Market Abuses Prevention and Detection Policy

1. Introduction

1.1. Definitions

Under MiCAR, the prevention and prohibition of market abuse applies to :

- “Acts carried out by any person concerning crypto-assets that are admitted to trading or in respect of which a request for admission to trading has been made;
- Any transaction, order or behavior concerning crypto-assets;
- In the European Union and in third countries.”

There are three types of market abuses defined as :

- Insider dealing;
- Market manipulation;
- Unlawful disclosure of inside information.

1.1.1. Insider dealing

Insider dealing refers to the act of using inside information to acquire, dispose of, or amend orders concerning related crypto-assets, directly or indirectly, for themselves or others. It also includes canceling or amending orders placed before obtaining inside information and recommending or inducing others to engage in such trading actions.

The prevention and prohibition of insider dealing applies to any person who possesses inside information as a result of:

- Being a member of the administrative, management or supervisory bodies of the issuer, the offeror, or the person seeking admission to trading;
- Having a holding in the capital of the issuer, the offeror, or the person seeking admission to trading;
- Having access to the information through the exercise of an employment, profession or duties or in relation to its role in the distributed ledger technology or similar technology; or
- Being involved in criminal activities.

1.1.2. Market manipulation

The following behavior shall, inter alia, be considered market manipulation :

- Securing a dominant position over the supply of, or demand for, a crypto-asset, which has, or is likely to have, the effect of fixing, directly or indirectly, purchase or sale prices or creates, or is likely to create, other unfair trading conditions ;

- The placing of orders to a trading platform for crypto-assets or with exchange service, including any cancellation or modification thereof, by any available means of trading, and which has one of the effects referred to in paragraph 2, point (a), by:

    - Disrupting or delaying the functioning of the trading platform for crypto-assets or engaging in any activities that are likely to have that effect;

    - Making it more difficult for other persons to identify genuine orders for crypto-assets or engaging into any activities that are likely to have that effect, including by entering orders which result in the destabilisation of the normal functioning of the platform for crypto-assets;

    - Creating a false or misleading signal about the supply of, or demand for, or price of, a crypto-asset, in particular by entering orders to initiate or exacerbate a trend, or engaging into any activities that are likely to have that effect;

    - Taking advantage of occasional or regular access to the traditional or electronic media by voicing an opinion about a crypto-asset, while having previously taken positions on that crypto-asset, and profiting subsequently from the impact of the opinions voiced on the price of that crypto-asset, without having simultaneously disclosed that conflict of interest to the public in a proper and effective way.

1.1.3. Unlawful disclosure of inside information

Unlawful disclosure of inside information arises when a person possesses inside information and discloses it to another person.

In order to prohibit the unlawful disclosure of inside information:

- No person in possession of inside information shall unlawfully disclose inside information to any other person, except where such disclosure is made in the normal exercise of an employment, a profession or duties;

- The onward disclosure of recommendations or inducements of an inside information about crypto-assets amounts to unlawful disclosure of inside information where the person disclosing the recommendation or inducement knows or ought to know that it was based on inside information.

1.2. Scope of the policy

In the course of its activities, Paymium may be confronted with situations that could potentially generate market abuse. This Policy is intended to present the legal framework that Paymium puts in place to prevent, control and manage market abuse.

This policy aims to ensure that Paymium prevent all forms of market abuses, such as insider dealing, the unlawful disclosure of inside information or market manipulation.

2. Monitoring and detection

2.1. Monitoring

The Company conducts compliance monitoring on a risk-based approach to ensure effective oversight of its activities. Monitoring for market abuse focuses on the potential receipt of inside information throughout the investment process, with measures in place to manage and mitigate this risk.

As part of its daily checks, the Compliance department reviews the trading activity in real time to identify any suspicious transactions.

It is important to recognize that sufficient indications of market abuse may only become evident after an order has been placed or a transaction has occurred. Monitoring staff must remain alert to the possibility that a sequence of events over several days might indicate potential market abuse, necessitating further investigation to determine whether a suspicious transaction order report (hereinafter referred to as a "**STOR**") should be filed.

2.2. ICT system

The Company employs ICT (Information and Communication Technology) systems and has put in place procedures which assist the detection of market abuse or attempted market abuse. These ICT systems are appropriate and proportionate in relation to its scale, size and the nature of its business activities.

The Company has designed its own ICT system to monitor transactions and orders as well as its trading engine.

The Company ensures full compliance with the General Data Protection Regulation (GDPR). This includes:

- Standards, including data minimization, security measures, and storage limitations;
- Safeguards for personal data handling;
- Protection of data subjects' rights and the security of personal data.

The tool and its settings meet the requirements of the Information System Security Policy of the Company, in compliance with MiCA and DORA regulations.

3. Prevention

The Company has implemented a comprehensive set of measures aimed at preventing any situations involving market abuses.

These measures are designed to ensure compliance with applicable regulations and promote transparency in all operations.

3.1. Safeguarding inside information

Employees of the Company shall assume that all information obtained during the course of their employment with the Company is not public, unless the information has been publicly disclosed.

The following are examples of some identified scenarios where employees of the Company may be at a high-risk of receiving inside information:

- Shared office building;
- Contact with public companies;
- Personal relationships.

To ensure the confidentiality of inside information, the following rules are implemented in the Company:

- Any communication involving inside information must be handled with extreme caution. Employees who come into possession of potential inside information must not share it with anyone, either internally or externally, except with the Compliance department. Discussions about inside information must be avoided in public areas such as hallways, elevators, or social events, and special care must be taken when using telephones in places where conversations could be overheard;

- Non-public information related to the Company's investment strategies and holdings must not be shared with third parties, except as necessary to execute investment decisions, conduct legitimate business, or comply with regulatory obligations. Employees are prohibited from disclosing details about proposed or pending deals or other sensitive matters to third parties without prior approval from the Compliance department;

- Exposed persons must exercise additional vigilance when working in open office environments. Discussions of inside information should only take place in private areas such as conference rooms;

- Documents containing inside information must be handled with the highest level of discretion and securely stored. This includes:

    - Avoiding leaving sensitive documents in plain sight;
    - Storing documents in closed cabinets or files;
    - Locking storage areas, especially outside business hours;
    - Limiting access to those authorized to view the information; and
    - Properly destroying duplicate or unneeded documents.

The leaking of any inside information by an employee may lead to disciplinary sanctions.

3.2. Information barriers

The Company prevents and controls the exchange of information between relevant individuals engaged in activities involving a risk of market abuses.

The Company restricts access to privileged information on a need-to-know basis, allowing only individuals whose roles specifically require such information to perform their job functions.

The Company implements IT systems access restrictions to manage access to privileged information such as:

- User permissions management: regular reviews and updates of user permissions ensure that access levels are current and appropriate for each user's role;

- Physical security controls: access to IT infrastructure and systems that store or process privileged information is restricted through physical security measures like locked server rooms and restricted areas;

- Password protection: access to privileged information is secured by requiring unique, strong passwords that are assigned only to authorized users;

- Encryption of information: the company may encrypt messages containing privileged information.

3.3. Media and disclosure

The Company follows a strict communication and commercial policy.

The Company maintains vigilant oversight to prevent the dissemination of misleading signals or unauthorized information that could impact the integrity of the market or its operations.

The media activities and interactions of exposed members of the Company, as well as the Company itself, are closely monitored.

In case of a detected leak or suspicious activity, immediate measures are implemented to control the situation and prevent further dissemination, including internal investigations and, if necessary, coordination with regulatory authorities.

4. Reporting

The dedicated team, which is composed of the Managing Director, the Money Laundering Compliance Officer and the Chief Technical Officer are in charge of the reporting obligations.

4.1. Internal reporting process

The Company establishes and maintains effective procedures that enable them to assess, for the purpose of submitting a STOR, whether there are circumstances indicating that market abuse has been committed, is being committed or is likely to be committed.

The Company has implemented an internal reporting process which is organized with 3 steps:

- Identification/ suspicion of a potential market abuse case;
- Initial assessment;
- Escalation.

The entire reporting process must be completed within five business days to determine whether a STOR will be transmitted to the AMF.

4.2. Confidentiality

The Company ensures and upholds the confidentiality of information at all times.

Specifically, procedures are in place to prevent disclosure to the person concerned by the STOR or to any individual not authorized to be informed due to their role within the Company. This includes safeguarding information related to:

- The generation of alerts or the assessments leading to a STOR submission, ensuring that the dedicated team completes the STOR without requesting information from the person involved to fill specific fields;
- The submission of a STOR or any intention to submit it to the competent authority.

Personal data under this policy and its implementing procedures are processed in accordance with the Data Protection Regulation.

4.3. Transmission of a STOR to the AMF

The Company has implemented a reporting process that ensures the prompt submission of a STOR

as soon as reasonable suspicion of market abuse is identified.

When a delay occurs, the dedicated team must include a detailed explanation within the STOR, addressing the reasons for the delay and outlining the specific circumstances that led to the late submission, as required by the AMF.

The Company shall submit, without delay, a STOR, along with any supporting documents or attachments, to the Market Surveillance Division of the AMF.

4.4. Record keeping of a STOR and market observations

The Company shall maintain the information documenting the analysis carried out with regard to orders, transactions and aspects of the functioning of distributed ledger technology that could constitute market abuse for a period of ten years. That information shall include the analysis made and the reasons for submitting or not submitting a STOR.

That information shall be provided to the AMF upon request.

People who have access to data storage are the Managing Director, the Money Laundering Compliance Officer and the Chief Technical Officer.

*
* *