Bahrain

Anti-Money Laundering & Counter-Terrorist Financing Policy

Role	Position
Policy owner	Compliance officer and MLRO
Approved by	Board of Directors
Version	2.0
Status	Approved
Last Reviewed Date	July 2025
Date of Next Review	March 2026
Distribution List	Management and Internal Audit

FASSET®

Contents

1. Introduction

1.1. Purpose & Objective

Fasset is a registered virtual asset service provider (VASP) which offers a variety of consumer products and services that are accessible through various Fasset branded channels including a mobile application and website.

As an asset service provider, Fasset might be used by criminals to commit financial crimes. Financial crimes is a term used to describe a variety of criminal acts, including money laundering, terrorist financing, tax evasion, sanctions violations, fraud and other types. To mitigate the risks, Fasset will introduce a number of systems and controls, including this Policy.

The **Bahrain Anti-Money Laundering (AML) Policy** ("The Policy") sets out the responsibilities of Fasset, its employees and anyone who performs services for or on behalf of the Fasset (collectively "Associated Persons[1]") in observing and upholding Fasset's commitment to detecting and preventing money laundering, terrorist financing and other forms of financial crime. Additionally, it sets out Fasset's standards in complying with applicable sanctions laws and regulations in every jurisdiction in which it operates.

1.2. Background & Governance

This Policy establishes the minimum standards of financial crime compliance that must be adhered to across all entities of Fasset. Fasset commits to following international standards for financial crime prevention, as outlined by leading global organizations such as the Financial Action Task Force ("FATF"). Specifically, Fasset aligns with:

- The FATF Recommendations, as amended, provide a comprehensive framework for actions national governments should take to combat money laundering and terrorist financing.
- FATF Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, detailing how entities in the digital asset space can effectively manage risks.
- Reviews of Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, assessing progress and compliance within the sector.

[1] Associated Persons may include relevant related third parties including agents, business partners or appointed representatives within or outside Fasset

Furthermore, this Policy recognizes the importance of adhering to the prevailing laws and regulations in the jurisdictions where Fasset operates. It emphasizes compliance with both international guidelines and local regulatory requirements to ensure a robust defense against financial crimes.

In instances of discrepancy between this Policy's requirements and local regulations, the principle of adhering to the stricter set of rules will be applied to ensure the highest standard of compliance is maintained.

1.3. Scope & Applicability

This Policy applies globally across Fasset and aligns with relevant international standards and guidance. Each legal entity within the global group will maintain its own policies to ensure compliance with applicable local laws and regulations.

All Fasset employees and Associated Persons, including consultants and contractors, regardless of department or job function—are required to adhere to this Policy.

The Compliance Team is responsible for maintaining this policy. It is reviewed annually or updated as necessary in response to material changes in Fasset's business operations, regulatory requirements, or industry's best practices. Any material amendments must be approved by the Board.

Once updated, the Policy is distributed to all Fasset employees and relevant Associated Persons, published on the Intranet, and accompanied by training as required.

1.4. Requirements, Compliance & Reporting

Fasset and its employees and associated people are required to adhere to the Policy and the laws and regulations undertaking it. Failure to comply with this Policy and any underlying procedures may result in personal liability, such as fines and imprisonment, as well as consequences within Fasset itself, from an internal warning up to and including employment termination (for employees) and termination of the relationship (for relevant third parties). In addition, it could expose Fasset to civil and criminal liability, fines, reputational damage, operational risk, and other serious consequences.

Any circumvention of this Policy is absolutely prohibited. Any deviation from this Policy must be approved by the Head of Compliance Department and appropriately documented. Fasset expects all employees and Associated Persons to report any violation or suspected violation of this Policy, as well as suspected financial crime or potentially suspicious activity to the Head of Compliance Department or the respective local Money Laundering Reporting Officer (MLRO) or Compliance Officer (CO).

Material breaches, including, but not limited to situations in which a regulatory requirement has not been met, must also be reported to the Head of Compliance for further review.

2. AML Program

Fasset has established policies and procedures to mitigate and effectively manage the risks of money laundering and terrorist financing specific to Fasset. Fasset's AML Program is risk-based and designed to detect and address these risks and it takes into account the findings of the Financial Crime Risk Assessment (FCRA), which is performed annually. The Program includes:

- Senior Management Oversight
- Financial Crime Risk Assessment
- Financial Crime Risk Appetite Statement
- Internal Controls
- Staff Training Program
- Independent Testing and Audit

Each of the Program's elements is outlined below.

2.1. Senior Management Oversight

Fasset has appointed Head of Compliance who is responsible for the oversight of Fasset's compliance with relevant laws, rules and regulations. Head of Compliance has the day-to-day responsibility for overseeing the implementation of, and monitoring compliance with the AML Program.

In addition, each Fasset's entity will appoint, where required by law, a local Compliance Officer ("CO") or Money Laundering Reporting Officer ("MLRO"), who will be responsible for Fasset's compliance with local laws and regulations. COs and MLROs will have the remit to receive and review internal disclosures of suspicious activity and file external reports with relevant agencies where appropriate.

2.2. Financial Crime Risk Assessment (FCRA)

In accordance with this Policy, Fasset conducts an annual Financial Crime Risk Assessment (FCRA) to evaluate risks arising from market changes, new or evolving products, customer profiles, and the broader regulatory and operational environment. Through the FCRA, Fasset identifies financial crime risks and assesses the effectiveness of its existing controls.

When conducting the FCRA, Fasset follows the best international practices for risk assessments, including:

- **FATF Guidance** for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (October 2021)
- **FATF Virtual Assets Red Flag Indicators** of Money Laundering and Terrorist Financing
- **European Supervisory Authority's Risk Factor Guidelines** (2018)
- **The Wolfsberg Group Guidance** on a Risk-Based Approach for Managing Money Laundering Risks (2006)

The FCRA is designed to enhance Fasset's understanding of its risk exposure and to inform the prioritization of resources for AML/CFT efforts. This includes assessing financial crime risks associated with the development and use of virtual assets, both for new and existing products and services.

Fasset's FCRA Methodology

The FCRA considers key risk factors, including:

- **Nature, scale, and complexity of the business**, including transaction volume and operational processes
- **Geographical locations** of Fasset's customers and business operations
- **Customer characteristics**, including risk profiles and behaviors
- **Products and services offered**, including those with enhanced anonymity features
- **Delivery channels** used for customer onboarding and transaction execution
- **Technologies** associated with virtual asset activities

If AML/CFT and financial crime risks cannot be adequately mitigated, Fasset will not offer such products or services or onboard clients presenting excessive risk.

The FCRA is conducted annually or whenever there is a significant change in the business—such as expansion into new customer segments, introduction of new products or services, or adoption of new delivery channels—to ensure that emerging risks are identified and assessed in line with both internal trends and external developments.

The Compliance Team, including the Compliance Officer and MLRO, is responsible for conducting the FCRA, while the Head of Compliance is responsible for its approval. If the FCRA identifies gaps in existing controls or the need for additional measures, Fasset must ensure that these gaps are appropriately addressed and that necessary controls are implemented.

2.3. Internal Controls

Fasset must ensure that its internal systems and controls are reasonably designed to deter, detect, and require the reporting of known or suspected money laundering, terrorist financing or any other form of financial crime. Fasset will implement the following risk-based controls to address this:

- Designation of an AML Officer
- Know-Your-Customer Program
- Transaction Monitoring Program
- Suspicious Activity Reporting

2.3.1. Designation and Duties of Compliance Officer & MLRO

In order to oversee the effective implementation of the internal compliance policies and procedures, Fasset has a designated Head of Compliance, who has obligatory reporting duty to the applicable Executive Board ("Board"). The Head of Compliance is responsible for coordinating, managing, and monitoring the AML and CTF Compliance Program, and ongoing compliance with the applicable AML rules and regulations. The Head of Compliance may act as the Compliance Officer (CO) or Money Laundering Reporting Officer (MLRO), who will perform regular internal reviews to ensure that Fasset is in full compliance with all the necessary requirements.

The CO / MLRO is appointed in the local jurisdictions where there is a Fasset Business Unit or where there is a Fasset-country entity registered as a virtual asset service provider. A resident MLRO may not be appointed for every local jurisdiction; in some instances, a Fasset Compliance Officer may be designated as the MLRO for more than one country.

The designated and appointed MLRO shall possess the minimum years of experience mentioned in the local legislation handling AML/CFT matters; and is considered as a Fit and Proper Person who possesses the necessary skills, qualifications and experience for the responsibilities.

The CO / MLRO shall be responsible for:

a. ensuring the Board and Staff are properly and adequately trained in respect of their understanding and compliance with all applicable AML/CFT laws and regulatory requirements, particularly those relevant to virtual asset activities.
b. developing and implementing AML/CFT policies and procedures while complying with local and international regulations delineated in this policy.
c. conducting AML/CFT risk assessments in accordance with FCRA guidelines of this Policy and implementing all necessary changes to Fasset's relevant policies and procedures to address such issues and risks.
d. monitoring and reporting Suspicious Activity and Transactions in accordance with this Policy and Internal SAR Procedure.
e. if necessary, ensuring appropriate corrective actions are taken in response to noncompliance with any local AML-CFT Laws.

f. reporting to the Board on a quarterly basis on the effectiveness of Fasset's AML/CFT policies and procedures, identifying any failures in such policies and procedures and/or any non-compliance with any AML-CFT Laws. The CO/MLRO in this report shall include a summary of all Anonymity-Enhanced Transactions and clients involved during that quarter. Additionally, the CO/MLRO shall make these reports available to regulatory authorities of respective operative jurisdictions.

The CO / MLRO may delegate AML/CFT activities to appropriate Entities, provided that the CO / MLRO shall continue to be held accountable for all responsibilities and obligations in relation to the implementation of the relevant policies and procedures, and all applicable requirements of this Policy, Compliance Policy, and outsourcing management.

2.3.2. Know-Your-Customer Program

Fasset established a risk-based Customer Onboarding Program which ensures the appropriate Customer Due Diligence (“CDD”) is executed to record information and obtain documents to identify and verify the identity of each customer who opens an account with Fasset and to assess the potential financial crime risks within those relationships. Fasset takes into consideration regulatory requirements, applicable industry best practice, and the latest developments in regulatory technology to design and implement its KYC program. A brief overview of Fasset’s customer due diligence processes is provided below.

Fasset may rely on third parties to perform CDD, in which case Fasset shall remain liable for ensuring such third parties perform CDD in accordance with all relevant Rules and Directives. In such scenarios, Fasset shall implement adequate measures in keeping with the nature and size of its businesses to ensure that such third parties’ performance of CDD is in accordance with all relevant Rules and Directives.

2.3.2.1. Customer Due Diligence

The fundamental basis of effective AML/CTF controls is complete, accurate and up-to-date customer due diligence. Appropriately complete CDD allows Fasset to check that its customers are who they say they are and that the transactions and activities carried out with or on behalf of each customer are consistent with Fasset’s expectations.

2.3.2.1.1. CDD Requirements for Individuals

As part of the Customer Due Diligence (CDD) process, Fasset shall verify the identity of its natural person clients using reliable and independent sources. This includes reviewing the following documents, data, or information:

- **Full name** (as stated on an official identification document, such as a national ID card or passport)
- **Nationality**
- **Residential address**
- **Date of birth**
- **Place of birth**
- **Name and address of employer**
- **Occupation**

Fasset requires clients to provide a copy of a valid and original identification document, such as a National Identity Card or Passport, in accordance with applicable local regulations.

Politically Exposed Persons (PEPs)

If a client is identified as a Politically Exposed Person (PEP), approval from both the MLRO and a member of Senior Management is required before establishing a business relationship.

Additionally, Fasset continuously monitors CDD requirements to ensure compliance with evolving regulatory standards and best practices.

2.3.2.1.2. CDD Requirements for Legal Entities

Fasset shall require the customer (a legal entity) to provide registration documents or notarized copies thereof, confirming the authenticity of the copies, containing the following information:

- name;
- legal form, registered office (address), address of actual operation;
- registration number (if such number has been issued);
- an extract of registration and its date of issuance;
- nature and types of commercial activities.

When identifying legal entities, Fasset collects the below documents:

- Trade License
- Organization Chart
- Shareholder & Ultimate Beneficial Owner Chart
- List of Shareholders
- List of Directors
- List of Authorized traders (with ID copy and full residential address)
- Board Resolution for appointment of Authorized Traders or a letter designating the authorized traders signed by an authorized signatory.
- Regulatory Authorization or License Copy
- The original or certified copy of the Certificate of Incorporation and Articles of Associations / By-laws
- The resolution of the Board of Directors or other persons or bodies acceptable as per local law to open an account and identification of those who have authority to operate the account.
- Fasset Enhanced Due Diligence Form
- Certified copies of the list of authorized signatories
- Documents of registration to the trade registry
- Copy of AML Policies and Procedures (if applicable)
- Identification documents of the Executive Manager (CEO, Director);
- Identification documents of the representative (in case legal person is represented by person other than Executive Manager);
- Identification documents of ultimate beneficiaries (UBOs);
- other documents that may be required under local laws.

In addition, Fasset may request one or more of the following documents from the customer (where necessary):

- latest financial statements;
- board resolution;
- signatory lists;
- company structure.

2.3.2.1.3. Identification of the Beneficial Owners

Fasset must demonstrate that it has identified the beneficial owner when it has determined the identity of any of the following individuals:

- A natural person who directly or indirectly owns or controls a legal entity through a significant proportion of its shares or voting rights, including bearer shares. This excludes publicly listed companies on regulated markets subject to European Union legal requirements or equivalent international standards for business disclosure. A person who otherwise exercises control over the entity is also considered a beneficial owner.
- A natural person who holds at **least 10% plus one share** or a proportion exceeding 10% (or 10% for higher-risk cases) in the Customer's equity is considered the **direct owner**. A natural person or person who controls a company or a group of companies that hold a**t least 10% plus one shar**e or a proportion exceeding 10% in the Customer's equity are considered **indirect owners.**
- For **High-Risk Customers**, the ownership threshold is lower. A natural person who holds **at least 10% plus one share** or a proportion exceeding 10% in the Customer's equity is considered the **direct owner**. Similarly, a natural person or persons who control a company or a group of companies holding **at least 10% plus one share** or a proportion exceeding 10% in the Customer's equity are considered **indirect owners**.
- If no individual meets the criteria above, a natural person in a **senior management position** (e.g., a company director) shall be considered the **beneficial owner**

After the customer and the beneficial owner were identified, Fasset shall obtain from the customer – legal entity – information enabling Fasset to understand its ownership and management structure and nature of its activities (business).

Fasset ensures it appropriately identifies and verifies each customer as a natural or legal person based on the documents provided and/or other reliable resources as applicable per jurisdiction. Where a prospective customer does not possess the standard documents or cannot produce information required under the risk-based approach, consideration will be given as to whether there are other ways of being reasonably satisfied with the prospective customer's identity. Where the customer is a legal person represented by a natural person, or the customer that is a natural person is represented by another natural person, the identity of these representatives

shall be verified in the same manner as the identity of the customer that is a natural person. The same information must be verified about the director of the legal person.

Identification and verification of prospective customers is automatically supplemented with screening against all applicable sanctions, PEP and adverse media lists. This ensures Fasset has an accurate and ongoing understanding of its customers. All existing customers are also screened real-time on a daily basis due to the ever-changing and updated nature of mentioned lists and databases.

When the prospective customer has been identified, verified, and checked against the PEP database, Sanctions lists, and answered any other requests, the customer will receive a preliminary risk classification based on its assessed risk level, more in-depth described in Individual Customer Risk Scoring Methodology. Fasset divides its customers into the risk levels of low, medium, and high.

Fasset will not establish a relationship with a new customer and will cease all activity, including transactions, and terminate relationships with existing customers if it is unable to apply appropriate **Customer Due Diligence (CDD)** standards, regardless of transaction volume.

Additionally, Fasset will assess whether submitting a **Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR)** to the relevant authorities is necessary. In all cases, Fasset will document and record the rationale for its decisions, including the reasoning for not submitting a SAR/STR for any suspicious transactions that were escalated for review.

In the case of carrying out occasional transactions in favor of a client for amounts equal to or exceeding the thresholds mentioned in the applicable jurisdiction legislations, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked, the Fasset shall still apply appropriate CDD measures.

Fasset will also refrain from onboarding or maintaining business relationships with customers whose risk level is deemed unacceptable.

In addition to statutory requirements, and beyond customers classified as “unacceptable,” Fasset is explicitly prohibited from opening accounts for or establishing relationships with the following:

- Anonymous, fictitious, or numbered accounts

- Individuals or entities on international blacklists
- Sanctioned individuals (as designated by the United Nations (UN), European Union (EU), or the U.S. Office of Foreign Assets Control (OFAC))
- Accounts operating under a Power of Attorney (PoA) or any similar mandate or mechanism
- Legal entities controlled by beneficial owners who are residents of countries classified as prohibited under Fasset's internal risk controls
- Legal entities where it is not possible to verify the management structure and the nature of their activities
- Shell banks, shell organizations, or any entities offering services to shell banks
- Entities or individuals located in sanctioned countries
- Customers who fail to provide sufficient information and documentation for identity verification

2.3.2.2. Enhanced Due Diligence

In addition to standard Customer Due Diligence (CDD) applied to all customers, Fasset implements Enhanced Due Diligence (EDD) in cases where the risk level requires additional scrutiny. This includes obtaining approval from the Money Laundering Reporting Officer (MLRO), Head of Compliance, or an authorized delegate before establishing or continuing a business relationship with the customer.

Fasset has defined the following criteria for conducting EDD:

High-Risk Profile:

EDD is applied in the following scenarios:

- High-Risk Customers: Customers identified as posing a higher risk of money laundering (ML) or terrorist financing (TF) during the initial risk assessment. This determination may be based on factors such as citizenship, country of residence, or nationality.
- Risk Level Escalation: Customers whose risk level has been increased to High Risk during the course of the business relationship.
- Politically Exposed Persons (PEPs): Customers classified as PEPs due to their political status or close association with a politically exposed individual.

- Vulnerable Customers: Customers considered vulnerable due to age, disability, or other risk factors.

Potentially Suspicious Transactions:

EDD is triggered when customers engage in transactions that raise suspicion, including:

- High-velocity transactions (frequent transactions in a short period).
- Transactions without a clear or legitimate purpose.
- Transfers between high-risk jurisdictions or from high-risk to low-risk jurisdictions.
- Transactions involving shared withdrawal or deposit addresses.
- Rapid deposits or purchases followed by immediate withdrawals to external wallets.
- High-value, single transactions.

Potentially Suspicious Customer Behaviors:

EDD is also applied in cases where customers exhibit behaviors that indicate potential illicit activity, such as:

- Refusing to provide requested information.
- Inquiring about reporting thresholds (e.g., asking how much they can transact without triggering a report).
- Being linked via device, IP address, or email to multiple accounts.
- Transacting from sanctioned or crypto-banned countries.
- Conducting transactions from jurisdictions identified on international sanction lists as supporting terrorist activities.
- Having adverse media records (e.g., involvement in financial crimes, fraud, or regulatory violations).
- Customers with adverse media records.

Enhanced Due Diligence (EDD) is conducted to gain a deeper understanding of the background and financial situation of Fasset's high-risk customers. This process includes, but is not limited to:

- Verification of Source of Wealth (SoW) and Source of Funds (SoF):

- Source of Wealth (SoW): Refers to the origin of a customer's accumulated wealth or total net worth.
- Source of Funds (SoF): Refers to the specific origin of the initial and ongoing funds invested with Fasset.
- Purpose: Collecting and verifying SoW and SoF ensures Fasset can assess the legitimacy of funds, understand the customer's financial background, and establish a foundation for ongoing monitoring.

- Increased Frequency of Periodic Reviews:

  - Customers subject to EDD undergo more frequent periodic reviews after onboarding.
  - This ensures that their activities align with the stated purpose and nature of their business relationship with Fasset.

2.3.2.3. Ongoing Monitoring

Fasset undertakes ongoing Customer Due Diligence (CDD) and account monitoring to support the information gathered during customer onboarding and ensure continuous updates to customer information. Ongoing monitoring will occur on a periodic basis, using a risk-based approach, as well as in response to trigger events or through transaction monitoring throughout the lifecycle of the relationship. Additionally, if there are doubts regarding the accuracy or adequacy of previously obtained identification information, the CDD procedure will be re-applied.

Periodic Reviews are conducted based on the customer's risk assessment score. High-risk customers will be reviewed more frequently than those with lower risk scores, according to the following schedule:

- **High Risk Customers** – every **1 year**
- **Medium Risk Customers** – every **3 years**
- **Low Risk Customers** – every **5 years**

Periodic reviews include a comprehensive review of the customer's transactional activity, IP addresses, and Source of Wealth (SoW) / Source of Funds (SoF) description and/or

documentation. If discrepancies or red flags are identified, further investigation will be conducted to determine the appropriate course of action.

Trigger Events are changes in customer information that prompt a review of the customer relationship outside of the periodic reviews. These events include:

- Changes in personal details (e.g., telephone number, name, or any other relevant information)
- Significant transactions
- Material changes in how the customer's account is operated
- Substantial changes in this Policy or the standards for documenting CDD information, or when Fasset becomes aware that it lacks sufficient information about the customer

A trigger event review involves assessing the specific event that triggered the review and evaluating the overall customer account activity. If necessary, further escalation and reporting obligations may be required.

Transaction Monitoring ensures that the transactions are consistent with Fasset's knowledge of each customer and affiliated risk score of that customer. Fasset has an automated transaction monitoring system which features multiple alerts based on customer profile and transactional activity. The alert system highlights potentially suspicious activity and customers who may not be utilizing their accounts for the intended purpose. Alerts generated by this system will be reviewed on a daily basis by the Compliance Team to detect potentially suspicious activities. Fasset ensures that appropriate action is taken where necessary.

2.3.3. Transactions Monitoring Program and Blockchain Technology

Fasset is committed to developing a comprehensive, multilayered Transaction Monitoring Program (TMP) utilizing industry-leading third-party vendors and proprietary technologies. The TMP is designed to detect, assess, and mitigate financial crime risks through a risk-based approach, screening transactions for relevant red flags and typologies in alignment with regulatory and industry standards.

The Compliance Team is responsible for analyzing alerts generated by the TMP, including reviewing associated transactions to identify unusual or suspicious activity. Customers or transactions that exhibit heightened money laundering (ML) or terrorist financing (TF) risks will

be subject to Enhanced Due Diligence (EDD) and potential escalation to regulatory authorities, as required.

Regulatory Alignment and Risk-Based Scenarios

Fasset's TMP is designed to operate in full compliance with relevant local regulations and Financial Action Task Force (FATF) standards, including but not limited to:

- FATF Report: Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (September 2020)
- Other relevant FATF recommendations and local legislative frameworks

Fasset will deploy both proprietary monitoring tools and third-party technologies to ensure compliance, provided such technology has been pre-approved by the relevant regulatory bodies.

Technological Integration and Blockchain Analytics

Fasset's TMP leverages blockchain analytics and distributed ledger technology (DLT) tools, alongside investigative tools for transaction monitoring and risk assessment. Given the dynamic nature of virtual asset transactions, the utilization of on-chain and off-chain analytics will be subject to continuous internal reviews to assess:

- Effectiveness of transaction monitoring tools
- Functionality and ability to detect evolving risks
- Performance and coverage across different virtual assets and transaction types

Fasset will document the capabilities and limitations of these tools and implement compensating controls to mitigate identified weaknesses.

Holistic Transaction Monitoring Approach

Beyond blockchain-based analytics, Fasset has developed a set of non-blockchain transaction monitoring rules, focused on identifying high-risk behavioral patterns such as:

- Volume and velocity anomalies in transactional activity
- Outlier rules for deviations from expected customer behavior

- Flow-through rules for monitoring transactional movement, including:
    - Crypto-to-fiat transactions
    - Fiat-to-crypto transactions
    - Crypto-to-crypto funneling and layering techniques

Through this integrated, multilayered approach, Fasset ensures robust detection, mitigation, and reporting of financial crime risks while adhering to regulatory requirements and industry best practices.

2.3.4. Suspicious Activity Reporting

2.3.4.1. Definition of Suspicious Activity

Suspicious activity refers to any action or behavior that raises reasonable suspicion or knowledge that a customer may be involved in, or planning to engage in, financial crime. This includes, but is not limited to, money laundering, terrorist financing, proliferation financing (e.g., weapons of mass destruction), fraud, or other illicit activities.

2.3.4.2. Employee Responsibility & Reporting Obligations

All Fasset employees, regardless of location, seniority, or function, must immediately escalate any suspicion or knowledge of financial crime involving a customer or employee. Reports must be made urgently to the local Compliance Officer (CO), Money Laundering Reporting Officer (MLRO), or Head of Compliance.

Failure to report is a regulatory offense, potentially resulting in serious consequences for both the employee and Fasset.

2.3.4.3. Indicators of Suspicious or Unusual Activity

Fasset maintains a **non-exhaustive list of red flags**, continuously updated to reflect evolving financial crime risks. Common indicators include:

Transaction-Based Indicators

- **Large Transactions**: Transactions that exceed typical amounts, inconsistent with customer profile.

- **Structuring (Smurfing)**: Small transactions designed to evade reporting thresholds.
- **High-Velocity Transactions**: Rapid and repetitive transactions without economic justification.
- **"U-Turn" Transactions**: Deposits and withdrawals using the same wallet, signaling potential layering.
- **Transactions Lacking Economic Purpose**: Deposits and withdrawals without engaging in services or transfers that cannot be explained by the customer.
- **Use of Mixing or Tumbling Services**: Attempts to obscure fund origins via coin mixers or tumblers.
- **Use of Privacy Coins**: Transactions involving Monero, Zcash, or other privacy-enhanced cryptocurrencies.
- **Suspicious Peer-to-Peer (P2P) Transactions**: Direct transactions without intermediaries, which may facilitate money laundering.
- **Crypto-to-Fiat & Fiat-to-Crypto Funneling**: High-volume movements between fiat and crypto that lack a clear business rationale.

Customer Behavior & Profile Indicators

- **Unusual Client Behavior**: Customers reluctant or refusing to provide transaction details.
- **Forged or Altered Documents**: Submission of doctored or suspicious KYC documentation.
- **Reluctance to Answer Compliance Queries**: Evasion when questioned about transaction purposes.
- **Use of VPNs or Anonymous Browsing Tools**: Accessing Fasset through proxies, Tor, or anonymized DNS registrars.

Geographic & Jurisdiction-Based Indicators

- **Transactions Involving High-Risk Countries**: Transfers to or from jurisdictions on FATF's **"High-Risk and Other Monitored Jurisdictions"** list.
- **Transactions Involving Unregulated or Non-Compliant Exchanges**: Transfers from non-licensed exchanges, including decentralized exchanges (DEXs).
- **Darknet-Linked Transactions**: Payments associated with darknet markets or criminal forums.

- **Involvement of Sanctioned or Blacklisted Entities**: Transactions linked to OFAC/EU/UN-sanctioned individuals or entities.

Confidentiality & Prohibition of Tipping Off

Employees must not:

- Conduct independent investigations beyond their responsibilities.
- Disclose to customers or third parties that a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) has been filed.
- Discuss ongoing investigations outside of Compliance channels.

Tipping off is a criminal offense, which may **compromise investigations and lead to legal penalties**.

2.3.4.4. Escalation & Regulatory Reporting

Internal Escalation: Employees must immediately report any suspicion to the local CO, MLRO, or Head of Compliance.
Review & Assessment: The designated CO/MLRO will evaluate whether there are sufficient grounds to file an external SAR/STR.

Regulatory Filing: If warranted, the CO/MLRO will submit a SAR/STR to the Financial Intelligence Unit (FIU) in the respective jurisdiction without delay.

Post-Submission Compliance:

- The CO/MLRO must respond promptly to additional information requests from regulators.
- All internal and external reports will be documented and retained for audit and compliance review.

By maintaining robust monitoring, reporting, and compliance practices, Fasset ensures adherence to international AML/CFT standards and mitigates financial crime risks effectively.

2.3.4. Travel Rule

To comply with the Financial Action Task Force (FATF) Travel Rule, Fasset has implemented FATF-compliant software. The Travel Rule has been in place for over 20 years for traditional financial institutions like banks. It requires them to send originator and beneficiary information to the receiving bank when making payments.

In June 2019, FATF updated its guidelines to include Virtual Asset Service Providers (VASPs), such as Fasset, as entities that must comply with the Travel Rule.

However, compliance for VASPs, like Fasset, differs from banks due to challenges with Attribution and Data Transmission:

- **Attribution**: The sending VASP must reliably identify if the destination crypto-asset belongs to another VASP and know which VASP to send the originator/beneficiary information to.
- **Data Transmission**: The sending VASP must securely and reliably transmit the required information to the receiving VASP in real-time.

Banks have addressed this by using unique identifiers like BIC codes and IBANs, which allow them to confidently identify the receiving financial institution and exchange information using systems like SWIFT.

To ensure compliance, Fasset uses Travel Rule solutions that meet the requirements of operating jurisdictions, comply with data protection regulations, and are interoperable with other VASPs.

Fasset will:

1. Comply with the Travel Rule as soon as customer operations begin.
2. Only allow inter-VASP transactions where the counterparty VASP provides the Originator and Beneficiary information.
3. Before executing transactions that meet minimum thresholds in specific jurisdictions, Fasset will obtain the Originator and Beneficiary information before processing outbound transactions or allowing clients to access funds received in inbound transactions.

Required Originator and Beneficiary information shall include, but is not limited to:

Information on the Originator Customer	Name
	Residential / business address
	Account number/ VA wallet address
Accuracy requirement falls on Originator VASP	
Information on the Beneficiary Customer	Name
	Account number/ VA wallet address
Accuracy requirement falls on Beneficiary VASP	

For transactions involving self-custody/unhosted wallets, Fasset acknowledges, in line with FATF guidelines, that these wallets may present a higher risk. Local jurisdictions may require VASPs transacting with unhosted wallets to perform additional risk assessments. As a result, Fasset may apply high-risk scoring measures to these transactions and may collect owner information (such as name and address) during the withdrawal process.

If Fasset ever enables Anonymity-Enhanced Transactions as part of its activities, the company will implement proportionately enhanced controls to ensure compliance with all applicable laws and regulations, rules, and directives. These controls will include conducting enhanced Customer Due Diligence (CDD) on each client using these services, which will be verified every six [6] months.

2.4. Staff Awareness and Training

As part of Fasset's commitment to preventing financial crime, the company will implement a global compliance training program that is reviewed and updated annually. All employees, regardless of their department or job title (including senior management), are required to complete annual mandatory Anti-Money Laundering and Counter-Terrorist Financing (AML & CTF) training courses.

These training courses cover key topics, including:

- Main definitions related to AML & CTF.

- Legal frameworks under which Fasset operate.
- Fasset's internal systems and controls to minimize risks of money laundering, terrorist financing, bribery, corruption, and other financial crimes.

Training for New Hires: All new employees will complete training within three months of onboarding.

Annual Refresher Training: Existing employees will participate in refresher training courses annually.

Advanced Training for High-Risk Roles: Employees in roles that involve AML-related tasks or are exposed to heightened AML risks will receive more advanced training. This ensures they fully understand their responsibilities and are able to appropriately identify and address risks.

Training Delivery: AML training will be provided using a combination of methods, including:

- Workshops,
- On-the-job training,
- Live webinars, and
- E-learning modules.

Recordkeeping: Attendance records will be maintained to ensure that all relevant employees have completed the mandatory training.

2.5. Independent Testing and Audit

Fasset's compliance with the **AML/CTF Program** will be tested and audited independently at least once every 12 months. Fasset will use both internal audits and external audit firms to assess the effectiveness of its AML/CTF systems and controls in each jurisdiction where it operates.

After each audit, a written report will be provided to Senior Management and the Board. If any issues or weaknesses are found, a remediation plan will be put in place to address and correct them promptly.

3. Recordkeeping

Fasset is committed to maintaining accurate records for audit and compliance purposes throughout the entire duration of the business relationship, and even after the relationship ends. Given the nature of our business, most of these records are stored digitally or electronically.

To ensure the security and integrity of these records, Fasset will store them in a designated, secure folder on a protected server with restricted access to authorized employees only. Access to this folder will be tracked via an audit trail.

Fasset will retain customer data ("Data") for as long as necessary to fulfill the purposes outlined in our Privacy Policy, including compliance with local laws . This retention will continue unless local laws mandate a longer retention period. Specifically, Fasset will keep Data for as long as it is needed to establish, exercise, or defend legal rights. For AML-CTF-related data, this includes, but is not limited to:

- Transaction Records: Virtual Asset transaction details, including operational and statistical records, documents, and information (whether publicly recorded on ledgers or not) regarding all transactions processed by Fasset.
- Customer Due Diligence (CDD) Records: Documents and information about clients (e.g., account files, business correspondence), as well as results from investigations and analyses of client activities.
- Third-Party Information: Information related to third parties hired to conduct CDD.
- Ongoing Monitoring Records: Records of ongoing monitoring of business relationships with clients.
- Suspicious Transaction Reports: Documents related to suspected illicit activities.

These records will be kept for no less than eight (8) years. In jurisdictions with longer retention requirements, Fasset will comply with local laws and regulations.

In line with Data Protection and Privacy Laws, Fasset will only use customer information for the purpose and nature of the business relationship. All employees are strictly prohibited from omitting, deleting, destroying, altering, or falsifying information and/or records for any reason—this includes trying to evade Fasset’s policies or conceal information from other financial institutions, banks, or regulators.

4. Cooperation with Regulatory Authorities

Fasset ensures full cooperation with regulatory authorities across Bahrain. We store all records, documents, and data for both local and international transactions in a readily accessible and retrievable format and provide this information to law enforcement and regulatory bodies, such as CBB, MOI.

Fasset receives Law Enforcement (LE) requests and Requests for Information (RFI) through the official Compliance mailbox. All such requests are documented and reviewed in accordance with the Service Level Agreements (SLA) specific to each jurisdiction. The regional Compliance Officer is responsible for managing LE and RFI requests, ensuring that responses are timely and compliant with relevant laws and company policies. Unauthorized access, disclosure, or handling of such requests is strictly prohibited.