REAL MONEY EUROPE

Metals Bank

WHISTLEBLOWING PROCEDURE

Reporting Violations System

pursuant to the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022, and Directive (EU) 2019/1937

1. What Whistleblowing Is and Why It Matters

Whistleblowing is the reporting, by a person — worker, collaborator, client or other party — of unlawful, irregular or non-compliant conduct of which they have become aware in the context of a work-related activity or a professional or business relationship.

Real Money Europe LIMITED (hereinafter “Real Money Europe” or "the Company"), as a Metals Bank, has adopted this Whistleblowing System in the belief that the timely reporting of any violations is a fundamental tool for:

- Preventing unlawful or non-compliant conduct before it causes harm;
- Protecting clients, workers and the integrity of the precious metals trading business;
- Promoting a corporate culture based on legality, fairness and transparency;
- Fulfilling the obligations set out in the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022, and in Directive (EU) 2019/1937, as well as adopting international best practices in governance.

> *The Whistleblowing System of the company is adopted in accordance with the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022, and with Directive (EU) 2019/1937 and constitutes, for a Metals Bank for Real Money Europe LIMITED, as a Metals Bank, a voluntary choice of best practice in governance, legality and transparency, consistent with the highest standards of the precious metals sector and with the AML/CFT obligations set out in applicable legislation.*

The System adopted by the Company is based on tools that guarantee the utmost confidentiality of the reporting person's identity, the protection of personal data, and an absolute prohibition on retaliation of any kind against anyone making a report in good faith.

1.2 Objectives of the Whistleblowing System

The Whistleblowing System of the company pursues the following fundamental objectives:

- Prevention: promptly identifying non-compliant conduct or conduct potentially harmful to corporate integrity;
- Protection: safeguarding reporting persons from any form of retaliation or discrimination;
- Transparency: ensuring a clear, well-defined process accessible to eligible parties;
- Continuous improvement: using reports as a tool to strengthen compliance safeguards;
- Regulatory compliance: ensuring compliance with applicable legislation.

1.3 Scope of Application

This document governs the Company's whistleblowing system and, in particular:

- a) defines the system for managing reports pursuant to applicable legislation;
- b) establishes the organisational roles and responsibilities for managing reports;

- c) governs staff training and awareness-raising activities;
- d) implements a whistleblowing system compliant with Directive (EU) 2019/1937 and with the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022;
- e) ensures the protection of reporting persons and the proper management of reports of regulatory violations.

1.4 Guiding Principles

The Whistleblowing System of Real Money Europe is based on the following principles:

- confidentiality of the reporting person's identity;
- prohibition of retaliation of any kind;
- access to the system through a single internal channel (the MITWhistle platform);
- timeliness in the handling of and response to reports;
- proportionality of actions relative to the severity of the violations;
- traceability of reports and of handling activities.

1.5 Definitions

Pursuant to the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022, the following terms shall mean:

Term	Definition
Reporting Person	The natural person who makes the report or the public disclosure of information on violations acquired in the context of their work-related activities.
Internal Report	Written or oral communication of information on violations, made through the internal reporting channel established by the Company pursuant to applicable legislation.
External Report	Communication of information on violations made through the external channels provided for by the Protected Disclosures Act 2014, including, where applicable, the designated bodies (*prescribed persons*) and the Protected Disclosures Commissioner.
Protected Disclosure	A report of information which, in the reasonable belief of the reporting person, tends to show a relevant wrongdoing and which was acquired in a work-related context, made in the manner provided for by the Protected Disclosures Act 2014, as amended.
Public Disclosure	Making information on violations publicly available through the press, electronic media or other means of communication capable of reaching a large number of people, in the cases and under the conditions provided for by applicable legislation.
Violations	Acts or omissions, committed or that could be committed, that fall within the notion of relevant wrongdoing under the Protected Disclosures Act 2014, as amended, including, in particular, the commission of offences, failure to comply with legal obligations, miscarriages of justice, dangers to health or safety, damage to the environment, certain breaches of European Union law, and the concealment or destruction of information relating to such violations.
Information on Violations	Information, including reasonable suspicions, concerning violations committed or that could be committed within the organisation with which the reporting person interacts in the context of their work-related activities.
Work-Related Context	Current or past work-related or professional activities, carried out in connection with employment relationships with the Company, through which persons acquire information on violations.
Person Concerned	The natural or legal person named in the report as the person to whom the violation is attributed or who is otherwise implicated in the reported violation.
Facilitator	The natural person who assists the reporting person in the reporting process, operating within the same work-related context, whose assistance must be kept

	confidential.
Retaliation	Any act or omission, including an attempted or threatened act or omission, which occurs because of a report and which causes or may cause unjustified harm to the reporting person.
Protective Measures	Measures aimed at protecting the reporting person, the facilitator and persons connected to the reporting person from retaliation.
Report Manager	The party designated by the Company, endowed with autonomy and independence, responsible for managing the internal reporting channel, identified as the Company's Compliance Officer.
Anonymous Report	A report made without disclosing the identity of the reporting person; anonymous reports are handled in accordance with applicable legislation.
Designated Person	The party identified under Irish legislation as the competent recipient for certain categories of external reports.

2. Regulatory References

This Procedure is adopted in accordance with the European and national regulatory framework on whistleblowing, compliance, personal data protection and the prevention of corporate risks. In particular, the company's reporting system is governed by the following main regulatory sources:

- Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022 — Irish legislation on protected disclosures and the transposition of Directive (EU) 2019/1937;
- Directive (EU) 2019/1937 — protection of persons who report breaches of European Union law;
- Regulation (EU) 2016/679 (GDPR) and applicable Irish legislation on the protection of personal data;
- Data Protection Act 2018 — Irish legislation on the protection of personal data;
- Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended — Irish legislation on the prevention of money laundering and terrorist financing;
- Any further provisions and measures of the competent Irish authorities applicable to the Company in relation to governance, compliance and AML/CFT.

3. Who May Make a Report

The Whistleblowing System of Real Money Europe is accessible to all persons who, in the context of a work-related or professional activity, become aware of violations under applicable legislation. Reports may be made by both internal and external persons, within the limits and under the conditions provided for by applicable legislation.

3.1 Internal Reporting Persons — Workers and Collaborators

All persons who work or have worked for the Company in any capacity are entitled to make reports:

- Employees on permanent and fixed-term contracts;
- Collaborators, consultants and self-employed professionals;
- Interns and trainees;
- Agency workers;
- Directors and members of the corporate bodies;
- Agents and representatives of the commercial network;
- Former employees or collaborators, in respect of matters of which they became aware during the relationship;
- Candidates during the recruitment process, in respect of matters learned during the hiring process.

3.2 External Reporting Persons — Third Parties

External parties who have or have had professional or business relationships with the Company are also entitled to make reports, including:

• Suppliers, business partners and third parties who work or have worked on behalf of the Company;

• Other persons who, in the context of professional or business relationships, have become aware of relevant violations.

The protections provided for by the Protected Disclosures Act 2014, as amended, apply to persons falling within the personal scope provided for by that legislation.

3.3 Conditions for the Protection of the Reporting Person

The protections provided for in this Procedure apply to reporting persons who make reports pursuant to the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022, provided that, at the time of the report, they have reasonable grounds to believe that the information communicated is true and falls within the scope of relevant violations under applicable legislation. In particular, the report must be made:

- on the basis of information learned in a work-related and professional context;
- with a reasonable belief as to the truthfulness of the facts reported;
- without abuse of the reporting tool.

Reports containing information which the reporting person knows to be false are excluded from the protections. Such conduct may give rise to disciplinary liability for workers, as well as civil or criminal liability under applicable Irish legislation.

4. What May Be Reported

Reports may concern violations, or reasonable grounds to suspect violations, provided for by applicable legislation, including, by way of example and not exhaustively, the following categories of rules and internal procedures applicable to the Company:

4.1 Violations of Anti-Money Laundering Legislation (AML/CFT)

Under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended:

- Failure to identify clients or breaches of customer due diligence obligations;
- Failure to report suspicious transactions to FIU Ireland and the Revenue Commissioners, as required under applicable Irish legislation;
- Breaches of Real Money Europe's internal KYC procedures;
- Deficiencies in the safeguards against money laundering and terrorist financing.

Reports of suspicious transactions (STRs) must be made through the dedicated AML channels and not through the whistleblowing system.

4.2 Violations of the Legislation Applicable to the Metals Bank

Under applicable Irish legislation:

• Irregularities in the purchase or sale of investment gold or precious metals;

• Deficiencies in the traceability and recording of precious metals transactions;

• Breaches of reporting obligations to the competent Irish authorities;

• Improper conduct towards clients in the purchase or sale of investment gold.

4.3 Violations in Relation to Governance and Internal Controls

Under applicable Irish legislation and internal procedures:

• Deficiencies in corporate governance, internal controls or the management of conflicts of interest;
• Conduct that does not comply with the Company's Code of Ethics and integrity principles;
• Conduct relevant under applicable legislation on the Company's liability;
• Breaches of IT security policies and corporate data protection safeguards.

4.4 Violations Relating to the Protection of Personal Data

Under Regulation (EU) 2016/679 (GDPR) and applicable Irish legislation:

- Processing of personal data carried out without a valid legal basis or in breach of GDPR principles;
- Failure to adopt adequate security measures, including unauthorised access or data loss;
- Failure to manage obligations relating to personal data breaches, including failure to notify the Irish Data Protection Commission;
- Breaches of data subjects' rights.

4.5 What CANNOT Be Reported Through This Channel

The following do not fall within the scope of this whistleblowing system:

- Personal complaints relating to employment or business relationships, to be handled through ordinary channels;
- Differences of opinion on management or strategic decisions;
- Reports known by the reporting person to be false;
- Reports of suspected money laundering transactions, to be sent through the dedicated AML channel;
- Complaints relating to products or services, to be handled through the Company's complaints procedure.

The reporting system does not replace ordinary assistance or complaints channels.

5. How to Make a Report — The Three Channels

Real Money Europe provides reporting persons with a reporting system compliant with applicable legislation, designed to ensure confidentiality, security and protection for the reporting person. Reports may also be made anonymously. However, providing personal contact details may facilitate any requests for clarification or updates.

The Company issues an acknowledgement of receipt of the report within 7 days, pursuant to the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022. Irish legislation also requires diligent follow-up of the report and, generally, feedback within 3 months.

5.1 Official Internal Channel — MITWhistle Platform

The official internal channel for submitting reports is the dedicated digital platform:

(INSERT MITWHISTLE LINK — to be completed)

The platform allows for:

- written and anonymous reports;
- confidential communication with the report manager;
- data protection through encrypted systems;
- separation between the reporting person's identity and the content of the report.

The system is provided by a specialised external provider. The processing of personal data is carried out in accordance with applicable legislation, and privacy roles are defined in compliance with the GDPR.

5.2 Residual Alternative Channel

As an alternative to the platform, the reporting person may request a direct, confidential meeting with the Compliance Officer or send a confidential written communication.

These channels also guarantee the confidentiality of the reporting person and are managed in accordance with the same protections provided for by applicable legislation.

5.3 External Channel

Where the conditions provided for by applicable legislation are met, the reporting person may make a report through the external channels provided for by the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022, by addressing the competent designated person (prescribed person) for the relevant matter or the Protected Disclosures Commissioner.

Recourse to the external channel is permitted, in particular, when:

• the reporting person reasonably believes that the violation falls within the competence of the designated person to whom the report is made;

• the reporting person reasonably believes that the information communicated, and any allegations contained therein, are substantially true;

• the report may be submitted to the Protected Disclosures Commissioner, who will, where possible, forward it to the competent party for follow-up.

5.4 Public Disclosure

In the cases provided for by the Protected Disclosures Act 2014, as amended, the reporting person may make information relating to a violation public, for example through the press or other media.

Public disclosure benefits from the protections provided for by law where the reporting person has reasonable grounds to believe that the information communicated, and any allegations contained therein, are substantially true, and at least one of the following conditions is met:

• the reporting person has already made an internal or external report substantially concerning the same information and no appropriate action has been taken within the timeframes provided for by law;

• the reporting person has reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest, for example in the presence of an emergency situation or a risk of irreversible harm;

• the reporting person has reasonable grounds to believe that, by making an external report, they may be exposed to retaliation;

• the reporting person has reasonable grounds to believe that there is little likelihood of the violation being effectively addressed, taking into account the specific circumstances of the case, for example where there is a risk that evidence may be concealed or destroyed, or that the competent authority may be involved in the violation or in collusion with the perpetrator.

6. Content of the Report

To enable the effective handling of a report, it is helpful — though not mandatory — to provide the following information:

- a description of the facts reported (what happened, in what context and with what frequency, if applicable);
- the dates or period in which the facts occurred;
- the place where the facts occurred;
- the persons involved, if known;
- any supporting documentation (emails, contracts, screenshots, other);
- how the facts came to the reporting person's attention.

The reporting person need not be absolutely certain that the violation has occurred: it is sufficient to have reasonable grounds to believe that the information reported tends to demonstrate a relevant violation. The protections provided for by law apply where the conditions set out in the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022, are met, regardless of the final outcome of the verification of the reported violation.

7. Protective Measures for the Reporting Person

The Company guarantees the utmost protection to reporting persons, in accordance with the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022, and with Directive (EU) 2019/1937.

7.1 Confidentiality of Identity

The identity of the reporting person is treated with the utmost confidentiality. It is known only to persons authorised to manage the report and is not disclosed to third parties without the explicit consent of the reporting person, except in the cases provided for by applicable legislation.

All reports and documents relating to the report are prepared so as not to contain references that could allow the reporting person to be identified.

The identity of the reporting person, or information from which it may be directly or indirectly inferred, may be disclosed only in the following cases:

- where disclosure constitutes a necessary and proportionate obligation under law in the context of investigations or judicial proceedings, including to safeguard the defence rights of the person concerned;
- where the party managing the report demonstrates that all reasonable measures have been taken to avoid disclosing the identity of the reporting person;
- where there are reasonable grounds to believe that disclosure of the identity is necessary to prevent a serious risk to State security, public health, public safety or the environment;
- where disclosure of the identity is otherwise required by law.

Where the identity of the reporting person must be disclosed without their consent, the reporting person shall be informed in writing and in advance, with an explanation of the reasons for the disclosure, unless such information would jeopardise:

- the effective conduct of the investigation into the reported violation;
- the prevention of a serious risk to State security, public health, public safety or the environment;
- the prevention of an offence or the prosecution of a criminal act.

7.2 Absolute Prohibition on Retaliation

The Company prohibits any form of retaliation, discrimination or detrimental conduct against the reporting person, their colleagues or family members, as a consequence of the report. The following are considered, by way of example, to constitute retaliation:

- dismissal, suspension or non-renewal of contract;
- demotion, transfer or unfavourable changes to working conditions;
- reduction in pay or benefits;
- negative performance evaluations not justified by objective criteria;
- failure to promote or advance;
- acts of bullying, isolation or undue pressure;
- termination or worsening of the business relationship (for external parties).

Irish legislation expressly prohibits the employer from taking, or threatening to take, any detrimental measure against a worker for having made a protected disclosure.

A reporting person who believes they have suffered retaliation may use the internal channel through the dedicated platform or, in the cases provided for by law, address the competent external channels, including the Protected Disclosures Commissioner, and avail of the remedies provided for under applicable Irish legislation.

7.3 Extended Protection

The protections provided for in this Procedure also extend to:

- facilitators: persons who assist the reporting person in the reporting process (lawyer, trade union representative);
- colleagues and family members of the reporting person who may suffer retaliation on account of their connection with the report;
- entities or legal persons owned by the reporting person, at which the reporting person works, or with which they are otherwise connected in a work-related context.

7.4 Processing of the Reporting Person's Personal Data

The personal data of the reporting person is processed in accordance with Regulation (EU) 2016/679 (GDPR) and the Irish Data Protection Act 2018. Processing is carried out solely for purposes connected with the handling of the report and in accordance with the legal bases provided for by applicable legislation.

Data and documentation relating to reports are retained for the period necessary and proportionate for the purposes of handling the report and fulfilling the obligations provided for by applicable legislation. Irish law requires the keeping of a record of reports, including anonymous ones.

For further information, please refer to the privacy notice available on the company website.

8. How We Handle Reports

The Company adopts a structured process for handling reports, organised into six stages, with timeframes defined in accordance with the deadlines provided for by the Protected Disclosures Act 2014, as amended by the Protected Disclosures (Amendment) Act 2022:

Stage	Timeframe	Activity	Responsible Party
1. Receipt	Day 0	Receipt via the MITWhistle platform, automatic logging and recording in the confidential register, with segregation of the reporting person's identifying information	Compliance Officer / MITWhistle System
2. Acknowledgement	Within 7 days	Sending an acknowledgement of receipt to the reporting person via the platform, with a case reference number and an indication of the timeframes	Compliance Officer
3. Assessment	Within 30 days	Analysis of admissibility, assessment of severity and urgency, any request for further information from the reporting person	Compliance Officer
4. Investigation	Within 90 days	Gathering of documentation, interviews with persons involved, technical checks, regulatory analysis. External consultants may be involved where necessary, subject to confidentiality	Compliance Officer + any consultants
5. Decision	Within 90 days	Presentation of the report to the Board of Directors, resolution on corrective and/or disciplinary action	Board of Directors, upon proposal of the Compliance Officer
6. Feedback	Within 90 days	Communication of the outcome to the reporting person (within the limits of confidentiality), initiation of the corrective action resolved upon	Compliance Officer

All stages of the process are conducted with the utmost confidentiality by the report manager. The confidentiality obligation regarding the reporting person's identity extends to all persons involved. The Reports Register is kept in a confidential and segregated form, accessible only to the Compliance Officer and to any other persons expressly authorised by the Company, where necessary.

9. Management of Conflicts of Interest

The Company has put in place specific measures to ensure the independent handling of reports in cases where conflicts of interest may arise.

9.1 Reports Concerning the Compliance Officer

Where a report concerns the Compliance Officer, it is handled through the MITWhistle platform and assigned directly to the Board of Directors, who shall assume responsibility for the investigation. The Compliance Officer is excluded from any access to, or involvement in, the report.

9.2 Reports Concerning One or More Directors

Where a report concerns one or more Directors of the Company, its handling is entrusted to the Company Secretary, provided they are not involved in the matters that are the subject of the report and there is no conflict of interest. Otherwise, the report is entrusted to an independent external party specifically appointed by the Company.

10. Relations with the Competent Authorities

The Company fully cooperates with the following competent authorities:

Protected Disclosures Commissioner	Receipt and handling of external reports in the cases provided for by law, and referral, where necessary, to the competent party
Persons Designated by Law	Receipt of external reports in matters within their respective competence
Data Protection Commission	Matters relating to the processing and protection of personal data
Irish Judicial and Police Authorities	Reports concerning possible offences, in accordance with applicable legislation

Real Money guarantees that use of the internal channel does not in any way prejudice the reporting person's right to have recourse to the external channels provided for by the Protected Disclosures Act 2014, as amended, in the cases and under the conditions provided for by applicable legislation.

11. Training and Communication

Real Money Europe undertakes to ensure that all persons to whom this Procedure is addressed are adequately informed and trained on the Whistleblowing System:

- mandatory training for all staff upon hiring and with annual refresher training;
- communication of this Procedure to all collaborators and agents of the corporate network;
- publication of the Procedure on the company website in the dedicated section;
- provision of the reporting channel.

12. Updates to the Procedure

This Procedure is subject to annual review by the Compliance Officer and the Board of Directors, or upon the occurrence of significant regulatory changes. Any amendment is approved by the Board of Directors and promptly communicated to all staff. The updated version is always available on the company website in the section dedicated to Whistleblowing.