

Confronting Cases of Fraud, Forgery & Deception Policy

UEXO GLOBAL MARKETS LLC

Business Activity:

**Securities & Financial Products Promotion
Introduction to Financial Services**

Confronting cases of Fraud, Forgery and Deception Policy

Confronting Cases of Fraud, Forgery & Deception Policy

Log of preparation, version of Policy & approval date.

Sr. No	Document Version	Document Release Date	Prepared By	Approved By
1	General Update v.1	Dec.2025	Compliance Manager Shan Muhammed Hussian Category Manager Louis DeTata	Louis Detata Owner & CEO Signature

Company Stamp



LOUIS GUY DETATA

Table of Contents

1- INTRODUCTION 4

2- Defining Fraud, Forgery, and deception..... 5

3- Managing the Risk of Fraud – Responsibilities 6

4- Fraud Response 7

5- Anti-Bribery & Corruption – Acceptable and Not Acceptable 8

6- Employee Responsibility in relation to Anti Bribery and Corruption 10

7- Training and Communication..... 10

8- Record Keeping 10

9- Monitoring and Review 10

Appendix 1..... 11

1- INTRODUCTION

We at **UEXO GLOBAL MARKETS L.L.C** with commercial license Number **1569040** issued by Dubai Economy & Tourism are confirming that we are seeking approval from the SCA to approve our Category 5 SCA application with reference number LIC-0011290 as arranging and advising with activities Promotion & Introduction that we are involved in with the SCA.

- Preamble

Introduction to Fraud Prevention, Anti-Forgery and Deception Policy.

here in after as (“UEXO” OR “Firm”) has a commitment to high legal, ethical, and moral standards & all employees of the Firm are expected to share this commitment.

Fraud is an issue that all organizations may face regardless of size, industry, or country. The Firm takes a zero-tolerance attitude to fraud and will uphold all applicable laws relevant to countering fraud in all jurisdictions in which it operates.

The Board of Directors of the Firm (“Board”) carries out overall responsibility to ensure that risk culture is established based on risk manual and policies and executive management must work very hard to make sure that all these rules were implemented and in action, and fraud awareness is continuously raised Firm-wide. Fraud is an ever- present threat and hence must be a concern to all employees. The Firm views fraud as an extremely serious matter and is committed to continuous promotion of anti- fraud culture throughout the Firm. The purpose of this Anti-Fraud Policy is to provide an overall framework for a response, advice and direction to those who find themselves having to deal with suspected cases of fraud.

The Policy applies to any suspected or accomplished irregularity, involving employees as well as consultants, vendors, contractors, and/or any other external parties having a business relationship with the Firm. Any investigative activity required will be conducted without regard to any person’s relationship to the Firm, position, or length of service. All employees have a duty to familiarize themselves with the types of improprieties that might be expected to occur within their areas of responsibility and to be alert to any indications (“red flags”) of fraud risk.

The anti-Fraud, forgery & deception policy exists to set out the responsibilities of UEXO Finds those who work for the Firm in regard to observing and upholding our zero-tolerance position on bribery and corruption.

The Firm is committed to conducting business in an ethical and honest manner and is committed to implementing and enforcing systems that ensure bribery is prevented and totally not allowed. The Firm has zero- tolerance for bribery and corrupt activities. UEXO is committed to acting professionally, fairly, and with integrity in all business dealings and relationships, wherever in the country of operation and has actual physical branch.

“UEXO” will constantly uphold all laws relating to anti-bribery and corruption in all the jurisdictions in which UEXO operate. The Firm is bound by the applicable UAE laws, SCA regulations and acts amounting to bribery under the Organization for Economic Co- operation and Development (“OECD”) Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. Additionally, the Firm strictly abides by all the applicable UAE Federal Regulations in regard to Anti-Fraud and Forgery along with deception.

Confronting Cases of Fraud, Forgery & Deception Policy

The Firm recognizes that Fraud, Forgery, and deception are punishable by law which may or may not include imprisonment and fines. If the Firm is discovered to have taken part in corrupt activities, it may be subjected to an unlimited fine, be excluded from tendering for public contracts, and face serious damage to the Firm's reputation, along with other criminal crimes as per local rules.

2- Defining Fraud, Forgery, and deception.

Fraud is generally defined as "any illegal act characterized by deceit, concealment, or violation of trust". These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by persons to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage." The term "fraud" commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, deception, bribery, abuse of authority, insider dealing and extortion. It may involve:

- Manipulation, falsification or adjustments of records or documents;
- Suppression or omission of the effects of transactions from records or documents;
- Recording of transactions without substance.
- Asset misappropriation or willful destruction, including theft of cash or other assets (suppliers, inventory, equipment, and information);
- Undisclosed personal economic interest (conflict of interest) in a transaction that adversely affects the organization or its shareholders;
- Offering, giving, receiving, or soliciting anything of value to influence an outcome.
- Provision of unreasonable donations to fake charity organizations.
- Deliberate misapplication of accounting or other regulations or policies.
- The criminal act is the attempt to deceive, and attempted fraud is therefore treated as seriously as accomplished fraud.
- Computer fraud arises where information technology equipment has been used to manipulate program applications or data dishonestly (for example, by altering, substituting, or destroying records, or creating spurious records), or where the use of an IT system was a material factor in perpetration of fraud (for example, unauthorized access to relevant systems, overriding systems of controls). Theft or fraudulent use of computer time and resources is included in this definition.

Some illustrations of incidents which would be classified as fraud are contained in Appendix 1 to this Policy.

Forgery & Deception refers to the act of offering, giving, promising, asking, agreeing, receiving, accepting, or soliciting something of value or of an advantage so to induce or influence an action or decision also to any inducement, reward, or object/item of value offered to another individual to gain commercial, contractual, regulatory, or personal advantage.

Forgery & Deception is not limited to the act of offering a bribe. If an individual is on the receiving end of a bribe and they accept it, they are also breaking the law.

Forgery & Deception is illegal. Employees must not engage in any form of Forgery & Deception, whether it be directly, passively (as described above), or through a third party. They must not bribe a foreign public official anywhere in the world. They must not accept bribes to any degree and if they are uncertain about whether something is a bribe or a gift or an act of hospitality, they must seek further advice from the company's compliance officer.

3- Managing the Risk of Fraud – Responsibilities

The Firm takes a proactive approach to fraud risk management via sustaining and continuously promoting zero-tolerance attitude towards fraud, promulgating fraud awareness culture among all employees.

The Firm will initiate and undertake an investigation where there is suspected fraud and take appropriate legal and/or disciplinary action in all cases where that would be justified. Where there is fraud (suspected or proven), each firm should make any necessary changes to the existing Internal Control Framework (i.e. systems and procedures) to ensure prevention of any future occurrence of similar fraud. The firm maintains records and subsequently monitors all discovered cases of fraud (suspected or proven) and the effectiveness of corrective measures implemented.

Overall responsibility for managing the risk of fraud has been assigned to the Senior Management and the Compliance and Risk functions.

Responsibility for exercising disciplinary actions, as consequence management, rests with the Human Resources department, where appropriate in consultation with the Senior Management Team.

The Management are responsible for overall management of fraud risk, including:

- Establishing and maintaining sound systems of risk management and internal control that support the achievement of company's strategy and business objectives;
- Defining a fraud risk profile and undertaking a regular review of the fraud risks associated with each of the key organizational objectives to keep the profile up to date;
- Establishing appropriate mechanisms for reporting issues related to fraud risk;
- Ensuring development of a system for prompt, competent, and confidential review, investigation, and resolution of instances of noncompliance and allegations involving potential fraud;
- Ensuring that all employees are aware of the Firm's overall attitude to fraud and their individual responsibilities in relation to combating fraud;
- Ensuring that appropriate anti-fraud training is available to the employees;
- Choosing appropriate consequence management towards employees committing fraud;
- Ensuring that appropriate actions are taken to safeguard the recovery of assets;
- Ensuring that efficient and economically sound actions are taken to prevent future recurrence of similar frauds;
- Ensuring there is a process for tracking and case management where all allegations of fraud are logged.

Each department have overall responsibility for preventing, detecting, and managing the fraud risk on a day-to-day basis, including:

- Identifying and assessing of fraud risks to which systems, operations and procedures within their area of accountability are exposed;
- Designing, developing and maintaining effective system of internal control which ensures prevention and timely detection of fraud risks;
- Ensuring that established internal controls are being continuously complied with and relevant systems continue to operate effectively.
- Regularly reviewing and testing controls in place, questioning the adequacy, relevance and robustness of the overall system of internal control, and, where appropriate, implementing new controls to reduce the risk of similar fraud occurrence in the future.

Confronting Cases of Fraud, Forgery & Deception Policy

Every employee is responsible for:

- Acting with propriety in the use of the Firm's resources and the handling and usage of funds whether they are involved with cash or payments systems, receipts or dealing with suppliers or customers.
- Being conscious of the possibility that unusual events or one-off transactions could be indicators of potential fraud.
- Immediately reporting details of suspected fraud or irregularity through the established information channel
- Co-operating fully with dedicated employees assigned to conduct internal checks, reviews, or fraud investigations.

Responsibilities of any appointed Internal Auditor include:

- Delivering an opinion to the Senior Management and Board or to whom the Board discharged has governance and control function over the systems of risk management and internal control, on the adequacy of arrangements for managing the risk of fraud and ensuring that the Firm promotes and sustains anti-fraud culture.
- Assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness and efficiency of internal controls commensurate with the extent of the potential exposure/risk in the various segments of the Firm's business.

4- Fraud Response

To ensure that effective and timely action is taken in a professional manner to any suspected or proved fraud or any other irregularity, the Firm has established an overall response procedure which defines the steps to be followed in such cases.

Fraud Detection

Every employee may come across indicators of potential fraud in the due course of daily operational activity. As an example, unusual events or one-off transactions as well as any unintentional incident or action, which is not part of the normal operation of the system or the expected course of actions and events, could be indicators of potential fraud. All employees should be alert to the possibility of fraud and ensure timely reporting of any suspicious indicators discovered.

Fraud may also be highlighted because of specific and/or unscheduled management checks or be brought to management's attention by a third party. Additionally, irregularities may occasionally come to light during audit engagements.

Reporting

When an employee suspects that a fraud or irregularity has occurred, the employee should notify the Compliance Officer.

Speed is of the essence and such initial report can be verbal and must be followed up within 24 hours by a written report addressed which should cover:

- The amount/value, if established;
- The position regarding recovery;
- The period over which the fraud or irregularity occurred, if known.
- The date of discovery and how the suspected fraud or irregularity was discovered;

Confronting Cases of Fraud, Forgery & Deception Policy

- Whether the person responsible has been identified;
- Whether any collusion with others is suspected;
- Details of any actions taken to date;
- Any other information or comments which might be relevant.

Investigation/Further Actions

A preliminary review will be conducted with respect to any allegation of potential fraud to validate the suspicion raised and assess whether the case is substantiated enough to start the investigation process.

The Firm is committed to perform comprehensive analysis of all factors, which gave rise to the suspicion of potential improper activity to conclude whether a genuine mistake has been made or irregularity has occurred and keep the regulator informed in all applicable cases.

The preliminary review and consequent investigation will be organized and performed strictly in a timely manner. Prompt action is an essential aspect.

Upon the completion of the investigation the Firm will determine the course of action to be taken, including application of the required legal and disciplinary measures and keep the regulator informed in all the cases which are deemed to be appropriate. A Suspicious Activity Report maybe filed if applicable in line with the AML Policy of the Firm and as mandated by the UAE Financial Intelligence Unit (FIU).

The Firm may, for example, incorporate changes to the existing internal control framework (business process re-engineering, incorporation of IT systems, development of internal policies and procedures) to prevent occurrence of similar cases in the future.

Information on all allegations regarding suspected or proved Improper Activities will be maintained in the corporate case-tracking registers. The data logged in the register will contain the executive summary of the results of all the conducted investigation and all consequence management in case organizer.

5- Anti-Bribery & Corruption – Acceptable and Not Acceptable

5.1. Gifts and Hospitality

The Firm accepts normal and appropriate gestures of hospitality and goodwill (whether given to/received from third parties) so long as the giving or receiving of gifts meets the following requirements:

- It is not made with the intention of influencing the party to whom it is being given, to obtain or reward the retention of a business or a business advantage, or as an explicit or implicit exchange for favors or benefits.
- It is not made with the suggestion that a return favor is expected.
- It is following local and SCA laws where applicable.
- It is given in the name of the company, not in an individual's name.
- It does not include cash or a cash equivalent (e.g. a voucher or gift certificate).
- It is appropriate for the circumstances (e.g. giving small gifts around Christmas or as a small thank you to a company for helping with a large project upon completion).
- It is of an appropriate type and value and given at an appropriate time, considering the reason for the gift.

Confronting Cases of Fraud, Forgery & Deception Policy

- It is given/received openly, not secretly.
- It is not selectively given to a key, influential person, clearly with the intention of directly influencing them.
- It is not above a certain excessive value, as pre-determined by the company's applicable policies.
- It is not offered to, or accepted by, a government official or representative or politician or political party, without the prior approval of the company's compliance manager.

****Please refer to the Firm's Compliance Policy and Manuals for details on the economic value acceptable for gifts.**

Where it is inappropriate to decline the offer of a gift (i.e. when meeting with an individual of a certain religion/culture who may take offence), the gift may be accepted so long as it is declared to the compliance manager, who will assess the circumstances, most important that staff of UEXO must declare about action of receiving and report the same Compliance manager.

The Firm recognizes that the practice of giving and receiving business gifts varies between countries, regions, cultures, and religions, so definitions of what is acceptable and not acceptable will inevitably differ for each. As good practice, gifts given and received should always be disclosed to the compliance manager. Gifts from suppliers should always be disclosed. The intention behind a gift being given/received should always be considered. If there is any uncertainty, the advice of the Compliance Officer should be followed.

5.2. Facilitation, Payments, and Kickbacks

The Firm does not accept and will not make any form of unapproved or informal facilitation payments of any nature. We recognize that some facilitation payments are a form of Forgery & Deception that involves expediting or facilitating the performance of a public official for a routine governmental action. We recognize that they tend to be made by low level officials with the intention of securing or speeding up the performance of a certain duty or action.

The Firm does not allow kickbacks to be made or accepted. We recognize that kickbacks are typically made in exchange for a business favor or advantage.

“UEXO” recognizes that, despite our strict policy on facilitation payments and kickbacks,

employees may face a situation where avoiding a facilitation payment or kickback may put their/their family's personal security at risk. Under these circumstances, the following steps must be taken:

- Keep any amount to the minimum.
- Ask for a receipt detailing the amount and reason for the payment.
- Create a record concerning the payment.
- Report this incident to the Compliance Officer.

5.3. Political Contributions

The Firm will not make donations, whether in cash, kind, or by any other means, to support any political parties or candidates. This may be perceived as an attempt to gain an improper business advantage.

5.4. Charitable Contributions

The Firm accepts the act of donating to charities – whether through services, knowledge, time, or direct financial contributions (cash or otherwise) – and agrees to disclose all charitable contributions it makes. Employees must be careful to ensure that charitable contributions are not used to facilitate and conceal acts of Forgery & Deception.

Confronting Cases of Fraud, Forgery & Deception Policy

All Charitable Contribution will be of the Firm will be with prior approval of the Compliance Department & the CEO of UEXO.

6- Employee Responsibility in relation to Anti Bribery and Corruption

As an employee of “UEXO”, you must ensure that you read, understand, and comply with the information contained within this policy, and with any training or other anti- Forgery & Deception and corruption information you are given.

All employees and those under our control are equally responsible for the prevention, detection, and reporting of bribery and other forms of corruption. They are required to avoid any activities that could lead to, or imply, a breach of this policy.

If you have reason to believe or suspect that an instance of Forgery & Deception or corruption has occurred or will occur in the future that breaches this policy, you must notify the Compliance Officer.

If any employee breaches this policy, they will face disciplinary action and could face dismissal for gross misconduct. The Firm has the right to terminate a contractual relationship with an employee if they breach this policy.

How to escalate

If you suspect that there is an instance of Forgery & Deception or corrupt activities occurring in relation to the Firm, you are encouraged to raise your concerns at as early a stage as possible. If you’re uncertain about whether a certain action or behavior can be considered Forgery & Deception or corruption, you should speak to the Compliance Officer via email.

Whistleblower policy to be implemented her in term of reporting and protect the reporter of violation.

7- Training and Communication

The Firm will provide training on this policy for all employees. Employees will also receive regular, relevant training on how to adhere to this policy, and will be asked annually to formally accept that they will comply with this policy.

8- Record Keeping

The Firm will keep detailed and accurate records and will have appropriate internal controls in place to act as evidence for all payments made. We will declare and keep a written record of the amount and reason for hospitality, or gifts accepted and given, and understand that gifts and acts of hospitality are subject to managerial review.

9- Monitoring and Review

UEXO’s compliance officer is responsible for monitoring the effectiveness of this policy and will review the implementation of it on a regular basis. They will assess its suitability, adequacy, and effectiveness.

Internal control systems and procedures designed to prevent bribery and corruption are subject to regular audits to ensure that they are effective in practice. Any need for improvements will be applied as soon as possible.

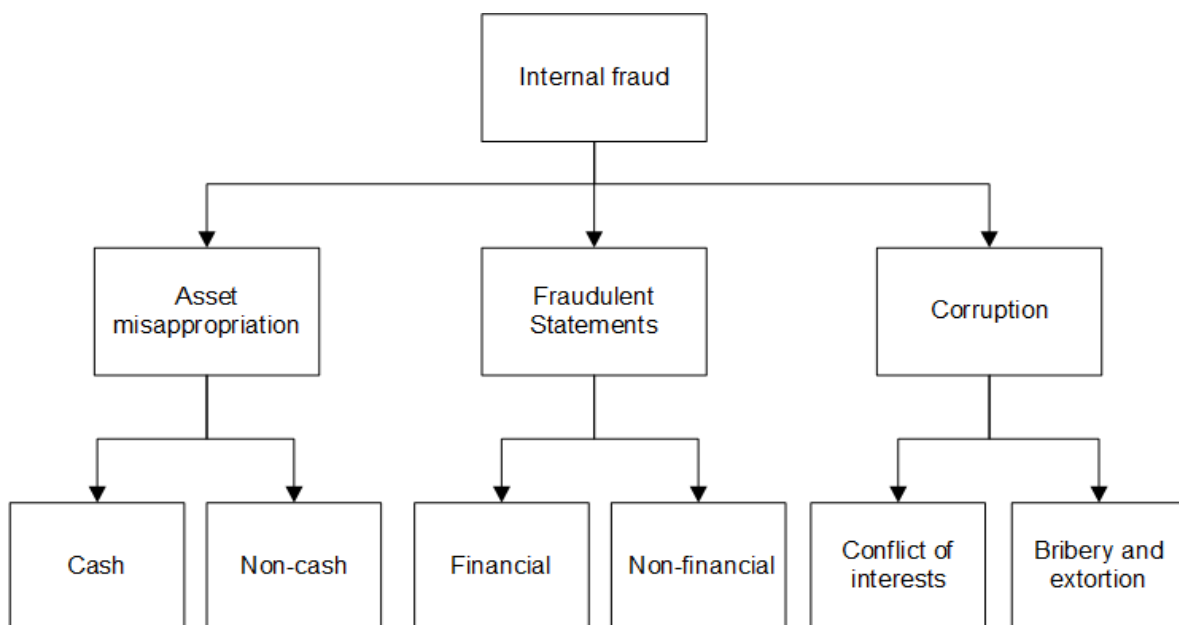
Appendix 1

Where Might Fraud Happen

Fraud can happen wherever employee, partnering organizations or independent contractors complete official documentation and can take financial advantage of the Firm. The risk of fraud is enhanced where employees or contractors are in positions of trust or responsibility and are not checked or subjected to effective monitoring or validation.

There are various frauds schemes used by perpetrators. As an example, below several types of internal fraud are provided:

Figure 1. Types of internal fraud



Examples of Internal Fraud include, but not limited to the below presented:

1. Asset misappropriation:

1.1.Cash:

- Theft of cash: stealing money from petty cash.
- False payments: employee creating false payments instructions with forged signatures and submitting it for processing.
- Billing schemes: over billing customers; recording of false credits, rebates or refunds to customers; pay and return schemes; using fictitious suppliers or shell companies for false billing.
- Misuse of accounts: unrecorded sales or receivables; employee account fraud (where an employee is also a customer, and employee makes unauthorized adjustments to their accounts)

1.2.Non-cash:

- Inventory and fixed assets: theft of inventory; false write-offs and other debits to inventory accounts.
- False sale of inventory; theft of fixed assets including computers and other IT related assets.
- Receiving free or below market value or goods from suppliers; unauthorized private use of corporate property.
- Theft or abuse of proprietary or other confidential information (customer information, intellectual property; pricing schedules, etc.);
- Contracting and procurement: falsifying documents to obtain authorization for payment.
- Forging signatures on payment authorization; submitting false invoices for payment or from fictitious suppliers.
- Sending fictitious or duplicate invoices to suppliers; mark- up invoices from contracts awarded to suppliers associated with employees.
- Intercepting payments to suppliers; sale of critical bid information, contract details or other sensitive information; improper change to supplier's payment terms or other details.

- Payroll: fictitious (ghost) employees on the payroll; falsifying work hours to achieve fraudulent overtime payments.
- abuse of commission schemes; improper changes in salary levels; abuse of holiday leave or time off entitlements; submitting inflated or false expense claims.
- adding private expenses to legitimate expense claims; applying of multiple reimbursement of the same expenses; false workers' compensation claims.

2. Fraudulent Statements:

2.1.Financial:

- Improper revenue recognition: holding the books open after the end of the accounting period.
- inflation of sales figures which are credited out after the year end;
- backdating agreements; improper classification of revenues;
- recording fictitious sales and shipments; inappropriate estimation of returns, price adjustments and other concessions; over/under estimation of work completed under long- term contracts; incorrect inclusion of related part receivables, etc.
- adjust allowances related to credit notes and or inventory balances and or security deposit amounts.
- Impose high and fake rate of bonuses to be paid to staff or TAX fraud.

Misstatement of assets, liabilities and/or expenses:

- Fake fixed assets;
- Overstating assets acquired (through mergers and acquisitions);
- Incorrect value attached to goodwill, manipulation of fixed assets valuation.
- Off balance sheet items.
- Delaying recording the expenses to the next accounting period, etc.;

Other accounting misstatements:

- Improper treatment of inter- company accounts; non- clearance or improper clearance of suspense accounts;
- fake general ledger accounts; journal entry fraud; improper or inadequate disclosures, etc.;

2.2.Non-financial.

Include falsified employment credentials (e.g., qualifications and references) and other fraudulent internal or external documents.

3. Corruption:

3.1.Conflict of interests:

- Kickbacks: kickback to employees by a supplier in return for a supplier receiving favorable conditions; purchase of a property at a price higher than market value in exchange of the kickback.
- Preference treatment of a customer in exchange for a kickback, etc.;
- Personal interest: collusions with customers/suppliers; favoring a supplier in which an employee has financial interest.
- Transfer of knowledge to a competitor by an employee who intends to join the competitor's company; insider trading; etc.;

3.2.Forgery & Deception

- Fraud, Forgery & Deception: payment of agency/facilitation payment in order to secure a contract; authorizing orders to a particular supplier in return for Fraud.

- Giving and accepting payment to favor/not to favor other commercial transactions or relationships; anti-trust activities, such as price fixing or bid rigging, etc.
- Extortion: blackmail (offering to keep information confidential in return for money or other consideration);
- Extortion (offering to keep someone from harm in return for money or other consideration).

These examples do not represent a comprehensive list of potential frauds but can be used only as an illustration only.

UEXO environment as per business module may differ if what mentioned above in this appendix, the main idea is just to give example per each case and to make sure that risk management team along with internal audit are able to do the needed register for all potential and actual cases so that can lead to more solid corporate governance along with process reengineering.