Credit cards/Loans: The employees availing frequent loans and credit cards should pose a question for the employer. Too many approvals and NOCs provided to employees can not only lead to defaults but can also cause the organization to be blacklisted for getting further benefits from banks etc.
- Overzealous nature and relation with select customers: There could be possibilities of customers offering bribes and commissions to employees for conducting frauds, embezzlements and money laundering, Frequent checks, and controls on the activities of employees can help detect these activities at an early stage.
- Timing: Many a times employees employed in critical areas of operations and accounts have been caught for internal fraud etc. These employees have been reported to have long working hours, coming early before the scheduled time to the office, sitting till late in the office and rarely taking annual vacations.
- Compromising on data and system integrity: Employees who have often been reprimanded for misuse of confidential data and systems should be monitored closely to mitigate any risk of fraud.

6. INDEPENDENT REVIEW:

A robust AML Compliance program shall be complete where a periodic review to assess the adequacy the policies and procedures, compliance officer's functions and other controls is performed.

The purpose of independent review is to review and test whether the policies, procedures and controls are in line with the regulatory guidelines and to suggest changes and modifications in procedures to have more effective controls in the fight against money laundering and terrorism financing.

6.1. Guidelines:

Both internal and external audits play an important role in evaluating the procedures of Cassa Payment Services Co. LLC (CPS):

a. External Audit: means testing of the internal procedures by an independent party i.e., performed by people not from within the company. The auditors must be sufficiently qualified to ensure that their findings and conclusions are reliable. It is advisable to conduct the independent testing by an external audit firm shall be on an annual basis.

b. Internal Audit: these audits may be performed internally within an organization if there is a provision of an internal audit department or could be outsourced to efficient partners.
   - There should be a well-defined audit program and checklist.
   - The frequency of such audits may be once in 6 months.
   - The auditor should report directly to the to the Owner / Partner for its findings.

6.2. Scope:

- Examine the adequacy of due diligence policies, procedures, and processes, and whether they comply with internal requirements.
- Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers, and geographic locations) on sample testing basis.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Assess compliance with applicable laws and regulations.
- Examine the integrity and accuracy of management information systems used in the AML compliance program if any.
- Reviewing policies, procedures, and processes for suspicious activity monitoring.
- Determining the system effectiveness for reports, blacklist screening, flagging of unusual transactions and more.
- Review Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transactions. Testing should include a review of policies, procedures, and processes for referring unusual or suspicious activity from all business lines to the personnel or department responsible for evaluating unusual activity.
- Assess the adequacy of recordkeeping.

7. TRAINING:

The role of AML and CTF training in a dynamic business environment is to be a partner to the employees to help them achieve their objectives. This is achieved by developing the knowledge and skills of the employees. The success of learning results from its integration with the business plan and the business culture. Hence the prime objectives for Training are:

- To enhance existing knowledge and skills of employees to enable them to successfully accomplish their duties and responsibilities.
- To upgrade the Product Knowledge of Front line / Operations and Sales Staff.
- To adhere to the guidelines of the regulatory authority on employee training.

7.1. Mandatory Teams for Trainings:

7.1.1. New employees – Induction Training

Newly joined employees need to undergo Induction program covering AML/CFT awareness and company's procedural guide, within fifteen days from joining. This training can be conducted internally by the qualified staff from AML/Compliance Department or through external vendor having expertise in trainings and AML/CFT Knowledge.

7.1.2. Front Line Staff – Induction and Refreshers Training.

All sales staff acts as a first line of defense for AML/CFT program and needs to be trained on an annual basis. This training can be conducted internally by the qualified staff from AML/ Compliance Department or through external vendor having expertise in training and AML/CFT Knowledge.

7.1.3. AML Compliance Department – Continuous Professional Development (CPD)

All the employees and members related to AML/Compliance Department shall undergo a continuous professional development program every year. This training can be earned through.

a. AML/CFT conferences or meetings or workshops whether inside or outside the UAE.
b. face to face training by external agencies whether inside or outside the UAE.
c. training by industry associations or regulatory bodies; and
d. Web based training

7.1.4. Auditors:

Auditors acts as a third line of defense for AML Program, hence needs to undergo Awareness and Assessment Training program to audit the operational and AML program implementation of the company. It is advised to conduct external training program for auditor's minimum once in a year.

7.1.5. Senior Management – AML Awareness Program

Senior Management and Board of Owners should undergo AML Awareness, Governance and Risk Framework, Latest updates on laws and regulations, minimum once in a year. This training shall be organized through the external agencies.

7.2. Topics:

The topics for AML and CTF training should focus on the different levels of employees, i.e., whether the employee is a customer facing employee, a supervisor or branch head or a back-office employee.

The medium and topics of training should be made available as per the nature of the role an employee is working in. The training mediums may be in the form of classroom sessions, circulars, e-learning modules, corridor specific trainings, role plays.

The topics should include:

7.2.1. General information:

Background and history pertaining to money laundering controls, what money laundering and terrorist financing are, why the bad guys do it, and why stopping them is important.

7.2.2. Legal framework:

How the AML Laws apply to institutions and their employees

7.2.3. Responsibility:

Responsibilities of the employees under local laws and regulations for obtaining sufficient evidence of identity, recognizing and reporting knowledge or suspicion of money laundering and terrorist financing.

7.2.4. Penalties:

Penalties for anti-money laundering violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment.

7.2.5. Other Topics:

How to react when faced with a suspicious client or transaction and Procedure for reporting of suspicious transactions, how to respond to customers who want to circumvent reporting requirements and Internal policies, such as customer identification and verification procedures and other topics such as below:

- Due Diligence policies
- What are the legal recordkeeping requirements?
- Red flags
- Suspicious transaction reporting requirements
- Duties and accountability of employees
- Fraud Prevention
- Tipping off

8. RECORD KEEPING:

Records should be kept and made available to Regulatory examiners and for investigation for minimum of 5 years. The objective for records keeping is to ensure that the company can provide the basic information to reconstruct the transaction undertaken, at the request of the relevant authorities.

8.1. Document retention:

The records prepared and maintained by the company must be such that:

- The requirements of the law and expectations of the regulator or the supervisor are fully met; and
- Auditors, reporting accountants, and regulators or supervisors are able to assess the effectiveness of CPS's AML/CFT policies and procedures.
- Any transaction or instruction conducted through CPS on behalf of any individual customer can be reconstructed.
- Any customer or underlying beneficial owner can be properly identified.
- All suspicious transaction reports received internally, and those submitted to the financial intelligence unit, can be identified; and
- The company can meet, within the required time frame, any inquiries or court orders from the appropriate law enforcement agencies.

8.2. How long should records be retained?

- The minimum periods for which records must be maintained to comply with the requirements of the law are outlined in the following table.

Type of Account	Length of Retention
Account opening records and documentary evidence of identity	At least 5 years after Account Closure
Account ledger records	At least 5 years
Individual transaction records	At least 5 years
Results of any analysis undertaken (e.g., inquiries to establish the background and purpose of complex, usual large transactions)	At least 5 years after Account Closure
Information after the account has been closed or after the last transaction	At least 5 years
AML Training registers	At least 5 years

Records relating to a customer's identity must be retained for at least 5 years from the date of closure of business with the client. The date on which the relationship with a customer end is the date of:

- carrying out a one-off transaction or the last in the series of transactions; or
- ending of the business relationship, that is, the closing of an account.

9. FINES AND PENALTIES

As per Federal Decree – Law (20) of 2018 the Regulator has the authority to impose the following administrative penalties on the financial institutions, designated non-financial businesses and professions and non-profit organizations in case they violate the present Decree-Law and its Implementing Regulation:

a) Warning
b) Fines of no less than AED 50,000 (fifty thousand dirham) and not more than AED 5,000,000 (five million dirham) for each violation.
c) Banning the violator from working in the sector related to the violation for the period determined by the regulatory authority.
d) Constraining the powers of the Board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointment of temporary inspector.
e) Arresting Managers, board members and supervisory and executive management members who are proven to be responsible of the violation for a period to be determined by the Supervisory Authority or request their removal.
f) Arrest or restrict the activity or the profession for a period to be determined by the supervisory authority.
g) Cancel the License.

Further, the Regulatory Authority publishes the administrative penalties through various means from time to time, as below:

- Cabinet Decision No (16) of 2021 regarding the Unified List of the Violations and Administrative Fines for the Said Violations of Measures to Combat Money Laundering and Terrorism Financing
- Federal Decree Law No (26) of 2021 to amend certain provisions of Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations

10. ANNEXURES

10.1. KYC Form

CPS - KYC form.docx

10.2. List of Country Risk Ratings as of February 2024

CPS - Know Your Country Ratings - 20

10.3. List of Red flags

Payment Services Sector - Redflags.docx

10.4. Sample Risk Assessment Process for Money Laundering

Risk	Score	Total band
High	3	>8
Medium	2	4-8
Low	1	<4

#	Name of customer	Service Risk[1]		Geographic Risk[2]		Delivery Channel Risk[3]		Customer Risk[4]		Total
		Detail	Score (S)	Detail	Score (G)	Detail	Score (C)	Detail	Score (D)	(S+G+D+C)
1										
2										

[1] Service Risk

Parameters	Risk
Leasing	High
Other	Medium

[2] Geographic Risk

Refer Annexure 10.2

[3] Delivery Channel Risk

Parameters	Risk
Face-to-face	High
Video call	High
Other methods	Low

[4] Customer Risk

Parameters	Risk
Designated Non-Financial Business/Profession	High
Financial Institution	High
General Trading	High
Other Cash Intensive Business	High
Politically Exposed Person, their relatives, or close associates	High
Special Interest Person	High
Sanctioned Person	High
Adverse Media	High
Other suspicious indicators	High
All Other	Low