Typologies Report on ML/TF through Legal Persons and Legal Arrangements in MENA region

May 2025

The Middle East and North Africa Financial Action Task Force (MENAFATF) is a voluntary and cooperative body, independent from any other international body or organization. It was established by agreement between the governments of its member countries and was not created based on an international treaty. MENAFATF determines its own work, systems, rules, and procedures, and cooperates with other international bodies, especially the Financial Action Task Force (FATF), to achieve its objectives.

For more information about the Middle East and North Africa Financial Action Task Force, please visit the website: http://www.menafatf.org/

This document and/or any data or map included herein are without prejudice to the status or sovereignty over any territory, the delimitation of international boundaries and borders, or the naming of any territory, city, or area.

Table of Contents

Introduction

General Background

Institutional mechanisms[1] such as companies, trust funds, private interest foundations, and other legal persons and legal arrangements play a vital role in the global economy, particularly through their engagement in various commercial, charitable, and other legitimate activities. However, due to the particular nature and legal status of these legal persons and arrangements, they may be vulnerable to misuse in criminal schemes and illicit purposes such as money laundering, terrorist financing, bribery, corruption, tax evasion, and sanctions evasion. Criminals often resort to various methods, techniques, and complex structures to conceal the identity of the beneficial owner, the source and destination of funds, and the underlying purpose of transactions.

The results of the second round of mutual evaluations for countries in the Middle East and North Africa region revealed clear shortcomings in compliance with relevant standards and in achieving adequate levels of effectiveness in preventing the misuse of legal persons and arrangements for money laundering and terrorist financing purposes. Evaluation reports for MENAFATF member countries showed that, out of the 10 countries assessed, 60% still require substantial improvements, while the remaining countries need basic improvements concerning Immediate Outcome 5, which focuses on preventing the misuse of legal persons and legal

[1] This report uses the term "institutional mechanisms" to refer to legal persons and legal arrangements, as defined in the terminology of the Financial Action Task Force (FATF) Recommendations.

arrangements for ML/TF and ensuring that information on beneficial ownership is available to competent authorities without impediments.

Accordingly, in response to the increasing threat posed by evolving ML/TF risks and the failure to prevent the criminal and terrorist use of legal persons and legal arrangements—due to the lack of sufficient, accurate, and up-to-date information on beneficial owners and those exercising effective control—the Financial Action Task Force (FATF) has, over the years, reviewed and identified the need to strengthen the standards to ensure greater transparency and to mitigate associated risks. This led to the FATF's adoption of: (a) amendments to Recommendation 24 and its Interpretive Note in March 2022; and (b) amendments to Recommendation 25 and its Interpretive Note in March 2023, as a significant first step in addressing the misuse of legal persons and legal arrangements. These changes are expected to significantly enhance beneficial ownership transparency requirements globally, while retaining some flexibility for countries to advance the improvement of their systems.

The FATF is also currently developing comprehensive guidance to assist countries in implementing the amended standards under Recommendation 25, as it did in March 2023 when it adopted detailed guidance for the implementation of the revised Recommendation 24. The FATF emphasized that effective implementation of the new standards and risk responsiveness will require constructive and ongoing efforts by all countries.

Objectives and Scope of the Project

Based on reports, research findings, and studies conducted on the subject of beneficial ownership transparency for legal persons and legal arrangements, it is evident that the misuse of legal persons and legal arrangements for money laundering and terrorist financing remains a challenge for many countries around the world. Mutual evaluations conducted by the Financial Action Task Force (FATF) have shown, in general, an insufficient level of effectiveness in combating the abuse of legal persons for ML/TF purposes globally, and that countries need to exert more effort to implement the current FATF standards promptly, fully, and effectively.

In light of the above, there emerged a need to implement a typologies project to study and understand the scope of risks associated with the misuse of legal persons and legal arrangements in money laundering and terrorist financing operations in the Middle East and North Africa region, to identify the key techniques and methods used by criminals, present several case studies that reveal instances of misuse, and highlight the most relevant red flag indicators and challenges.

This project primarily aims to achieve the following objectives:

- Understanding and identifying the risks of legal persons and legal arrangements in ML/TF operations by studying threats and vulnerabilities.
- Identifying the methods, ways, and techniques used in money laundering and terrorist financing through legal persons and legal arrangements in the region.
- Presenting the most important red flag indicators.

- Analyzing case studies that will enable countries to detect and report instances of misuse of legal persons and legal arrangements in ML/TF operations.
- Identifying the challenges faced by countries in detecting the misuse of legal persons and legal arrangements and in ensuring the availability of beneficial ownership information to competent authorities without obstacles.
- Proposing recommendations that would enhance the effectiveness of applying the relevant international standards and address the challenges faced by countries in confronting these risks and ensuring compliance with international standards.

Methodology Adopted in the Preparation of the Project

1. The Literary Approach:

This involves reviewing all reports, research, and references issued by international organizations on the subject, in order to establish a clear vision that serves as the fundamental basis for determining the information required to be collected from member countries for subsequent analysis, in line with the study's objectives and nature. The information used in this project was collected from multiple sources, as outlined below:

- Information and case studies provided by member countries in response to the project's information request questionnaire. The relevant questionnaire is divided into four parts: the first and second parts address vulnerabilities and threats; the third part focuses on trends, methods, and techniques used; and the final part covers practical case studies and key red flag indicators.

- The FATF guidance on "Transparency and Beneficial Ownership" (2023).
- Review of FATF Recommendations 24 and 25 along with their Interpretive Notes, and the amendments to the Glossary, in addition to FATF guidance related to Recommendations 24 and 25, whether published or under development.
- The IMF guidance titled "Unmasking Control: A Guide to Beneficial Ownership Transparency" (2022).
- The World Bank report titled "Signatures for Sale: How Nominee Services for Shell Companies Are Abused to Conceal Beneficial Owners" (2022).
- The OECD report on the Beneficial Ownership Implementation Toolkit (2019).
- The Egmont Group report titled "Concealment of Beneficial Ownership" (2018).
- Any other relevant reports.

2. The Descriptive/Analytical Approach :

This involves analyzing all data and information collected through the questionnaire and case studies submitted by MENAFATF member countries, in order to draw conclusions.

3. The Inductive Approach:

This consists of identifying the challenges and developing recommendations and suitable solutions to overcome them.

Contributing Entities, Project Team, and Report Preparation Stages

1. Contributing Entities

- **Provision of information and case studies:**
  Hashemite Kingdom of Jordan, United Arab Emirates, Kingdom of Bahrain, Republic of Tunisia, People's Democratic Republic of Algeria, Kingdom of Saudi Arabia, Republic of the Sudan, Syrian Arab Republic, Republic of Iraq, Sultanate of Oman, State of Palestine, State of Qatar, State of Kuwait, Arab Republic of Egypt, Kingdom of Morocco, Republic of Yemen.
- **Technical work on the project:**
  The Secretariat of the Middle East and North Africa Financial Action Task Force (MENAFATF), and the German Agency for International Cooperation (GIZ).

2. Project Team

- **Project Leader**
  Sara Sandid, Senior Officer for Technical Assistance and Typologies Department, FATF Certified Assessor, and Trainer, MENAFATF Secretariat,
- **Experts Involved in the Project**
  - *Literature Review:*
    Andres Knobel, Expert at the German Agency for International Cooperation.
  - *Analysis, Conclusions, Recommendations, and Drafting Report:*
    Sara Sandid, Senior Officer for Technical Assistance and Typologies Department, FATF Certified Assessor, and Trainer, MENAFATF Secretariat
  - *Literature Review of Member State Contributions:*
    - *Sara Sandid*, Senior Officer for Technical Assistance and Typologies Department, FATF Certified Assessor, and Trainer, MENAFATF Secretariat
    - *Raghad Abdelrahman Abu Hassan*, Financial Analyst, Anti-Money Laundering and Counter-Terrorist Financing Unit – Hashemite Kingdom of Jordan
  - *Quality Review of Information Provided by Member States:*
    To ensure the accuracy and relevance of the information and model case studies submitted, national experts from contributing countries played a key role in validating, reviewing, and refining the contributions. These reviewers worked closely with the Secretariat to ensure that all examples included in the report adhered to methodological and confidentiality standards.
    - *Yousef Harbawi* – Information and Analysis Department, Financial Follow-Up Unit – State of Palestine
    - *Rahma Al-Inglais* – Head of Statistics and Strategic Analysis Unit, Tunisian Financial Analysis Committee – Republic of Tunisia

- *Mohamed Ritan* – Head of Supervision and Compliance Department, National Financial Intelligence Authority – Kingdom of Morocco
- *Raghad Abu Hassan* – Financial Analyst, Anti-Money Laundering and Counter-Terrorist Financing Unit – Hashemite Kingdom of Jordan
- *Zainab Fouad Thanoub* – Officer at the Information Collection Unit, Financial Investigation Unit – Syrian Arab Republic
- *Nardine Samy Gabriel Afram* – Researcher, Research and Strategic Analysis Department, Anti-Money Laundering and Counter-Terrorist Financing Unit – Arab Republic of Egypt
- *Ahmed Al-Mazrouei* – Research and Studies Executive, Executive Office for Anti-Money Laundering and Counter-Terrorism Financing – United Arab Emirates

- *Review of the First Draft of the Report:*
  The following experts from member countries contributed to reviewing the technical content and analytical accuracy of the report:
  - *Raghad Abu Hassan* – Financial Analyst, Anti-Money Laundering and Counter-Terrorist Financing Unit – Hashemite Kingdom of Jordan
  - *Ahmed Al-Mazrouei* – Research and Studies Executive, Executive Office for Anti-Money Laundering and Counter-Terrorism Financing – United Arab Emirates
  - *Hamza Najmi* – Kingdom of Saudi Arabia
  - *Mohamed Ritan* – Head of Supervision and Compliance Department, National Financial Intelligence Authority – Kingdom of Morocco

3. Report Preparation Stages

The project was implemented according to a defined timeline from November 2022 to April 2025. The main stages included:

- November 2022: Project Launch
- January 2023: Formation of the Project Team
- February 2023: Development of the Report Structure
- March – November 2023: Drafting of Concepts and Chapter One
- November 2023: Preparation and Distribution of the Questionnaire
- November 2024: Preliminary Results – 16 Countries (over 70%)
- December 2024 – April 2025: Data Analysis and Conclusion Drawing
- April 2025: Preparation and Circulation of the First Draft
- April – May 2025: Preparation and Final Approval of the Second Draft

Concepts and Definitions

- **Legal Arrangements**: This term refers to express trusts or similar legal arrangements. Examples of such arrangements for AML/CFT purposes include (but are not limited to): *fiducie*, certain types of *Treuhand*, *fideicomiso*, and *waqf*.
- **Legal Persons**: Legal persons refer to any entity other than natural persons that can establish a permanent business relationship with a financial institution or own assets.

These include companies, corporate bodies, private interest foundations, *Anstalt*, partnerships, associations, or any similar entities.

- **Legal Entities**: Legal entities refer to any entity established by law that has a separate legal personality, the ability to own assets, enter into contracts, and sue or be sued. These include corporations such as joint stock and limited liability companies, associations, foundations, cooperatives, and any other legally registered entity.
- **Legal Structures**: Legal structures refer to arrangements or legal relationships used to manage or control assets on behalf of a third party, without necessarily having separate legal personality. These include trusts and similar arrangements found in some legal or customary systems, such as *waqf*, typically used for asset management or distribution for specific purposes.
- **Nominator**: A person, group of persons, or legal person who directly or indirectly instructs another person to act on their behalf as a director or shareholder. This individual is sometimes referred to as a "shadow director" or "silent partner."
- **Nominee Director**: An individual or entity officially appointed as a board member of a legal entity but who does not act independently, rather implements instructions from another party considered to be the real beneficial owner. This arrangement is sometimes used to conceal the identity of the true controller and is also known as a "resident director," who routinely performs director duties on behalf of the nominator but is not the beneficial owner.
- **Nominee Shareholder**: An individual or legal person who holds shares or ownership in a company on behalf of another person (the beneficial owner), based on a formal or informal agreement. The nominee exercises voting rights and may receive dividends according to the nominator's instructions, without being the actual beneficial owner. This setup may be used to conceal the identity of the real owner of a legal entity.
- **Beneficial Owner**: The natural person who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is conducted. It also includes those who exercise ultimate effective control over a legal person or arrangement.
- **Beneficiary**: Under trust law, a beneficiary is a person or persons entitled to benefit from a trust arrangement. The beneficiary may be a natural or legal person or arrangement. All trusts (except charitable or otherwise legally permitted non-charitable trusts) must have identifiable beneficiaries. While trusts must always have an ultimately ascertainable beneficiary, they may initially have no defined existing beneficiaries, only potential ones—until a specific point (the accumulation period) when a person becomes entitled to income or capital.
- **Bearer Shares**: These are negotiable instruments that confer ownership in a legal person to the individual physically holding the share certificate, without requiring identification. This term does not include dematerialized or registered certificates that can be traced and whose ownership is clearly identifiable.
- **Bearer Share Certificates**: Negotiable instruments granting ownership in a legal person to whoever physically holds the certificate, without the need to verify identity. This category excludes dematerialized forms or registered shares that are traceable.

- **Bearer Negotiable Instruments**: These include monetary instruments in bearer form such as traveler's cheques, negotiable instruments (including cheques, promissory notes, and money orders) that are either bearer, endorsed without restriction, made out to fictitious payees, or otherwise transferable by delivery; as well as incomplete instruments signed but with the payee's name left blank.
- **Trustee**: The terms "trust" and "trustee" should be understood as defined in Article 2 of the Hague Convention on the Law Applicable to Trusts and Their Recognition. Trustees may be professionals (e.g., lawyers or trust companies, depending on the jurisdiction) when paid to act in the course of business, or non-professionals (e.g., a family member acting without compensation).
- **Settlor**: A settlor is a natural or legal person who transfers ownership of assets to trustees via a trust deed or similar legal arrangement.

Report on Structure

The report was structured based on the study's methodology and objectives. In **Chapter (I)**, it provides an overview of the misuse of legal persons and legal arrangements by criminals, based on the results of the review of existing studies. In **Chapter (II)**, it presents the most significant trends and methods used to misuse legal persons and legal arrangements in the Middle East and North Africa region, as revealed by the analyzed case studies. This structure aims to lead to a general conclusion that highlights the key findings and major challenges, and consequently, proposes recommendations aligned with the actual context of the misuse of legal persons and legal arrangements in the MENA region.

Chapter I: An Overview of the Misuse of Legal Persons and Legal Arrangements by Criminals – A Review of Studies

Legal entities (or "corporate vehicles") are essential tools in supporting the global economy by facilitating trade, investment, and philanthropy. While their use is lawful and legitimate in most cases, their flexibility, ease of establishment, and ability to access the global financial system—such as by opening bank accounts, obtaining loans and other financial products, and owning assets—make them vulnerable to misuse in financial crimes such as money laundering, terrorist financing, corruption, fraud, and tax evasion.

Given the difficulty in distinguishing between legitimate entities and those used for criminal purposes, identifying such misuse poses a significant challenge. However, understanding the threats, legal vulnerabilities, and common methods of misuse can help authorities better allocate resources for monitoring, investigation, and prevention of financial crimes.

1.1. Key Money Laundering and Terrorist Financing Threats Facing Legal Persons and Legal Arrangements

A **threat** refers to a person, group of persons, entity, or activity that has the potential to cause harm. Below is a list of major financing threats involving **corporate vehicles**, from a global perspective:

- Tax crimes (e.g., tax fraud and tax evasion).
- Corruption (e.g., concealing and transferring bribe payments or embezzled public funds, illegal financing of political parties, hiding conflicts of interest—particularly involving politically exposed persons (PEPs)).
- Fraud (e.g., against the state, as well as defrauding customers who invest in or purchase goods and services from bogus companies).
- Trade-based crimes (e.g., circumventing capital controls, money laundering, and evading import/export duties by involving exporters, importers, shipping companies, and facilitators).
- National security risks (e.g., high-risk or conflict-state actors, or sanctioned individuals holding interests in strategic industries with cutting-edge or military technologies, or in sensitive economic or political infrastructure).
- Circumvention of sanctions and prohibitions (e.g., natural or legal persons listed on UN or national sanctions lists who evade sanctions by concealing their assets or interests in corporate vehicles, especially in financial institutions—and hiding their identity to engage in trade, investments, or to obtain financing).
- Political interference (e.g., foreign states, parties, or individuals engaging in fake news, phishing, divisive rhetoric, or other strategies to influence political processes).
- Illicit trafficking in narcotic drugs and psychotropic substances.
- Illicit cross-border transportation of cash.
- Human trafficking and migrant smuggling.
- Environmental crimes (e.g., illegal fishing, illegal deforestation, etc.).

1.2. Inherent, Internal, and External Vulnerabilities of Legal Persons and Legal Arrangements

Corporate vehicles can be misused for the purposes of money laundering and terrorist financing by concealing or disguising:

(a) the identity of their managers and owners (especially the beneficial owners); (b) the income and assets held by the corporate vehicles, including their source, use, and destination; or
(c) the purpose of the corporate vehicles, their transactions, and relationships.

1.2.1. Concealment of Owners and Controllers (Beneficial Owners)

In summary, the main vulnerability affecting corporate vehicles lies in the concealment or obfuscation of their **beneficial owners**. The vulnerability regarding beneficial ownership information may manifest as follows:

- **Availability of beneficial ownership information**:
  In many cases, beneficial ownership information is not collected at all. This may be due to:
    - The corporate vehicle is not subject to beneficial ownership information requirements, either deliberately (e.g. based on the type, nationality, or ownership of the entity, or by virtue of certain exemptions), or inadvertently

(e.g. due to inadequate scope or definitions, especially for foreign legal persons).
    - The legal definition of "beneficial owner" does not encompass all relevant individuals (e.g. due to definitional elements or thresholds).
- **Identification of the beneficial owner (actual identification of the real individual)**: Although both the corporate vehicle and its beneficial owner are supposed to be identified and verified, the process is often hindered. This may stem from:
    - Use of shelf companies
    - Complex ownership structures
    - Use of bearer shares
    - Appointment of nominee directors or shareholders
    - Use of online virtual corporate service providers
- **Accuracy of beneficial ownership information**:
    - Information on beneficial owners may be outdated
    - Details may be incorrect or unverified
- **Collection or retention of beneficial ownership information**:
  The availability of beneficial ownership data may be undermined due to:
    - Government registries (of legal and beneficial ownership) being inadequate or ineffective
    - Financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs)—such as lawyers, notaries, and corporate service providers—not being subject to adequate AML/CFT obligations, lacking awareness of their duties, or failing to implement them.
- **Access to beneficial ownership information**:
  The ability of competent authorities to access such information may be limited due to:
    - Lack of access, or untimely/inappropriate access mechanisms
    - Lack of international information exchange with foreign jurisdictions
    - Professional secrecy provisions, such as attorney-client privilege

Availability of Beneficial Ownership Information

A) The Corporate Vehicle

The main vulnerability affecting a corporate vehicle lies in the fact that one type—or in some cases all types—of corporate vehicles may not be subject to beneficial ownership information requirements. This means that no beneficial ownership information may be available for that corporate vehicle. This lack of information may result from the following :

- **Absence of a Beneficial Ownership Framework:** The country's legal framework does not mandate the collection of beneficial ownership information for any type of corporate vehicle under any approach (e.g. registry-based, company-based, or existing information-based approaches).
- **Inconsistencies Within the National Legal and Regulatory Framework:** The country may contain multiple jurisdictions or regions, including free zones or special

economic zones, where beneficial ownership requirements may not apply or where there are inconsistencies in definitions and scope. This may result in arbitrage opportunities exploited by individuals seeking to conceal their identity.

- **Country of Incorporation Loopholes:** The legal framework may mandate beneficial ownership registration (e.g. through a national register), but apply this requirement only to domestic corporate vehicles, excluding foreign entities, even if those foreign entities hold assets or conduct operations within the jurisdiction.
- **Entity Type Loopholes:** The beneficial ownership framework may apply only to companies and exclude other legal persons or apply only to legal persons and exclude trusts or other legal arrangements, or exclude certain vehicles deemed not to have separate legal personality (e.g. limited partnerships in certain jurisdictions).
- **Exemptions From Scope:** The legal framework may exempt specific sub-categories of entities, such as state-owned enterprises and their subsidiaries, publicly listed companies and investment funds, or other entities like charities, non-profits, and political parties.
- **Lack of Awareness or Inconsistency with Foreign Legal Frameworks:** The framework may:
    - Lack provisions for "exotic" foreign legal vehicles (e.g. Liechtenstein Anstalt, companies limited by guarantee, discretionary trusts, or protected cell companies).
    - Treat foreign entities as domestic based on naming similarities, even when legal differences exist (e.g. treating a foreign private-interest foundation as a local public charity or a foreign *waqf* as a local trust).
- **Inactive Entities:** Dormant or inactive entities—those that conduct no operations and fail to submit filings (e.g. no annual returns or accounts)—may continue to exist in registers without being struck off, particularly in weak enforcement environments. These entities may still hold assets or operate abroad, but their inactive status means beneficial ownership data may not be updated or available in response to foreign requests.

B) The Beneficial Owner

The main vulnerability affecting the beneficial owner lies in the fact that, although the corporate vehicle may be subject to the collection of beneficial ownership information (e.g., through registration in the beneficial ownership register), the definition of the beneficial owner does not cover all relevant beneficial owners. This means that authorities may not have information about all relevant individuals. This lack of beneficial ownership may be due to :

- **The definition does not cover all relevant elements: ownership, control, benefit.** According to the paper titled *"Beneficial Ownership Registration Around the World, 2022"*, some countries have defined the beneficial owner using three elements (i.e., ownership or control or benefit): individuals who ultimately own or exercise control over the corporate vehicle, or who may benefit from it (e.g., by receiving dividends). The EU AML Directive takes into account ownership, voting rights, or control through

other means. Most countries follow the FATF criteria as provided in the Interpretive Note to Recommendation 10 and include controlling ownership and control through other means. However, some countries consider only one element in their definition (e.g., only ownership, or only control, or only benefit). In addition, some countries do not take any measures in cases where no individual meets the ownership or control tests, allowing the entity to legally declare that it has no beneficial owners at all (instead of identifying at least a senior managing official).

- **High thresholds in the definition of the beneficial owner.** The FATF allows the use of a threshold in defining beneficial ownership that should not exceed 25%. In practice, however, any threshold can be circumvented. For example, Al Jazeera and Kroll described cases of corruption and money laundering where even a 5% threshold was circumvented. For this reason, some countries, particularly in Africa and Latin America—use lower thresholds in their definitions, such as 15%, 10%, 5% of shares, or even no threshold at all (where any individual with at least one share or vote must be considered a beneficial owner). However, some countries fail to include a threshold or define the beneficial owner as holding a "majority" of votes, which may suggest a 51% threshold.
- **Not all parties to the trust or private interest foundation must be identified.** Although FATF Recommendation 10 emphasizes the need to identify all parties to the trust (settlor, trustee, protector, beneficiaries, or class of beneficiaries, or any other natural person exercising ultimate effective control over the trust), some countries do not fully comply with this requirement, especially concerning protectors and indirect beneficiaries. The OECD has extended the reporting standard to include these indirect beneficiaries. As private interest foundations are structurally similar to trusts, the EU Directive mandates applying the same beneficial ownership rules to both. However, some countries do not extend this definition to cover private interest foundations or apply it only to simplified types of trusts, creating regulatory gaps that hinder transparency and facilitate misuse in financial crimes.
- **Inappropriate definitions for the type of entity.** The Interpretive Note to FATF Recommendation 10 highlights the need to tailor the beneficial ownership definition to the type of legal entity. While beneficial ownership in companies is defined through ownership of 25% or more of shares or control through other means, trusts require identifying all associated parties, including settlers, trustees, protectors, beneficiaries, and any person exercising effective control. However, some countries apply a unified and simplified definition based solely on ownership, even to entities where this criterion does not apply, such as trusts or limited partnerships—resulting in failure to identify the actual controlling parties. For instance, in limited partnerships, the general partner who manages the partnership may not be listed as a beneficial owner if he does not exceed the ownership threshold, despite exercising actual control.

  Additional issues arise with protected cell companies, such as U.S.-style series limited liability companies, where each sub-cell may have distinct owners and assets. If the definition of beneficial ownership applies only to the core entity without extending to sub-cells, the real owners of the sub-cells will be excluded—especially if their

ownership is distributed below the set threshold (e.g., 25%). This uniform and non-specialized approach to defining beneficial ownership creates significant gaps in transparency and facilitates the misuse of legal entities for money laundering and terrorist financing purposes, highlighting the need for accurate, tailored definitions that align with the nature of each legal entity to ensure the effectiveness of oversight efforts.

Identification of the Actual Beneficial Owner

Even if the corporate vehicle is subject to the collection of beneficial ownership information (e.g., through the beneficial ownership register), and the applicable definition of the beneficial owner is appropriate, there may still be obstacles to identifying the actual beneficial owner. This absence of a beneficial owner may be due to the following:

- **Shelf Companies.** These are companies that were deliberately established in the past by lawyers or other corporate service providers to be sold in the future. Typically, shelf companies already hold a bank account, have creditworthiness, a list of directors, and the appearance of legitimacy due to their long-standing existence. This means that criminals may purchase shelf companies for quick access to the financial system. In addition, if the shelf company fails to report a change in shareholders (and beneficial owners) in a timely manner, criminals can operate without disclosing any ownership information.
- **Complex Ownership Structures.** Complex ownership structures are among the main obstacles to identifying the beneficial owner, especially when they involve long chains of entities across several countries. The longer and more geographically spread these chains are, the higher the likelihood that intermediate layers cannot be traced, particularly if some entities are based in tax havens that do not comply with registration or information exchange. Some studies have revealed that ownership chains may include dozens of layers, making it difficult for authorities to confirm the identity of the ultimate beneficial owner and presenting a real challenge to transparency. The risks increase when complex structures such as circular ownership or multi-layered pyramidal structures are used, which may be intentionally designed to obscure real control from oversight authorities.
- **Bearer Shares.** Bearer shares are among the most dangerous tools for concealing the identity of the beneficial owner, as they are transferable instruments that allow the transfer of ownership without any official record. The bearer of the document is considered the effective owner at any time. This makes it difficult—if not impossible—to identify the beneficial owner unless up-to-date and accurate information about the holders is available. Although companies issuing this type of shares are required to disclose to their beneficial owners, that information may become inaccurate or unverifiable immediately after any transfer of ownership.
- **Nominees.** Nominee shareholders and directors are used in some countries, particularly those based on common law—as a means of concealing the identity of the beneficial owner. Professionals may register their names as shareholders or directors on behalf of

the real stakeholders, enabling the latter to remain hidden. In some cases, these nominees play an actual role as representatives of institutional investors, and the nomination is formal, documented through contracts or legal instructions, with the nominee acting as a paid legal front with no real knowledge of the entity's activities. In other cases, their role is limited to signing documents and receiving correspondence, with no oversight or actual knowledge of the entity's operations. They may be appointed verbally (informally) or through undocumented understandings, without any formal contractual relationship. This informal setup is particularly used in environments that lack oversight or where evasion of disclosure is easy, which increases the risk of exploiting such arrangements to conceal true identities and facilitate illicit activities.

- **Online Virtual Services.** The ability of individuals to create corporate vehicles virtually and remotely (via the internet) means fewer identity verification procedures (if any), which facilitate the use of fake identities and allows abuse of actual nominee proxies or individuals used as fronts.

Accuracy of Beneficial Ownership Information

Even if the corporate vehicle is subject to an appropriate definition and the beneficial owner refers to the actual beneficial owner (not a nominee proxy), there may still be issues with the quality of the information about beneficial owners, especially if the list of beneficial owners or their details is not updated when any changes occur, or if the information is incorrect.

- **Outdated Beneficial Ownership Information.** The FATF requires beneficial ownership information to be kept up to date. Some countries require corporate vehicles to update information on beneficial owners within 15 or 30 days of becoming aware of a change. In other cases, entities are only required to file an annual return with the current list of beneficial owners. In both scenarios, there is a risk of weak enforcement of these requirements, especially if authorities do not verify the number of entities that filed their annual returns or reported changes in beneficial ownership.
- **Incorrect Details of the Beneficial Owner.** As described by Global Witness based on their analysis of the UK beneficial ownership register, most countries face challenges in verification processes. This means that even if the registered beneficial owner is the actual beneficial owner rather than a nominee (which would be a very good starting point), the details may be incorrect. Errors may include misspellings of names, incorrect addresses or birthdates, and unclear information on the nature of beneficial ownership (e.g., whether the person is the actual owner, exercises control through indirect relationships, the nature of their control—direct ownership, voting power, informal influence—and the rationale or mechanism by which the person qualifies as a beneficial owner). In such cases, one challenge is the ability to contact or locate the beneficial owner.

Collection of Beneficial Ownership Information

The availability of beneficial ownership information may be affected by inadequacies in the entities that hold such information—such as the beneficial ownership register or the obliged entities collecting it. This may be due to:

- **Inadequate Registers for Beneficial Ownership.** The authority responsible for maintaining beneficial ownership information may be unsuitable. For example, there may be no centralized register. Instead, there may be registers in each province, region, or free zone, which are not interconnected.
- **Inadequate AML/CFT Framework.** In countries that rely on obliged entities to collect beneficial ownership information or report discrepancies—particularly where company service providers and other DNFBPs are heavily involved in the formation or management of corporate vehicles (e.g., by offering nominee services)—the main vulnerabilities are:
    - **Limited Scope.** The AML/CFT provisions may not cover all types of financial institutions or DNFBPs (e.g., in some countries, lawyers or investment funds are outside the scope).
    - **Conduct and Role of the Obliged Entity (from Willful Blindness to Collusion).** There is a spectrum of behaviors among obliged entities. Aside from fully honest and committed entities that seek to prevent money laundering and terrorist financing, these entities may range from being "willfully blind" (not asking questions or filing suspicious transaction reports for seemingly unrelated or separate transactions), to "corrupt" (maintaining willful blindness despite multiple red flags), to "fully complicit" (actively helping conceal beneficial ownership or directly engaging in ML/TF).
    - **Lack of Awareness and Understanding.** Financial institutions and some DNFBPs, especially small firms or sole practitioners, may be unaware of the rules or lack the infrastructure to comply.
    - **Weak Law Enforcement by Authorities.** Authorities may be unable to carry out supervision, inspections, or impose sanctions on obliged entities that fail to apply AML/CFT systems, do not file suspicious transaction reports, or fail to respond to information requests (or violate AML/CFT disclosure requirements).

Access to Beneficial Ownership Information

Even if the entities responsible for maintaining beneficial ownership information are effective in collecting such information, there may still be challenges for authorities in accessing it, which may prevent them from accessing the information in full or result in excessive delays in obtaining it. This may be due to the following:

- **Some authorities do not have adequate or timely access to the information.** Although most legal frameworks tend to permit many competent authorities to access beneficial ownership information, some authorities may still be excluded (e.g., law enforcement authorities), or access may be limited to the entity maintaining the information (such as tax administration) and not available to other authorities. Furthermore, even for authorities that are legally authorized to access the information, they may rely on obtaining a court order or submitting a formal request for information,

all of which may take weeks before the information is obtained. For example, before the United Kingdom established beneficial ownership registers, some law enforcement authorities reported that they could spend up to 50% of their time just to obtain beneficial ownership information.

- **Inadequate exchange of information with relevant foreign countries.** Given that foreign entities may not be covered by the beneficial ownership framework, competent authorities may need to request information from the foreign countries where those corporate vehicles are incorporated or administered. The same applies when authorities need information on a foreign entity that is part of an ownership chain and holds shares in a local entity. In both cases, authorities will depend on the existence of an international agreement or framework that permits the exchange of information (e.g., through the Egmont Group or through international agreements on the exchange of tax-related information). If the country lacks a legal basis for such an international exchange of information, or if the foreign country refuses to provide the information, or if the response takes several months, the competent authorities will not be able to identify or verify the beneficial owner in a timely manner.
- **Professional secrecy (e.g., attorney-client privilege).** Although the FATF requires designated non-financial businesses and professions (DNFBPs) to be subject to AML/CFT obligations (including responding to information requests from competent authorities), in some countries, certain professions such as lawyers may be excluded from the scope. Even if such professions fall within the scope of AML/CFT obligations, they may refuse to comply with information requests from authorities by invoking professional secrecy, especially attorney-client privilege. This becomes problematic when national frameworks do not properly distinguish between the lawyer's activities as part of the human right to a fair trial (where attorney-client privilege must apply), and situations where the lawyer acts as a corporate service provider unrelated to any legal proceedings.

1.2.2. Concealment of the Income and Assets of Corporate Vehicles

Given that there is usually no registration or reporting to a third-party regarding income (except for employers in some countries), and that there is limited information about asset ownership and value, corporate vehicles may conceal or falsify their income and assets for the purpose of conducting money laundering and terrorist financing activities. This issue is exacerbated by the following:

- **Virtual Assets.** Criminals may conceal their income and assets by holding encrypted assets such as Bitcoin, especially if they are held in "cold wallets" (rather than through an intermediary subject to anti-money laundering and counter-terrorist financing obligations).
- **Absence of (centralized) information on asset ownership and value.** Countries may have multiple local property registers instead of a centralized registry. Furthermore, there is no registration at all for some types of assets (e.g., precious metals, artwork, and virtual assets). Lastly, even for existing asset registers, information on price and ownership is not always collected. For this reason, except for some information on real

estate, vessels, vehicles, or aircraft—asset and income information are based on self-declaration by the corporate vehicle, making it difficult to verify its accuracy and authenticity.

- **Involvement of Gatekeepers.** Obliged entities, particularly lawyers, notaries, intermediaries, corporate service providers, and trust and company service providers may facilitate money laundering and terrorist financing through:
    - **Carrying out transactions (e.g.,) the purchase of real estate.** Professional intermediaries may facilitate the purchase or sale of real estate, either by claiming to perform due diligence on behalf of their clients or by executing the transaction directly on their behalf.
    - **Use of lawyer-held accounts or escrow accounts.** Lawyer-held accounts, such as bank accounts maintained by lawyers, pool funds from multiple clients for the purpose of securing fees related to legal proceedings. However, these accounts can be misused to enable money laundering and terrorist financing transactions for corporate vehicles (unrelated to any litigation), without alerting other obliged entities (e.g., banks) or authorities.
    - **Use of virtual offices, management services, and mailing addresses.** These services allow corporate vehicles to establish a nominal presence in a country, enabling the entity to falsify its activities, owners, and controllers, while the actual beneficial owners, their assets, and their activities remain concealed.

1.2.3. Concealment of the Purpose of Corporate Vehicles, Their Transactions, and Their Relationships

Due to the widespread use of corporate vehicles and the extensive nature of their transactions, relationships, and contracts, and the lack of transaction, relationship, or contract registration, it becomes extremely difficult to determine whether they are genuine or falsified, or whether they form part of a money laundering or terrorist financing scheme. This lack of information may be further aggravated by the following:

- **Shell Companies:** Entities that have no actual operations, office, staff, or physical presence beyond the incorporation document make it easy to falsify the purpose of the corporate vehicle (in the articles of association) and to pretend to offer other services or activities. In addition, they can usually be created remotely and within a few hours, allowing criminals to use them for a scheme and dissolve them immediately. A specific type of shell company is the "shelf company," which was incorporated a long time ago and may already have a bank account. By purchasing such a shelf company, criminals can use it easily without disclosing any new information.
- **Inadequate AML/CFT Measures by Obliged Entities:** Corporate vehicles may also refrain from disclosing relationships with other entities, politically exposed persons (PEPs), or sanctioned individuals. It is up to the obliged entities (e.g., financial institutions, lawyers, accountants, and corporate service providers) to analyze and determine whether banking transactions, contracts, or other relationships (e.g., with PEPs or sanctioned persons, etc.) are suspicious, fake, or legitimate.

- **Provision of Services (Instead of Goods):** While all types of transactions may be falsified, it is easier to simulate the provision of services. Unlike the sale of goods—which requires production, storage, and many other requirements—providing services such as "consultancy services" may not require any special infrastructure. In this case, it may be difficult or even impossible for authorities or obliged entities to verify whether the service was actually delivered, or whether the value or price of the service seems reasonable.

1.3. Methods and Techniques Used by Criminals to Misuse Legal Persons and Legal Arrangements

This section describes the specific methods and techniques observed in the exploitation of the vulnerabilities outlined in the previous section. Although each element is described individually, it is likely that any money laundering or terrorist financing scheme will involve a combination of the following Typologies.

To classify these Typologies, they are presented based on their **location (where)**, the types of **institutional vehicles or elements used (what)**, and the **specific details of the scheme (how)**.

Where?

- **Use of Multiple Jurisdictions:** One of the most common methods is to spread the scheme across as many jurisdictions as possible. For example, the beneficial owners reside in Country A, the institutional vehicles are based in Countries B, C, and D, while the directors and shareholders (nominee individuals or institutional vehicles) are from Countries E and F. The assets are located in Country G (bank account) and Country H (real estate).
  The use of multiple jurisdictions serves various purposes, enabling criminals to exploit key vulnerabilities specific to each country.

What?

- **Companies – Shell Companies, Shelf Companies, and Front Companies:** According to the 2011 "Puppet Masters" report on major corruption cases, companies were the most commonly used vehicle. This is due to their widespread legitimate use, ease of incorporation, and the ability to abuse certain types of companies, such as:
  - **Shell Companies:** These can be created inexpensively, without the need for actual operations. Shell companies may have no assets, income, business activities, or employees, and can be established remotely to serve as directors or shareholders, to comply with ownership structures, or to simulate transactions such as loans or services. The FATF/Egmont report on concealment of beneficial ownership notes: "In cases involving shell companies, the majority were foreign-registered."
  - **Shelf Companies:** A category of shell companies, shelf companies are pre-registered entities with an existing bank account, credit history, and list of

directors. This makes them ready for use in a money laundering or terrorist financing scheme while maintaining a façade of legitimacy.

- **Front Companies:** Unlike shell companies, front companies conduct actual operations, employ staff, and generate revenue. They can be used to disguise or obscure the proceeds of crime or to justify income as part of money laundering or terrorist financing schemes. These companies often operate in cash-intensive sectors such as restaurants, dance clubs, hotels, casinos, and others.

- **Partnerships:** Although partnerships are less commonly used than companies for money laundering or terrorist financing purposes, they offer some privacy advantages. Partnerships—especially limited partnerships with general and limited partners—have more complex structures than shareholding companies. Limited partners benefit from a degree of anonymity due to their lack of involvement in day-to-day management, which may be exploited to conceal the identity of actual beneficiaries.
- **Trusts:** Although trusts are not as frequently used in money laundering and terrorist financing as companies, one interpretation suggests that their secrecy and efficiency are such that reports may underestimate their involvement due to authorities' limited resources for investigation or prosecution. According to the FATF/Egmont report on concealment of beneficial ownership, trusts are rarely used in isolation, but often in combination with companies. As trusts are legal arrangements and not legal persons, they cannot directly own assets in many cases—the trustee appears as the owner. Therefore, many trusts use a company to hold assets. Additionally, some parties to the trust may be entities (rather than natural persons), particularly the trustee. Many private investment funds use corporate trustees.
- **Private Interest Foundations:** These can be misused in financial crimes due to their "unfamiliar" structure within local legal frameworks. These foundations exist in some jurisdictions and resemble trust in structure. Countries unfamiliar with private interest foundations often treat them like public interest foundations or charities, thereby exempting them from registration or only requiring the registration of officials (rather than all parties such as founder, board members, beneficiaries, etc.).
- **Private Investment Funds:** These include hedge funds, which may not be subject to AML/CFT obligations. While they may be regulated for investor protection, they are not always subject to AML laws, especially in terms of identifying the beneficial owner. They offer a high degree of secrecy, as ownership interests may be so fragmented that no single investor exceeds the 25% or even 5% threshold.
- **Nominee Directors and Shareholders (Formal and Informal):** Criminals often use nominee directors and shareholders to create a legal façade concealing the identity of the beneficial owner. These nominees may be formal, appointed via notarized contracts, or informal, with their names used without clear legal documentation. In some cases, the nominee has no actual role in daily operations and merely receives correspondence or signs documents. In other cases, the nominee may be directly involved in money laundering or terrorist financing schemes or at least contribute to the intended opacity. The World Bank report *"The Puppet Masters"* notes that some service providers explicitly advertise nominee services to protect the secrecy of beneficial ownership,

with statements such as: "The sole purpose of the nominee service is to preserve the confidentiality of the beneficial owner. Its role is limited to company formation."

Strategies for using nominee individuals include:

- **Beneficial Owner's Tools to Control the Nominee Director:** As described in the article *"The Secret World of Fake Directors,"* the beneficial owner may ensure that nominee directors have no real control over the entity by requiring them to sign three preliminary documents:
  1. A waiver promising not to sue the beneficial owner.
  2. The power of attorney in favor of the beneficial owner to maintain control.
  3. A pre-signed undated resignation letter.
- **Multiple Nominees to Create False Audit Trails and Mislead Authorities:** Criminals and clients may use multiple nominee "gatekeepers" to act as shareholders or directors across various companies, misleading authorities into believing that these entities are unrelated, simply because they use the same professional nominee.
- **Nominee Beneficial Owner:** This is a more expensive service. Unlike regular nominees, who may appear to own many companies but cannot justify the legal source of funds, the "nominee beneficial owner" is a special service using a wealthy-looking individual with characteristics of a real beneficial owner to disguise the actual one and bypass red flags that would apply to regular nominees.
- **Informal Nominees – Deliberate Identity Fabrication and Victims:** In addition to informal nominees based on family ties, there are informal nominees with no relation to the actual owner who sell their identity information to third parties out of financial desperation. According to the FATF/Egmont report, "In a New Zealand case study, bank accounts belonging to students were used to receive funds from foreign accounts for real estate purchases. Another case (Case 77) showed how low-income individuals were manipulated into selling their identity information to professional money launderers, who then used them to form companies and open bank accounts."

- **Professional Intermediaries and Their Use in the Formation of Legal Persons and Legal Arrangements:** Professional intermediaries such as lawyers, accountants, and corporate service providers play a central role in establishing and managing legal persons and arrangements. In some cases, clients use them to implement complex structures that obscure the beneficial owner's identity without the intermediaries' full awareness of the purpose or nature of the activities. Their role may be limited to formalities such as document certification or incorporation services. However, poor due diligence or failure to report suspicious activity may render them indirect participants in money laundering or terrorist financing schemes, highlighting the need to strengthen oversight and professional accountability.

Strategies for exploiting professional intermediaries include:

- **Number of Professional Gatekeepers Employed:** A common method is to employ several nominee parties to eliminate suspicion or detection. According to the FATF/Egmont report, "Criminals may use the services of multiple professional intermediaries simultaneously, each playing a separate but essential role in the criminal scheme. Over one-third of the case studies supporting the report involved the use of more than one professional services sector, and a similar number involved multiple intermediaries from the same sector. This indicates that criminals likely avoid suspicion by not relying on a single professional party—often using more than one lawyer or accountant."
- **Involvement by Profession – Lawyers vs. Accountants:** According to the FATF/Egmont report, the degree of involvement and attitude varies from collusion to willful blindness among lawyers and accountants: "Approximately one-third of the cases were assessed to involve a complicit professional intermediary. In many of these, the intermediary was found to have designed and promoted the scheme themselves (often as a tax avoidance strategy). Of the three professional sectors assessed, accountants were more likely to be complicit in schemes to conceal beneficial ownership. Furthermore, accounting and legal professionals were more likely to be the architects of the scheme, not merely complicit facilitators in a client-designed plan. Compared to accountants, legal professionals were more prone to either direct involvement or willful blindness.

- **Bearer Shares:** Although bearer shares (new issuances) are banned in most countries, older companies with existing bearer shares may still allow any holder to be considered a beneficial owner, making it extremely difficult for authorities to determine the current owner. One common strategy involves a nominee party incorporating a company (appearing as the initial subscriber), but the shares are actually owned by someone else and then transferred to the real beneficial owner.

How?

A) Concealing or Falsifying the Owner

- **Complex ownership or control structures:** The main strategy aimed at achieving opacity is the creation of an extremely complex structure, whether in terms of the length of the ownership chain leading to the beneficial owner or the geographic breadth (see above: "Use of multiple jurisdictions"). In addition, combining the most opaque elements—such as nominee parties, bearer shares, and unfamiliar types of legal tools—ensures difficulty in identifying beneficial owners, as competent authorities need substantial resources to uncover the full ownership structure and confirm the controlling and owning parties at each layer. According to the FATF/Egmont report on concealment of beneficial ownership: "More than half of the case studies supporting this report involve the use of complex ownership structures, where control is affected by a mix of direct and indirect control."
- **Foreign ownership:** Regardless of the complexity of the layer, foreign ownership of institutional vehicles results in decreased interest from local authorities in investigating

them (e.g., due to difficulties in applying domestic laws or because the non-resident criminal is not subject to local prosecution), especially if the crime is unrelated to the country (e.g., tax evasion that affects a foreign country rather than the country of incorporation). Moreover, foreign ownership means authorities have fewer resources to verify personal details (name, date of birth, address, etc.), particularly if the person is not resident or does not have dealings in the jurisdiction.

- **Control without ownership – power of attorney, contracts, and financial instruments:** Although most definitions of the beneficial owner cover ownership and control elements (e.g., holding more than 25% of shares or controlling them through other means), it is difficult to prove or verify "control through other means." As a result, in most cases, only individuals owning more than 25% of shares are identified, enabling others to avoid registration as beneficial owners—even while controlling the entity or its assets (e.g., the bank account)—by using the power of attorney to manage the entity or its assets. Similar cases include secret contracts or cumulative voting rights, along with convertible shares or financial instruments (such as stock options) to retain control over the company without owning any shares.
- **Fake identities:** The use of virtual and remote services to establish companies and open bank accounts, combined with poor awareness or implementation of AML/CFT obligations by obliged entities, allows criminals to use fake identity documents to conceal their true identity or avoid direct prosecution. For example, traffickers in Paraguay used real identities (of deceased persons) but altered the photo.
- **Misuse of professional secrecy:**
  Corporate service providers—particularly lawyers—may abuse professional secrecy, such as attorney-client privilege, to facilitate money laundering and terrorist financing without submitting suspicious transaction reports or disclosing their clients' identities to authorities.

B) Concealing or Falsifying Transactions and Income

- **Entities with misleading names:**
  Entities can be created under any name, allowing criminals to establish shell companies with names resembling legitimate entities (e.g., "Mitta" instead of "Meta") to simulate transactions with legitimate companies.
- **Fake transactions—especially involving services (such as loans and false invoices):**
  Contracts are generally not registered, and it is nearly impossible to verify the delivery of services such as consultancy. In this way, criminals can establish multiple entities to engage in fake transactions such as:
    - **Fake invoices:** Fake invoices allow legitimate entities to evade taxes (by artificially reducing their taxable income through fictitious expenses). Fake invoices can also serve the same purpose as fake loans (see below).
    - **Fake loans:** Loans that are never intended to be repaid can be used to justify the transfer of funds. In many cases, shell companies transfer funds among themselves (minus a small fee) or divide the amounts to reduce suspicion and

then withdraw the funds from the last layer or return them to the origin as seemingly legitimate income.

- **Disguising transfers as legitimate salaries:** Front companies can be used to pay salaries that appear legitimate to individuals who are not actual employees of the company but who receive payments as part of drug trafficking operations.
- **Use of lawyers' trust accounts or client accounts:** Accountants may hold bank accounts that pool client funds for legal fees or other obligations owed to third parties. Criminals may use such accounts held by lawyers—either complicit or unaware—for laundering. For example, in one case, a company affiliated with a criminal entered into a contract with a lawyer and transferred funds to him for a pending legal case. Shortly thereafter, the company claimed to have reached a settlement with the opposing party and requested that the lawyer return the funds to a different bank account.

1.4. Risk Indicators for the Misuse of Legal Persons and Legal Arrangements

The methods described above for exploiting vulnerabilities often leave traces that can be tracked by authorities. Based on the risk indicators identified in the FATF/Egmont report on the concealment of beneficial ownership, the following is a list of risk indicators or red flags that authorities can monitor to assess whether further investigation is warranted concerning a corporate vehicle to ensure it is not involved in money laundering or terrorist financing.

A. Country Risks

Country-related red flags refer to a foreign corporate vehicle operating or holding assets in the domestic country, or to a foreign company with direct interests in a domestic entity or being part of an ownership chain of a domestic entity. They also refer to the location of shareholders, beneficial owners, nominees, and directors of the corporate vehicle. The indicators include:

- A foreign country listed on the FATF grey or blacklist.
- A foreign country with low ratings, particularly on FATF Recommendations 10, 22, 24, and 25, and Immediate Outcomes 4 and 5.
- A foreign country with low ratings in peer review reports by the Global Forum on Transparency and Exchange of Information.
- A foreign country mentioned in tax haven lists / national or regional lists of non-cooperative jurisdictions.
- A foreign country listed by civil society organizations (e.g., Basel AML Index, Financial Secrecy Index, Corruption Perceptions Index).
- A foreign country with low levels of transparency (e.g., no beneficial ownership registration, failure to update information).
- A foreign country that has no information exchange agreement with the local country.
- A foreign country that imposes little or no income tax.

B. Ownership and Control Structure and Other Corporate Vehicle Details

- Use of multiple jurisdictions, where the place of incorporation, location of assets, business operations, and residence of beneficial owners and directors are all in different jurisdictions (especially when some are high-risk countries per section A).
- Complex ownership structures, especially when they appear disproportionately complex given the type of business, sector, number of employees, or declared income.
- The combination of legal persons and legal arrangements (e.g., a trust settlor, trustee, or beneficiary is a company).
- Long ownership chains (multiple layers up to the beneficial owner), especially when appearing unusually complex for the business type, sector, number of employees, or declared income.
- Use of trusts, especially discretionary trusts.
- Use of "unfamiliar" entities not covered by local legal frameworks, such as private interest foundations, Anstalten, holding insurance companies, etc.
- Use of shell companies :
    - Long period of inactivity after incorporation, followed by a sudden, unexplained increase in financial activity.
    - cannot be found on the internet or social media (e.g., LinkedIn).
    - The address refers to a P.O. box.
    - No employees and no tax registration.
    - No electricity, gas, or water consumption (indicating no actual business activity).
- Entity with an unusually high number of beneficial owners (to obscure the actual beneficial owner) or with many shareholders just below the threshold (e.g., 24.9% if the minimum threshold is 25%).
- Entity that grants the power of attorney to unrelated individuals for managing the company or its assets (e.g., bank accounts).
- Inconsistency between the entity's name and its activity (e.g., "United Agricultural Company" supposedly selling furniture) or mimicking the names of well-known companies.
- Registered at an address shared with hundreds of other entities.
- Engaging many professional parties (lawyers, accountants) without a clear reason.
- Frequent and illogical changes in address, directors, or beneficial owners.

C. Beneficial Owner, Director, or Shareholder Details

- A local or foreign person posing risks, or their family members or associates.
- Listed on a sanctions list, or convicted of fraud, tax evasion, money laundering, or included in a disqualified directors or barred professionals list, etc.
- Non-resident (especially if residing in a high-risk country as defined in section A).
- Possible involvement of nominee individuals:
    - Owning, controlling, or managing an unusually high number of entities.
    - Economic profile inconsistent with the number of companies owned/managed (e.g., low-income persons or social welfare recipients appearing to own highly profitable companies).

  - Age inconsistency of the shareholder or director (e.g., one or two years old, or over 80 years old).
  - Inconsistent profile (e.g., an art student managing a fintech company).
  - Employee of a law or accounting firm.
- The address cannot be located on Google Maps.
- Address is used by a large number of companies at the same time.
- Inconsistent lifestyle and assets with declared income.
- Beneficiaries of the trust have no clear relation to the settlor (e.g., not from the same family).
- Shareholders granting power of attorney to a family member with justifications focused on tax minimization strategies.

D. Transactions, Assets, and Income

- Transactions are economically irrational (e.g., circular transactions) or inconsistent with the company profile.
- Continuous fund transfers to high-risk countries listed in section A.
- High-value transactions involving a small number of recipients.
- Transactions with offshore companies without justification (e.g., a small pizza shop doing business with offshore entities).
- Receiving large sums of money which are spent, transferred, or withdrawn shortly thereafter without commercial justification, thus maintaining a near-zero bank balance despite frequent incoming and outgoing flows.
- The number and location of bank accounts is inconsistent with the company's profile.
- Company credit cards or bank accounts appear to be used for personal expenses.
- Transfers occur between companies that share the same directors, shareholders, or beneficial owners.
- Most company funding comes from non-repayable loans or suspicious sources.

1.5. FATF Standards on Preventing the Misuse of LP & LA

▪ FATF Standards

Between 2022 and 2023, the Financial Action Task Force (FATF) amended Recommendations 24 (Transparency and Beneficial Ownership of Legal Persons) and 25 (Transparency and Beneficial Ownership of Legal Arrangements). In summary, in the case of legal persons, the amended Recommendation 24 requires countries to:

- Apply a risk-based approach and consider the risks posed by legal persons incorporated in the country and foreign legal persons with sufficient links to the country (this includes identifying and describing the various types and core features of legal persons in the country, defining and describing their creation processes, collecting and registering basic and beneficial ownership information, and making this information publicly available).
- Ensure that accurate, adequate, and up-to-date beneficial ownership information and control structures of legal persons are available and accessible in a timely and efficient

manner to competent authorities. (The amendments to Recommendation 24 explicitly require countries to use a multi-pronged approach, relying on a combination of different mechanisms to collect beneficial ownership information to ensure its accuracy, adequacy, and timely accessibility, including for foreign legal persons with sufficient links to the country that may pose ML/TF risks).

- Prohibit the issuance of new bearer shares or bearer share warrants and take appropriate measures to prevent misuse of existing ones (e.g., by requiring conversion or immobilization and identification of owners prior to exercising rights).
- Implement effective measures to prevent the misuse of nominee shareholders and directors for money laundering and terrorist financing purposes, by either prohibiting or requiring disclosure of the nominee status and the identity of the nominator and/or requiring licensing.
- Consider facilitating access to beneficial ownership and control information by financial institutions and DNFBPs in line with Recommendations 10 to 22.
- Establish effective, proportionate, and dissuasive sanctions to enforce compliance.
- Ensure maximum international cooperation regarding basic and beneficial ownership information.

In the case of legal arrangements, the amended Recommendation 25 requires countries to:

- Assess risks related to domestic legal arrangements, including those administered in the country or where the trustee (or equivalent) resides in the country and has sufficient links. Countries must identify and describe the types of legal arrangements subject to local law, the creation of mechanisms, the collection of basic and beneficial ownership information, and ensure such information is publicly accessible.
- Ensure that resident trustees hold and provide competent authorities with adequate, accurate, and up-to-date information on express trusts and similar legal arrangements, including information on the settler(s), trustee(s), protector(s) (if any), beneficiary(ies), and other natural persons exercising ultimate effective control over the trust. This includes both basic and beneficial ownership information where any of the parties are legal persons. Competent authorities must be able to access this information in a timely and efficient manner, such as through a central register or from other authorities (e.g., tax authorities), DNFBPs, or other sources.
- Require trustees to disclose their status when dealing with financial institutions and DNFBPs.
- Consider facilitating access to beneficial ownership and control information by financial institutions and DNFBPs, per Recommendations 10 to 22.
- Establish effective, proportionate, and dissuasive sanctions to enforce compliance.
- Ensure maximum international cooperation regarding basic and beneficial ownership information.

▪ Recommendations

According to the 2023 FATF Guidance on Beneficial Ownership for Legal Persons and other published materials (including those issued by civil society organizations), the following is a

list of recommendations and best practices that countries should implement to comply with FATF standards and address vulnerabilities affecting corporate vehicles.

Threats

- **Comprehensive risk assessment:** Conduct a comprehensive risk assessment of all types of legal persons (including foreign entities with links to the country), based on registration statistics, suspicious transaction reports, enforcement reports, company service providers' disclosures, and consultation with the private sector, experts, and civil society.
- **Intensify cooperation and expand local data sharing and information exchange:** To detect emerging threat scenarios and develop risk mitigation measures.
- **Enhance international cooperation and exchange of information with foreign countries:** Given that the most complex ML/TF schemes are global in nature, establishing international cooperation and information exchange mechanisms helps address ML/TF risks.
- **Establish risk mitigation measures:** These may include additional disclosure requirements, enhance investigative and enforcement capacities, and requiring the presence of a local natural person responsible for any domestic or foreign legal vehicle.

Vulnerabilities

A) Availability of Beneficial Ownership Information

- **Comprehensive basic information:** Ensure the availability of basic information on corporate vehicles (such as company type, list of legal owners and directors, and the full ownership chain).
- **Multi-source approach to beneficial ownership information:** In addition to having a register or an equally effective mechanism, ensure that various sources collect and provide legal and beneficial ownership information (e.g., tax authorities, commercial registry, land registry, obliged entities, securities markets, etc.).
- **Legal framework consistency:** Where multiple legal frameworks exist for collecting beneficial ownership information (e.g., a legal framework in each province or free zone), or where the beneficial ownership register and obliged entities collect such information, ensure they are all subject to the same legal requirements, such as definition of beneficial owner and ownership thresholds.
- **Comprehensive scope:** Ensure that all types of legal vehicles are subject to beneficial ownership information requirements. Avoid or minimize exemptions to prevent loopholes. Acceptable exemptions may be based on duplication (e.g., another authority like the stock exchange already holds the same beneficial information on ownership).
- **Comprehensive definition of beneficial owner:** Ensure the definition captures multiple elements (e.g., control, ownership, benefits), and that thresholds are as low as possible, at least based on risk (e.g., lower thresholds for high-risk sectors like extractives or procurement, or when a risk-exposed person has interests in the company). Define examples of control through other means (e.g., voting rights, veto

rights, power of attorney, right to appoint or remove directors), and also control without ownership, such as through financial instruments (e.g., convertible shares). For example, the U.S. legal framework for beneficial ownership includes financial instruments as a form of ownership interest.

- **Comprehensive definition of beneficial ownership in complex legal arrangements:** Ensure the identification of all parties to the trust or similar legal arrangement (or private interest foundation) and set specific rules when any of the parties are legal persons, such as institutional trusts, to clarify which parties should be identified as beneficial owners. For example, some countries apply the general beneficial ownership rules for companies to institutional trusts.
- **Alternative approach for identifying beneficial owners of unfamiliar entity types:** Allow flexibility in applying specific rules to special types of entities (e.g., partnerships, companies limited by guarantee, Anstalt, discretionary trusts, holding insurance companies, private interest foundations, etc.), instead of applying a uniform beneficial ownership definition which may not suit certain foreign entities.
- **Complex ownership structures:** Assess and monitor complex ownership structures by identifying risk based on ownership chain length and the risk level of each jurisdiction involved. Review ownership structures of legal vehicles to identify anomalies (e.g., structures disproportionately complex for the entity type, sector, size, or income). For example, Trans-crime analyzes European company ownership structures and associated risks.
- **Shell and dormant companies:** Remove inactive or non-functional entities from the register and monitor low-activity entities with limited transactions that may indicate a shell or paper company.
- **Bearer shares:** Prohibit bearer shares not only for domestic legal vehicles but across the entire ownership structure of such vehicles.
- **Nominees:** Either prohibit nominees or require them to be licensed and assess nominee risks by analyzing the number of entities owned or controlled by the same persons, use of P.O. boxes, or inconsistencies between profile and purported directors or beneficial owners. For example, the Tax Justice Network recommends a "constitutive effect" upon registration (i.e., rights are created only upon registration, making the nominee the legal owner by law, thus deterring beneficial owners from hiding behind nominees due to their legal authority to override the true owner).
- **Effective sanctions:**
  To promote compliance, impose dissuasive sanctions, such as prohibiting non-compliant entities from public procurement or engaging with obliged entities. Restrictions could include barring such companies from amending contracts or ownership structures, filing financial statements, or renewing leases in free zones, until they update their beneficial ownership data. For instance, North Macedonia prohibits financial institutions from dealing with companies that fail to disclose their beneficial owners, prompting banks to encourage clients to register their beneficial owners in the official register. Moreover, measures should target non-compliant shareholders, such as restricting voting rights, withholding dividends, or directly cancelling shares.

B) Possession of Beneficial Ownership Information

- **Centralization of legal and beneficial ownership information:** Establish a register (administered by the most appropriate government authority, such as the commercial registry, tax authority, or a newly created beneficial ownership register) to hold (or centralize through inter-agency linking) legal and beneficial ownership information for all types of legal vehicles. This step enables cross-checking to prevent discrepancies (e.g., if Company "A" discloses that its beneficial owner is "John" through Company "B," but Company "B" declares "Mary" as the shareholder and beneficial owner).
- **Compliance of obliged entities with AML/CFT requirements:**Ensure that obliged entities (e.g., financial institutions and DNFBPs) operate under an appropriate legal framework (without loopholes), including awareness campaigns and training on AML/CFT requirements, regular audits, and dissuasive sanctions for non-compliance. Audits can include monitoring public disclosures and conducting "mystery shopper" operations as suggested in the World Bank's *"The Puppet Masters"* report. Additionally, monitor the submission of STRs (seeking outliers) and provide training and feedback on the quality and use of such reports.

C) Accuracy of Beneficial Ownership Information

- **Verification and automated cross-checking mechanisms:**Establish automated validation protocols to prevent the submission of incorrect data when incorporating companies (e.g., mandatory fields like "name") and implement cross-checking mechanisms to ensure consistency of registered information (e.g., verifying that the tax ID matches the person, or whether the person is still alive according to the civil registry). According to FATF's 2019 *Best Practices on Beneficial Ownership*, Denmark, Belgium, and Austria have sophisticated verification systems.
- **Red flags based on economic profile:**Various authorities, especially tax administrations, can assist in verification by setting red flags based on individuals' economic information. For example, a red flag might be raised on someone who fails to declare income or assets but appears to own highly profitable companies. Austria uses its tax authority to validate beneficial ownership data within the beneficial ownership register.
- **Mandatory discrepancy reporting:**The more entities with access to the information (see below), the more accurate the information becomes, by requiring them to report discrepancies (e.g., the client discloses that John is the beneficial owner, but the register shows Mary).
- **Requiring a local obliged entity to validate the information:**Following the Slovakia model, require a local obliged entity (e.g., a bank, lawyer, etc.) to verify and assume responsibility for confirming the accuracy of the beneficial ownership data before registration. This includes providing analysis, evidence, and confirmation to support those granted access to the beneficial ownership register.
- **Enhanced verification for virtual/online company service providers:**Where entities are formed via virtual service providers, require enhanced due diligence including video

identification, submission of original documents, and document validity verification to prevent the use of fake identities.

- **Confirmation of authorization – contacting the local beneficial owner or director:**At a minimum, for local beneficial owners and directors, countries can contact them using official contact information to confirm that they are aware of their listing as directors or beneficial owners of the entity, thereby preventing identity theft. Alternatively, countries can allow individuals to check whether their name has been used in the beneficial ownership register with proper authorization.
- **Address confirmation:**To verify an address, preliminary checks—electronic or automated—may include confirming that the address exists (e.g., via Google Maps) and refers to a credible structure (not a government building). For example, the Argentine tax authority sends a code via post to the declared address, and the taxpayer must confirm accuracy by submitting the code received.

D) Access to Beneficial Ownership Information

- **Ensure broad access to information:**Maximize access to information for all legally authorized stakeholders, such as domestic and foreign competent authorities, obliged entities, legitimate interest stakeholders, or the general public (or assess, in line with the European Court of Justice's ruling, whether investigative journalists and civil society organizations involved in ML/TF monitoring have a legitimate interest). Many countries offer free online public access, including the UK, Ukraine, Ecuador, Denmark, Latvia, Serbia, and others, some requiring a small access fee.
- **Searchability and relationship mapping:**Enable searches through the greatest possible number of fields (e.g., entity name, beneficial owner name, address, country of residence, etc.) and allow the system to map all relationships (e.g., all entities owned or controlled by the same beneficial owner, and those sharing the same address or directors).
- **Leverage external data sources to verify beneficial ownership, including:**
    - *Forbes Global 2000 List:* http://www.forbes.com/global2000/list/#search
    - *BO Registers of other countries:*
        - UK: https://beta.companieshouse.gov.uk/
        - Poland: http://krs.infoveriti.pl/index.html
        - Czech Republic: https://rejstriky.finance.cz, https://rejstrik.penize.cz
        - Cyprus: https://efiling.drcor.mcit.gov.cy, http://cy-check.com
        - Non-profit databases: e.g., Charity Commission, Jordan Companies Control Department, registries in other countries
        - http://www.guidestar.org/Home.aspx
    - *FBI Most Wanted:* https://www.fbi.gov/wanted/topten
    - *Private company databases:* http://orbisdirectory.bvdinfo.com/OrbisDirectory/Companies
    - https://www.importgenius.com/search
    - *Offshore Leaks Database:* https://offshoreleaks.icij.org/
    - *Commercial data providers:*

  - World-Check: https://www.world-check.com/frontend/logout
  - Thomson Reuters Risk: https://risk.thomsonreuters.com
  - LexisNexis: http://www.lexisnexis.com
  - Dow Jones: http://www.dowjones.com
  - Factiva: https://professional.dowjones.com/factiva
  - Accuity Global PEP: http://www.accuity.com
  - Other databases, watchlists, or search engines.
- **Professional secrecy:**Ensure that the AML/CFT framework covers all DNFBPs, including lawyers, and requires them to submit STRs or respond to information requests concerning their role as company service providers. It should also regulate or define the scope of attorney-client privilege or other professional secrecy conditions relating to legal persons' service providers.

E) Assets and Income from Institutional Mechanisms

- **Registers of beneficial owners' assets:**Create asset registers (e.g., real estate, vehicles), or require third-party reporting (e.g., auction houses and insurers reporting on the ownership of artwork). These registers should collect beneficial ownership data and pricing information. Alternatively, asset registers may collect legal ownership and price data only, which can then be cross-referenced with the beneficial ownership register to identify the beneficial owner of the asset. Competent authorities must have access to the beneficial ownership information of such assets.

Chapter Two: Trends and Methods of Misuse of Legal Persons and Legal Arrangements in the

Region – Analysis of Questionnaires and Case Studies

2.1. Overview

This chapter analyzes the information and data collected from a questionnaire distributed to the member countries of the Middle East and North Africa Financial Action Task Force (MENAFATF). The aim was to understand how these entities and legal structures are misused in illicit activities, thereby paving the way for proposing regulatory solutions and recommendations to mitigate these risks. Sixteen out of twenty-one countries responded. This analysis aims to provide a comprehensive overview of the legal forms of legal persons and legal arrangements in the region, in addition to assessing the risks associated with them, particularly in relation to money laundering and terrorist financing.

First. Legal Persons in the Region

✓ Classifications and Economic Roles

The data indicate that several main types of legal persons are recognized and legally available in most of the countries participating in the study. Commercial companies are the most common form, with 58% of responding countries reporting the availability of limited liability companies within their legal frameworks, followed by partnerships (such as general partnerships, limited partnerships, and partnerships limited by shares) at 52%, and joint-stock companies at 49%. Furthermore, 45% of countries reported the existence of branches of foreign companies, 40% reported companies in free zones, and 30% reported the existence of holding

companies among their recognized legal forms. Additionally, 35% of countries stated that they have state-owned or mixed-ownership companies within their legal framework.

Besides commercial companies, non-profit entities constitute an important component of the legal and economic framework of the region. According to participating country data, 38% reported the existence of cooperative associations among the recognized legal forms of legal persons, while 55% indicated recognition of non-profit organizations with cultural, social, sports, professional, charitable, and environmental purposes as part of their approved legal systems.

In terms of economic activities and relevant sectors, commercial companies play a central role in international trade, real estate, and financial investment. Conversely, non-profit organizations focus on social development, charitable work, education, and health.

✓ Risk Assessment Associated with Legal Persons

Participating countries in the study assessed the risks related to money laundering and terrorist financing associated with legal persons.

With regard to money laundering risks, 35% of participating countries rated these risks as low, while 45% rated them as medium, and 20% rated them as high—especially in companies involved in international trade activities. The data indicate that commercial companies with complex ownership structures, particularly those registered in free zones, are the most vulnerable to misuse in money laundering schemes.

As for terrorist financing risks, the majority of participating countries (60%) rated these risks as low, while 30% rated them as medium, and 10% rated them as high, particularly in the non-profit organization sector.

Second. Legal Arrangements in the Region

✓ Types and Uses

In addition to legal persons, legal arrangements form a core part of the economic and legal infrastructure in the participating countries. Data show that trusts are available in 40% of countries, while waqf (charitable endowments) are more prevalent, being available in 65% of countries. Private legal arrangements, such as dual legal structures, are less common, with a prevalence of only 20%.

These legal arrangements play multiple roles in different fields. Trusts are used for asset and investment management, while waqf focuses on charitable, educational, and religious activities. On the other hand, private legal arrangements are used for tax planning and estate management.

✓ Risk Assessment Associated with Legal Arrangements

Participating countries in the study assessed the risks related to money laundering and terrorist financing associated with legal arrangements.

Regarding money laundering risks, 50% of the participating countries rated these risks as low, 35% rated them as medium, and 15% rated them as high—particularly in countries that permit the establishment of legal arrangements.

As for terrorist financing risks, 70% of participating countries rated these risks as low, 20% as medium, and 10% as high—especially in certain trusts and waqf. The data indicate that undeclared trusts and waqf not subject to disclosure requirements due to their exclusion from the legal definition of arrangements are the most vulnerable to misuse in terrorist financing.

2.2. Description of Cases of Misuse of Legal Persons and Legal Arrangements in the MENA Region

This section presents a descriptive analysis of 30 case studies submitted by 14 out of 16 responding member countries (Annexed). This part provides a detailed and practical quantitative depiction from the field level, based on these thirty cases, by determining detailed statistics regarding predicate offenses, the economic sectors misused, the stages of money laundering (placement, layering, integration), and terrorist financing (collection, transfer, use). This analysis follows a structured framework that combines both objective and analytical descriptions to enhance a more integrated understanding of contemporary patterns and practices in financial crimes.

2.2.1. Objective Description

The thirty presented cases revealed a broad and sophisticated range of methods used in financial crimes across multiple jurisdictions. They included complex schemes involving money laundering, terrorist financing, tax evasion, fraud, corruption, and the misuse of companies and legal entities.

Several money laundering cases involved investment fraud schemes, particularly in the real estate sector, where offenders established companies that falsely claimed to be implementing profitable projects to attract a large number of investors, only to embezzle the funds for personal use. These schemes typically relied on multi-layered corporate structures and misleading marketing practices to conceal the absence of actual business activity.

Other cases uncovered the extensive use of shell companies for money laundering purposes, where entities that appeared legitimate were used as fronts for channeling and laundering money through complex networks of bank accounts, international transfers, and fictitious companies. Techniques such as using dormant accounts, forged invoices, fake financial records, and nominal ownership structures were frequently observed, significantly hindering oversight and monitoring by competent authorities.

The misuse of legal persons was particularly evident in the use of complex ownership structures, often established in free trade zones or jurisdictions with low regulatory oversight, to conceal the identity of beneficial owners and obscure the flow of illicit funds.

In terrorist financing cases, similar methods appeared, with specific features aimed at supporting terrorist entities. Entities such as import-export companies were used as fronts to receive and redistribute funds from high-risk jurisdictions, with minimal or no actual business operations, and the use of informal financial channels such as hawala to avoid detection.

The cases also highlighted the importance of cooperation and coordination between domestic and international authorities. Financial Intelligence Units (FIUs) and supervisory bodies played a key role in uncovering these complex schemes. Advanced investigative

techniques—such as digital financial analysis, IP address tracking, and detailed financial auditing—were instrumental in dismantling criminal networks.

Technological loopholes, especially in the fintech sector, were clearly exploited in several cases. Criminals used digital financial services and regulatory gaps to execute rapid and anonymous transactions. Authorities in these cases recommended legislative enhancements, stricter controls, and the imposition of more rigorous standards to prevent the exploitation of such gaps.

The cases consistently emphasized the serious deficiencies in corporate transparency, including the misuse of outdated or unupdated commercial registries and the lack of clarity on beneficial ownership, which greatly facilitated the abuse by criminals in hiding illicit financial flows and evading legal accountability.

Regulatory responses to these cases were comprehensive and multi-dimensional, including asset freezes, account suspensions, international cooperation for asset recovery, and the prosecution of those involved. These actions were coupled with recommendations to strengthen legislation and oversight. The measures combined criminal prosecutions for fraud, money laundering, and terrorist financing with administrative sanctions and recommendations to enhance transparency.

In sum, these thirty cases illustrate the substantial risks posed by complex financial crime networks exploiting legal structures, technological tools, and regulatory loopholes across jurisdictions. They clearly underscore the need to strengthen international cooperation, develop legal frameworks, and impose strict financial transparency standards to effectively combat such financial crimes.

2.2.2. Analytical Description

It should be noted that what is presented here represents only an analytical description of the cases and should not be considered a final conclusion. The final results and conclusions of the study will be based on a comprehensive analysis that combines the findings of these cases with the independently analyzed results of the distributed questionnaires. Accordingly, the observations provided here aim to offer a preliminary understanding of the recurring patterns and behaviors in the received cases, which will later be deepened through integration with the survey data to achieve scientifically and practically accurate conclusions.

It was observed from this analytical description that all the studied cases (100%) involved the misuse of legal persons and did not include any case related to the misuse of legal arrangements, which reflects a clear tendency to misuse legal persons for concealing illicit financial activities.

Inactive companies such as shell companies or shelf companies (non-updated) were the most misused type of legal person at a rate of 27%, followed by officially registered import and export companies at 10%, and then joint-stock companies and sole proprietorships at approximately 7% each.

Regarding the nature of the crime, most cases (57%) were related to money laundering only, while a significant proportion (43%) involved both money laundering and terrorism financing, indicating a strong overlap in the use of companies with the aforementioned

characteristics to carry out these two crimes, particularly in sectors such as diverse commercial activities, import and export, and financial services.

From a sectoral perspective, the import and export sector emerged as the most exposed to money laundering and terrorism financing crimes at 23%, with most of these cases clearly involving both crimes, indicating the misuse of this sector to move funds and obscure their true origin with ease. The real estate sector appeared at 13%, with most of its cases linked to money laundering only, through the misuse of real estate entities in large-scale financial fraud operations, highlighting the sector's attractiveness for hiding funds and creating a façade of legitimacy. A 10% share was recorded in the diverse commercial activities sector, which included both money laundering and terrorism financing cases, indicating this sector's vulnerability to financial manipulation due to the broad scope of its activities. Financial and banking services sectors were targeted in 17% of the cases, with a clear connection to both money laundering and terrorism financing.

The cases showed significant variation in the sectors used at each stage of money laundering. In the placement stage, the import and export sector was the primary entry point at nearly 30%, followed by diverse commercial activities and financial services sectors at about 20% each, and the real estate sector at approximately 17%, owing to the ease of injecting cash or conducting large transfers through these sectors without raising suspicion. In the layering stage, the financial services and banking sector topped the list at about 27%, due to heavy reliance on repeated and complex transfers between accounts and companies to obscure the origin of funds, alongside the import and export sector at around 23%, owing to the use of fictitious invoices and contracts as an effective concealment tool. In the integration stage, the real estate sector was clearly at the forefront with a rate of about 33%, due to the ease of purchasing luxury real estate assets which allows the reintegration of laundered money into the formal economy, while the diverse commercial activities and import/export sectors followed closely at around 20%, reflecting the relative ease of integrating funds through seemingly legitimate business operations.

As for the stages of terrorism financing, different sectors were targeted. In the collection stage, diverse commercial activities and import ranked first at about 35%, due to the ease of collecting funds from external sources through entities that appear legal and commercial. In the transfer stage, the banking and financial services sectors were the most utilized, at about 40%, with terrorists relying on bank transfers and informal remittance systems to move funds across borders. In the usage stage, the primary sectors were diverse commercial activities and service sectors, as well as direct cash distribution at approximately 30%, used to distribute funds to individuals and entities linked to terrorist organizations.

It was clearly shown that the layering stage is the most utilized and complex in money laundering operations, with 100% of money laundering cases involving complex layering, indicating a heavy focus on concealing financial flows. On the other hand, the transfer stage was the most prominent in terrorism financing, involved in 85% of the studied cases, underscoring the critical need to intensify oversight over money transfer systems, both formal and informal such as hawala, to reduce terrorist organizations' ability to receive and use funds.

Regarding the methods and trends observed, several clear patterns emerged related to money laundering and terrorism financing. For money laundering, the most common method

was reliance on shell or inactive companies as legal fronts for transferring funds, appearing in about 30% of the total cases studied. This was followed by the use of complex ownership structures and multilayered companies to conceal the identity of the beneficial owner at 23%. Other techniques included transferring funds through non-updated or inactive bank accounts (17%), misusing legally established companies in fictitious or fraudulent activities, especially in the real estate sector (13%), using fake invoices and contracts to justify financial transfers (10%), and lastly, reliance on informal remittance networks such as the hawala system at 7%.

Regarding the predicate offenses associated with these money laundering operations, financial fraud and scams, especially in the real estate and investment sectors, constituted the highest percentage at 27%, followed by receiving and transferring funds from unknown or suspicious sources without any actual economic activity, suspected to be linked to terrorist or prohibited activities, at 20%. Tax evasion through fake invoices and manipulation of financial records appeared at 17%. Lower percentages were observed for political corruption and abuse of influence (10%), terrorism financing as a predicate offense (10%), illegal currency trading (7%), and dishonesty in providing financial and investment services (6%). A small percentage of predicate offenses were not clearly identified, at 3%. Therefore, the most common predicate offenses for money laundering are financial fraud, followed by receipt of suspicious funds, and tax evasion.

On the other hand, the cases revealed the main patterns of terrorism financing operations, where the most used method was the misuse of legally registered legal persons with no actual economic activity, used to transfer funds to terrorist entities, at 31%. Another method involved receiving financial transfers from foreign sources in high-risk countries and redistributing them domestically to prohibited groups at 25%. The use of legal entities operating in the import and export sector to obscure the true purpose of the transfers appeared at 19%. Unlicensed exchange companies and informal remittance systems were used to transfer funds to terrorism-linked entities at 13%, while cash was distributed in an untraceable manner within the country at 12%.

Based on this analysis, it is clear that the misuse of shell or inactive companies is the dominant pattern in money laundering operations, while reliance on legally registered companies with no real economic activity constitutes the most used pattern in terrorism financing operations.

2.3. Analysis of the Main Techniques and Methods for the Misuse of Legal Persons and Legal Arrangements in the MENA Region

In this section and based on the responses of sixteen member countries from the region, we present a dual reading of the data obtained from the region's countries, by providing a comprehensive strategic reading of internal and external threats, and vulnerabilities that represent an enabling environment for the misuse of legal persons and legal arrangements. Then, we present a qualitative analytical reading based on the classification of the most prominent techniques and patterns observed in money laundering (ML) and terrorism financing (TF) through legal persons and legal arrangements in the Middle East and North Africa region.

We present a deep analysis of the threats related to money laundering (ML) and terrorism financing (TF) and the vulnerabilities related to legal persons and legal arrangements

as a fundamental step to understanding how these threats use vulnerabilities as tools for committing financial crimes, which in reality take the form of misuse techniques and patterns. This is followed by an analytical presentation of the classification of methods, patterns, and Typologies used in money laundering (ML) and terrorism financing (TF) through legal persons and legal arrangements.

2.3.1. Classification of Threats Related to the Misuse of Legal Persons and Legal Arrangements in ML/TF

Before proceeding to the analysis of the techniques and methods used in the misuse of legal persons and legal arrangements, it is necessary first to understand the threats and vulnerabilities associated with them. Evaluating the nature of these risks forms the basis for understanding how legal structures are used as tools for money laundering and terrorism financing. Accordingly, this chapter provides a detailed analysis of the main threats in the region and the key vulnerabilities exploited in both legal persons and legal arrangements, highlighting the methods used by illicit actors in this context.

Based on the responses of the participating countries, the threats related to ML/TF in the Middle East and North Africa region can be classified according to specific domains, where the percentage of each type of threat was identified, reflecting their prevalence and relative significance.

- ✓ **ML Threats Related to the Misuse of Legal Persons and Legal Arrangements**

The extracted data indicates that tax crimes, including tax evasion and tax fraud, constitute the most widespread threat for ML through the misuse of legal persons, as 45% of countries reported a strong association between such misuse and these crimes. This is followed by corruption at 40%, and then financial fraud at 38%. Commercial crimes, such as evasion of capital controls and false invoicing, are also prominent threats, reported by 35% of countries. Additionally, the illicit trafficking of narcotic drugs was reported at 32%, while the illicit cross-border transportation of cash was cited at 30%.

In terms of relative importance, tax crimes, corruption, and illicit drug trafficking were classified as the most impactful, rated 3 out of 3. Meanwhile, financial fraud, commercial crimes, and illicit cash transportation were rated 2 out of 3.

- ✓ **TF Threats Through the Misuse of Legal Persons and Legal Arrangements**

Regarding TF, the decentralized threat posed by individuals or informal networks was identified as the most significant, related to the presence of individuals who collect or transfer funds in support of terrorism, whether ideologically motivated, under a humanitarian guise, or due to family or social pressures. This phenomenon was reported by 30% of countries. It is followed by individuals or intermediaries supporting terrorism (either independent decentralized actors or members of centralized organizations), relying on the illicit cross-border movement of funds, which was reported at a similar rate (30%). The centralized threat, which involves official entities or central control hubs, was reported at 25%. Additionally, 20% of countries identified threats associated with terrorist networks linked to organized crime, especially human trafficking and migrant smuggling, while 15% pointed to complex and covert

networks related to terrorist organizations relying on sanctions evasion and circumvention of prohibitions.

In terms of relative importance, the decentralized threat was ranked the highest, at 3/3, while the presence of covert networks linked to terrorist organizations circumventing sanctions, networks linked to organized crime (particularly human trafficking and migrant smuggling), and individuals or intermediaries involved in the illicit cross-border transportation of funds were rated medium, at 2/3.

✓ **The Overlap Between ML and TF Through the Misuse of Legal Persons and Legal Arrangements**

The analysis shows an overlap between ML and TF through certain tools used in both crimes, where legal persons and legal arrangements are misused to conceal the identity of beneficial owners and to move illicit funds through complex channels. One of the most notable channels is the illicit cross-border transportation of funds, which is a common channel for moving illicit assets across both categories. Also, the concealment of financial flows and the use of commercial activities as a front are among the common methods shared by money launderers and terrorist financiers.

2.3.2. Classification of Vulnerabilities in Combating ML/TF

Countries in the Middle East and North Africa suffer from several key vulnerabilities that affect their ability to combat ML and TF. These challenges can be classified into three main areas: lack of transparency, limited access to information, and ineffective oversight of financial operations. These factors make it difficult for supervisory authorities to trace illicit financial transactions and identify the real beneficial owners behind suspicious financial activities.

✓ **Lack of Transparency and Disclosure of Beneficial Ownership**

The data indicates that 45% of responding countries experience difficulty in identifying accurate data on the real beneficial owners (owners/controllers) of legal persons and legal arrangements, which complicates financial oversight efforts. Additionally, 40% of countries reported the absence of effective legislation or weak enforcement of laws requiring beneficial ownership disclosure, which allows concealment of the true identities of those who control these entities. Moreover, 35% of countries pointed out that inaccurate or outdated beneficial ownership data is being provided, which hampers financial investigations and limits the effectiveness of audits and controls.

This point is considered one of the most critical vulnerabilities in the region, with a relative importance rating of 3/3, and is widely exploited by criminals, representing 55% of ML cases and 40% of TF cases.

✓ **Limited Access to Information**

A major obstacle to combating ML/TF is the lack of data collection tools. 40% of countries reported that their systems lack advanced central mechanisms for registering and updating beneficial ownership data. Furthermore, 35% of responding countries stated that the

complexity of legal procedures or the existence of legislative constraints such as professional secrecy hinders regulatory authorities from accessing information in a timely manner, thus reducing the effectiveness of financial investigations and increasing the opportunities for misuse of legal structures.

This vulnerability is rated 2/3 in terms of regional importance and is significantly exploited by criminals, as it represents 50% of ML cases and 30% of TF cases.

✓ **Weak Oversight of Financial Operations and Ownership**

Concealing income and assets through shell companies and trusts poses a major challenge in combating ML. 30% of countries confirmed that these legal structures are used to disguise the sources of illicit funds. Additionally, 25% of countries stated that company registrations without clear purposes or with nominee directors complicate the tracking of suspicious financial flows and increase the difficulty of detecting fraudulent structures.

This vulnerability is rated 2/3 in the region and is heavily exploited by criminals, representing 45% of ML cases and 35% of TF cases.

➢ **→ Classification of Vulnerabilities by Legal Persons and Legal Arrangements**

Vulnerabilities in combating ML/TF are classified based on the differing nature of risks between legal persons and legal arrangements. The results indicate that lack of disclosure of beneficial ownership is among the most serious vulnerabilities in both categories. 45% of countries reported that the absence of a clear legal framework for beneficial ownership in legal persons represents a major challenge, while 40% of countries stated that trusts are not subject to adequate beneficial ownership disclosure.

Additionally, the use of fictitious nominee directors and the lack of requirement for companies to disclose their actual ownership are major threats. 45% of countries reported that such practices are used in ML/TF operations. Similarly, trusts registered under pseudonyms and endowments not subject to effective oversight serve as additional means to conceal the identities of beneficial owners, increasing the difficulty of detecting illicit financial activities.

2.3.3. Analysis of Methods, Trends, and Typologies in Money Laundering and Terrorism Financing Based on National Responses

Based on the responses of 16 member countries, the methods, trends, and Typologies used in money laundering (ML) and terrorism financing (TF) through legal persons and legal arrangements were classified. This classification is based on three essential elements: location (where), purpose (what), and method (how), along with an evaluation of the percentage indicating the level of importance and frequency of use by criminals.

▪ **Methods, Trends, and Typologies Used in Money Laundering**

✓ **Money Laundering through the Misuse of Legal Persons**

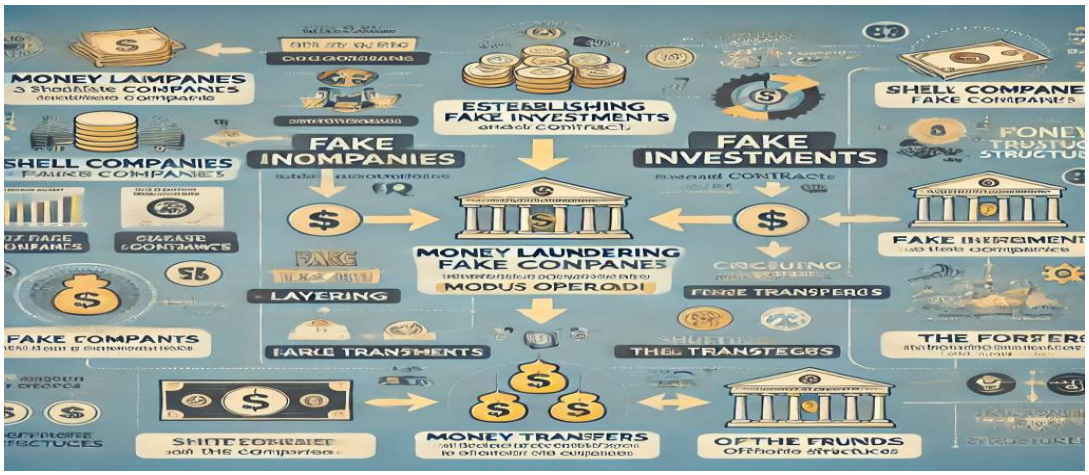
The data reveals that 45% of ML activities through legal persons occur across multiple jurisdictions, highlighting the cross-border nature of these crimes. In addition, free zones and

jurisdictions with weak regulatory controls are misused in 35% of cases, while shell companies registered in tax havens account for 30%.

The main purpose of using legal persons in money laundering is to establish shell companies to justify illicit financial flows—this practice was identified in 50% of the cases. Other purposes include the misuse of corporate bank accounts for the transfer of funds (40%) and the use of companies to purchase real estate and luxury vehicles (35%).

The most common techniques for the misuse of legal persons in money laundering cases are: 55% the use of shell companies and front businesses, 45% of cases involved the use of nominee directors to register companies, and 35% of cases involved the use of professional intermediaries to conceal identity.

✓ **Technique: Use of Shell Companies and Front Businesses**



This technique relies on the creation or misuse of shell companies or front businesses that do not carry out any actual economic activity but are instead used as a channel to move illicit funds. These entities are registered under the names of fictitious or unrelated individuals, which makes it difficult to trace the beneficial owner. These companies are used to conduct fictitious commercial transactions, issue fake invoices, or execute complex financial transfers in order to conceal the origin of the funds and present them as proceeds of legitimate activity.

*** Country Kh: Case Study No. 12***

Use of a Network of Multi-National Shell Companies to Transfer Large Funds Without Actual Activity Through Interlinked Ownership Structures to Launder Money and Conceal the Identity of the Ultimate Beneficiaries

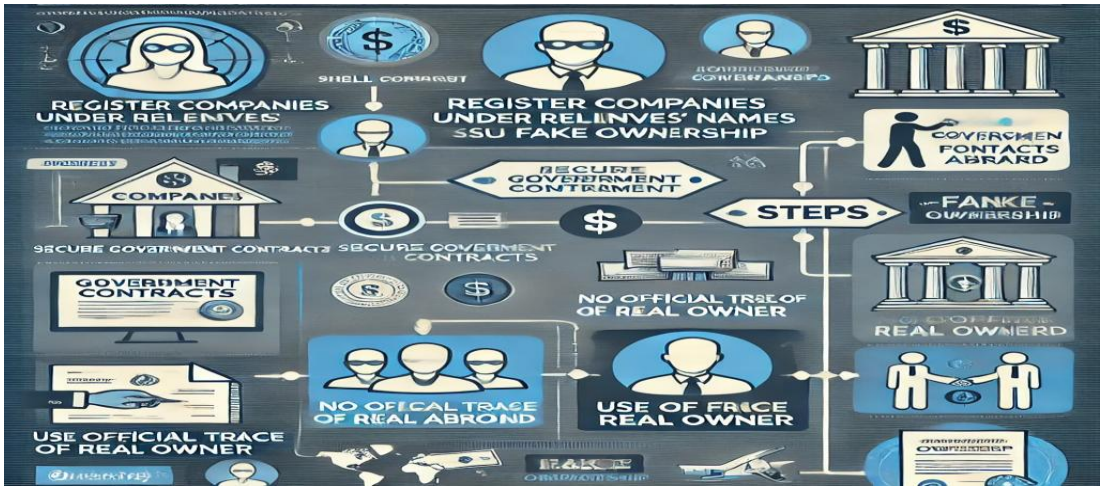
- **Case Background:** International financial investigations uncovered an extensive network of shell companies that were established and used to transfer large sums of money without engaging in any actual commercial activity. The perpetrators relied on creating multiple companies in free zones and various countries, exchanging financial transfers among them using fictitious contracts and investments, before ultimately closing these companies and transferring the funds abroad.

-Sequence of Events:

1) The suspect established several limited liability companies in a foreign country, without conducting any real commercial activity.

2) Large financial transfers were made between these companies using fake investment contracts. 3) These transfers were introduced into the banking system in a way that made them appear legitimate. 4) Shortly after the intensive financial activity, the companies were closed, and the funds were transferred abroad through complex financial networks.	
Legal Nature	Limited Liability Company registered in free zones and offshore jurisdictions
Sector	Financial services / Investment companies / Multi-activity entities
Relevant Stages	✓ **Placement**: Channelling funds through fake investment contracts to shell companies ✓ **Layering**: Exchanging transfers between shell companies registered in various countries within interlinked ownership structures
Predicate Offense	Not precisely defined (implicitly understood due to the presence of illicit sources of funds)
Techniques Used	- Establishing shell companies with no actual activity, solely for conducting internal financial transfers - Using fictitious contracts and investments between companies to justify financial flows - Closing companies shortly after receiving and transferring funds abroad - Creating an interwoven ownership structure among multiple companies to hide the identity of the real beneficiaries
Red Flags – Indicators	Multiple newly registered companies over short timeframes linked to unjustified financial transfers The same individuals or service providers appear in the registration of multiple companies Large financial transfers between companies with no logical commercial relationships Active bank accounts for companies that are not updated or do not engage in real activity
Regulatory Gaps	▪ Weak verification of the activities of companies registered in free zones and virtual offices ▪ Lack of regular monitoring to update company and ownership data ▪ No requirement for companies to fully disclose complex ownership structures and ultimate beneficial owners ▪ Weak international coordination in tracing financial flows through multinational entities ▪ Deficiencies in bank alert systems related to inactive or outdated corporate accounts

✓ **Technique: Use of nominee directors to register companies**



This method relies on appointing "Nominee Directors" to assume managerial positions in companies instead of the actual controlling person. These individuals are selected to register the company in their names only, without having any actual role in management or decision-making. The purpose of this technique is to conceal the true identity of the beneficial owner of the company, making it more difficult for authorities to uncover the links between the legal entity and the illicit funds associated with it. This method is used to provide an additional layer of concealment and camouflage within money laundering operations.

*** Country R: Case Study No. 18***

Use of Companies Registered in the Names of Nominated Relatives to Conceal the Beneficial Owner, Obtain Government Contracts, and Transfer Funds Abroad in a Coordinated Pattern of Evasion, Concealment, and Money Laundering

- **Case Background:** Investigations revealed that a businessman used his relatives to register several commercial companies in their names, while he was the real beneficial owner and actual controller of their operations. This concealment helped obscure his connection to government contracts and major investments concluded by these companies, which were also used to transfer funds to foreign companies without showing the relationship between the entities**.**

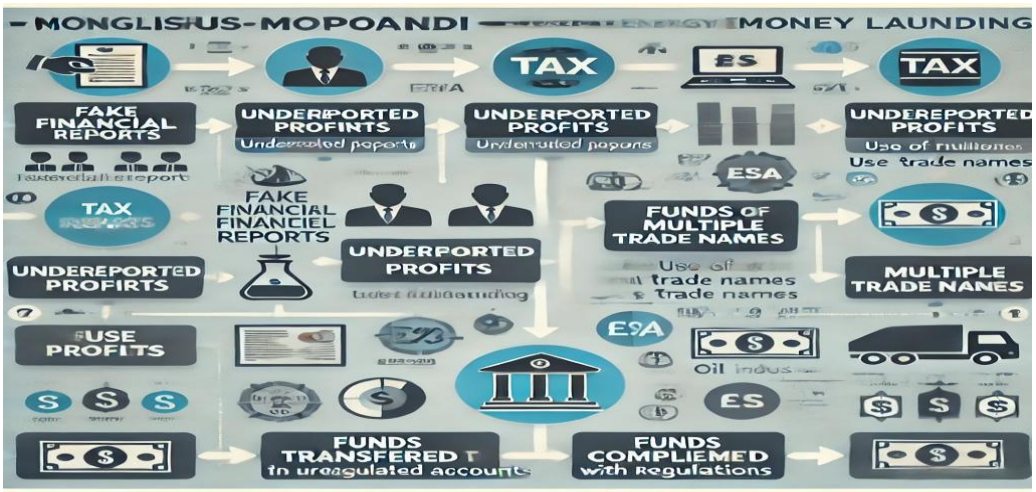
-Sequence of Events:

5) The businessman established several companies in various sectors (such as contracting, logistics services), registering them under the names of his relatives to avoid direct association.
6) Some of these companies obtained government contracts and domestic investment projects due to their "clean" legal façade.
7) The funds collected from these contracts were transferred to accounts of other companies abroad, helping obscure the relationship between the entities and the real owner.
8) The businessman's name did not appear in any founding documents or bank accounts, while investigations revealed that all financial decisions were managed under his direct instruction.

Legal Nature	Limited Liability Company
Sector	Commercial companies in various sectors (contracting, logistics services, supply)
Relevant Stages	✓ **Layering:** Use of companies registered in the names of nominated relatives and transferring funds abroad
Predicate Offense	Not precisely defined (implicitly understood due to the presence of illicit sources of funds)
Techniques Used	- Registering companies in the names of relatives and nominee partners to conceal the true decision-maker's identity

	- Using legal façades to obtain government projects or major investments - Routing funds from domestic companies to foreign entities without showing links between the parties - Managing financial operations behind the scenes without official documents proving actual control
Red Flags – Indicators	✚ Significant similarity in the structure of several companies in terms of activity and address despite differing registered owners ✚ Newly established companies receiving large government contracts without a clear commercial track record ✚ Outbound transfers from companies with no clear activities abroad ✚ Personal or family relationships between the owners of multiple companies despite differing registered names ✚ Repeated use of the same parties to sign contracts or submit similar documentation
Regulatory Gaps	▪ Absence of an effective mechanism to verify the identity of the beneficial owner at the time of company registration ▪ Weak oversight of conflicts of interest in government contracting ▪ Lack of coordination between contracting authorities and supervisory bodies to review the background of companies ▪ Limited tools to analyze the true economic ownership behind legal structures ▪ Weak procedures for ongoing verification of financial relationships between domestic and foreign entities

✓ **Technique: Using professional intermediaries to conceal identity.**



This technique is based on the misuse of professional services such as lawyers, accountants, or company formation agents to create or manage legal entities on behalf of the real client. These intermediaries are used as a legal front to conceal the identity of the beneficial owner, making it difficult for supervisory authorities to trace the source or true owner of the funds. The intermediary often provides services without seriously verifying the client's background, or exploits legal loopholes in due diligence requirements, making this technique effective in obscuring the connection between the funds and the associated criminal activities.

*** Country J: Case Study No. 7***

Systematic Tax Evasion in the Energy Sector through Fictitious Records, Complex Corporate Structures, and Profit Transfers to Unsupervised Accounts with the Assistance of a Certified Accountant

- **Case Background:** As part of tax audits on companies operating in the energy sector, a company engaged in the import of petroleum derivatives was discovered to have submitted financial statements for several years that did not reflect its actual business activity. Investigations revealed that the company used multiple corporate structures to conceal true commercial operations and reduce its due tax obligations.

-Sequence of Events:

9) A company was formally established to operate in the energy sector and import petroleum derivatives.
10) For nine years, the company consistently submitted tax returns that significantly understated its actual level of activity.
11) A certified accountant prepared fictitious financial statements and tax declarations, deliberately understating declared profits and tax liabilities.
12) The company used multiple bank accounts and registered its activities under different trade names to hide real income and fragment financial operations.
13) The case was referred to the tax and judicial authorities after repeated inconsistencies in the reports were observed.

Legal Nature	Limited Liability Company
Sector	Energy Sector (Import of Petroleum Derivatives)
Relevant Stages	✓ **Placement:** Concealing profits and transferring them to accounts not subject to tax oversight ✓ **Layering:** Using different trade names to fragment activities + using multiple accounts ✓ **Integration:** Retaining profits and recycling them within the financial system away from supervision
Predicate Offense	Tax evasion
Techniques Used	- Preparation of fictitious financial data to reduce the actual value of profits - Use of multiple bank accounts to hide income flows - Registration under multiple trade names to fragment operations and confuse oversight - Collaboration with a certified accountant to produce misleading tax returns - Prolonging the tax evasion scheme by appearing to comply formally with regulations
Red Flags – Indicators	Significant discrepancy between tax data and customs/banking records Presence of multiple trade names linked to the same legal entity Same certified accountant filing financial returns for several years with no substantive changes High financial activity compared to declared profits Registration of multiple branches without clear and separate financial records for each branch
Regulatory Gaps	▪ Weak coordination between tax and banking authorities for real-time data exchange ▪ Excessive reliance on data provided by companies without independent verification ▪ Absence of an active risk analysis mechanism for companies with high financial activity ▪ Inability to track relationships between multiple bank accounts and the company's activities ▪ Lack of periodic monitoring of commercial activities registered under different trade names for the same entity

✓ Money Laundering through Legal Arrangements

Legal arrangements are also a key channel for money laundering, particularly through unregistered or unregulated trusts and waqfs. The misuse of unregistered waqfs is the most common method, followed by the use of foreign legal arrangements and the movement of funds through complex illicit trusts.

The primary objective in these cases is to conceal the sources of illicit funds by establishing charitable waqfs and using unregistered legal arrangements to hide the actual ownership of assets, while illicit trusts are used for obfuscating transfers.

Among the most commonly used misuse techniques by criminals: registering charitable waqfs as a front for money laundering (50%), concealing the beneficial owner by appointing nominee beneficiaries in legal arrangements – especially foreign ones (45%), and using bank accounts held by illicit trusts in suspicious transfers (40%).

- **Methods, Trends, and Typologies Used in Terrorism Financing (TF)**

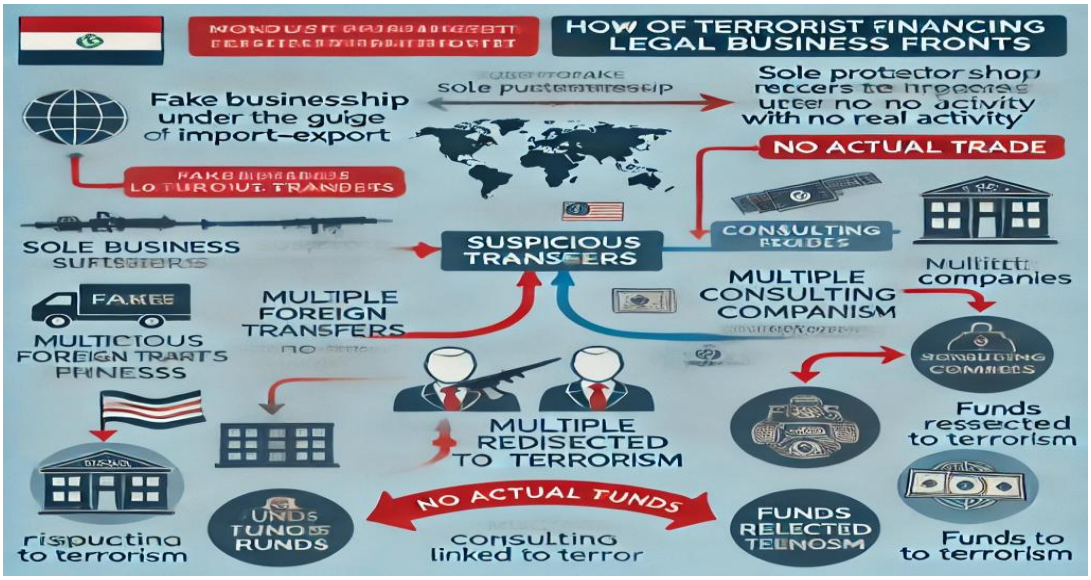
✓ **Terrorism Financing through Legal Persons**

Terrorism financing through legal persons primarily occurs via locally registered small and medium-sized enterprises (SMEs). Other relevant locations include conflict zones, unregulated borders, and commercial entities in smuggling areas.

The primary purpose in these cases is to use small businesses as a front for terrorism financing. Other objectives include collecting donations under the cover of commercial activities and diverting company profits to terrorist networks.

The most widely used techniques by terrorists include: using small businesses as a front for financing (50%), companies making direct financial transfers to individuals linked to terrorism (particularly non-profit organizations) (45%), and concealing financial flows through inflated corporate invoices (40%).

Technique: Using small companies as a front for financing.



This technique relies on the misuse of small businesses, such as shops or sole proprietorships (special interest entities), as a visible front to channel funds designated for terrorism financing. These businesses are often subject to weak or limited oversight, which facilitates their use in conducting financial transfers or collecting donations without attracting attention. The bank accounts and business activities of these entities are used to justify financial flows and conceal their true purpose, taking advantage of their small size and local nature to evade regulatory scrutiny and strict compliance.

*** Country A: Case Study No. 3***

Camouflaging Terrorism Financing through a Sole Proprietorship for Import and Export as a Financial Front

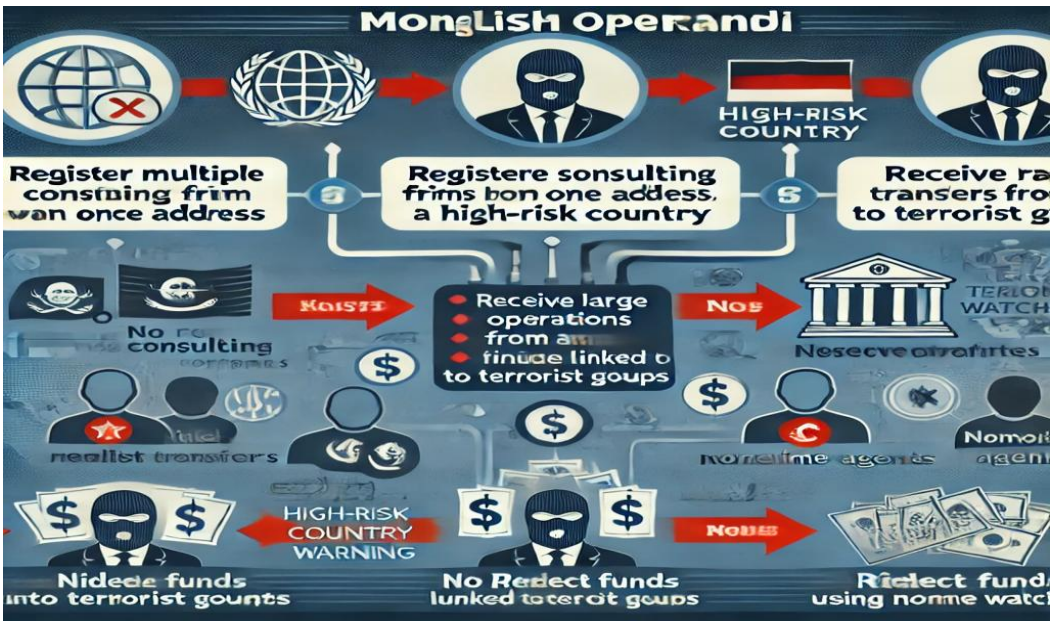
- **Case Background:** As part of the monitoring of financial activities related to terrorism financing, a sole proprietorship officially operating in the import and export sector was identified as receiving large and regular financial transfers from a company located in a country listed as high-risk for money laundering and terrorism financing.

-Sequence of Events:

1) The offender established a sole proprietorship officially registered with the competent authorities and opened a bank account in the name of the establishment.
2) The entity began receiving financial transfers from a foreign company under the pretense of importing goods and services.
3) There were no actual commercial activities or customs imports to correspond to these transfers.
4) Subsequently, investigations revealed that the owner of the foreign company was listed on terrorism watchlists, and the transferred funds were used to finance terrorist groups inside Egypt.
5) These transfers were not reported by the concerned bank, as the entity was officially registered and showed no overtly suspicious activity.

Legal Nature	Sole proprietorship
Sector	Foreign trade sector (import and export)
Relevant Stages	✓ **Transmission:** Receiving transfers from abroad via the sole proprietorship ✓ **Usage:** Distributing funds to domestic parties linked to terrorist groups
Techniques Used	- Establishment of a sole proprietorship operating under the guise of a legitimate activity (import and export) - Receiving large financial transfers from a suspicious foreign entity - Absence of any actual commercial transactions corresponding to the transfers - Withdrawing funds locally and directing them to terrorist entities - Misuse of the legitimate legal form of the entity to avoid raising suspicion
Red Flags – Indicators	Large and repeated financial transfers to a newly established sole proprietorship Absence of imports or customs data corresponding to the alleged transfers Financial relationship with a foreign company based in a high-risk country Excessive use of cash accounts without clear invoices or contracts Lack of actual import licenses or documented dealings with foreign parties
Regulatory Gaps	▪ Weak customer due diligence (CDD) procedures in dealing with sole proprietorships ▪ Absence of integration between supervisory authority databases and international sanctions lists ▪ Banks relying solely on the legal form without analyzing actual activity and transfers ▪ Lack of effective mechanisms to detect transfer patterns related to terrorism financing ▪ No obligation for sole proprietorships to submit periodic disclosures on their commercial activities and financial data

✓ **Technique: Companies conducting direct financial transfers to individuals linked to terrorism**



This technique relies on the use of companies, whether legitimate or shell entities, to carry out direct financial transfers to individuals suspected or known to be linked to terrorist activities. These transfers are recorded as commercial dues, salaries, or payments for services, giving them a legal appearance. The corporate framework of the company is exploited to legitimize these transfers and avoid scrutiny, relying on weak beneficiary verification procedures in some financial systems.

*** Country D: Case Study No. 13***

Use of registered consultancy companies as legal fronts to transfer suspicious funds without actual activity for terrorism financing purposes

- Case Background:

Joint investigations by Financial Intelligence Units and security authorities revealed that some companies officially established as consultancy firms were in fact used as legal fronts to transfer suspicious funds for the purpose of terrorism financing. Shell structures were used to conceal the identity of the beneficial owner.

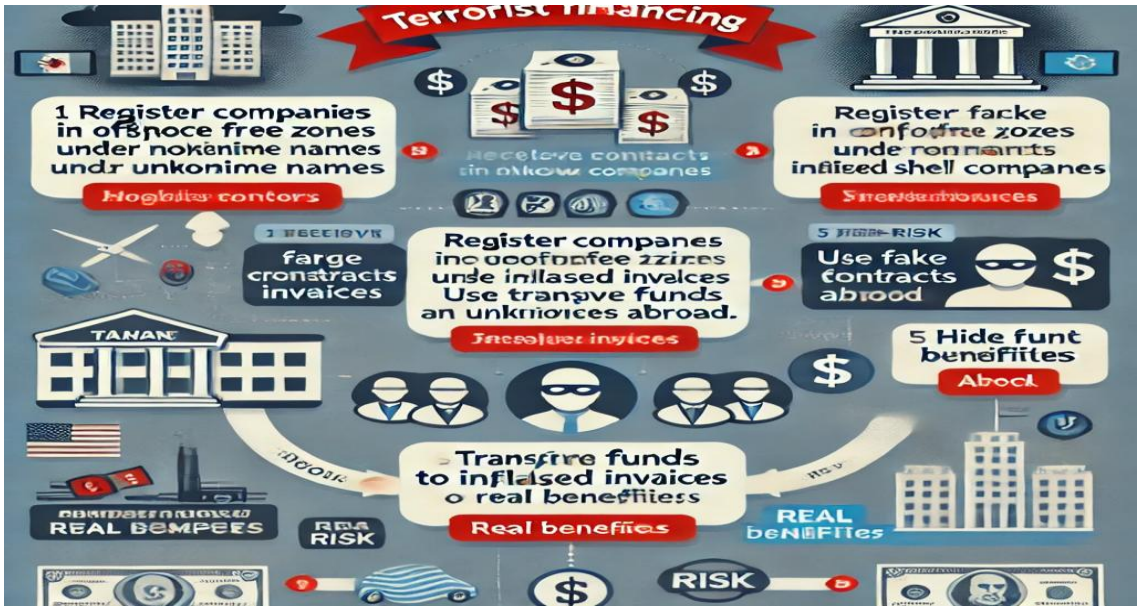
-Sequence of Events:

1) The suspect established several limited liability companies all operating in the consultancy and services sector, registered at the same address.
2) Authorities could not locate any accounting records or documents supporting the existence of legitimate business activity.
3) Large financial transfers were detected in the accounts of one of these companies, linked to a country classified as high-risk for terrorism financing, with no contracts or actual services provided corresponding to those transfers.
4) Investigations revealed that the transferred funds were directed to accounts of individuals suspected of affiliation with terrorist entities.

Legal Nature	Limited liability companies
Sector	Consultancy and services sector

Relevant Stages	✓ **Collection:** Receiving large financial transfers from a high-risk country in the field of terrorism ✓ **Transmission:** Transferring the funds to accounts of individuals or entities linked to terrorist activities
Techniques Used -	- Establishment of multiple consultancy firms registered at the same address to mislead authorities - Rapid redirection of received funds to external entities to obstruct traceability - Concealment of the beneficial owner through the use of nominee agents - Presenting the company as a "service" entity not subject to strict oversight of actual commercial activity
Red Flags – Indicators	Multiple companies registered at the same location and operating in the same sector Large financial transfers from parties in high-risk countries without clear justification Absence of real operational activity or known clients Immediate transfer of incoming funds abroad without invoices or supporting documents Transfers linked to suspicious individuals listed on terrorism watchlists
Regulatory Gaps	▪ Weak oversight of professional and consultancy service companies compared to financial sectors ▪ Lack of effective verification mechanisms for company addresses and the nature of their activity ▪ No field or regulatory inspections of newly established companies despite receiving large transfers ▪ Failure to verify the nature of the economic relationship between local companies and sending or receiving parties ▪ Limited international cooperation in tracing transfers

✓ Technique: Concealing financial flows through inflating commercial invoices of companies



This technique relies on the use of legal companies to inflate the value of invoices in commercial transactions, with the aim of concealing the transfer of funds intended to finance terrorist activities. Invoices with amounts higher than the actual value of goods or services are issued between affiliated

or colluding companies to justify suspicious financial flows that appear legal on the surface. This method allows the passage of funds without raising suspicion, especially when using companies with a seemingly reputable profile or operating in sectors with high volumes of commercial transactions, such as import and export.

*** Country Dh: Case Study No. 16 ***

Use of front companies in free zones and outdated, non-updated accounts to carry out large financial transfers through fake contracts and inflated invoices for the purpose of terrorism financing while concealing the identity of the beneficial owners

- Case Background:
Investigations revealed that a number of individuals exploited companies registered in free zones with weak supervision to conduct suspicious financial operations related to terrorism financing, and to conceal the identity of the real beneficiaries of the transfers. Fake contracts and inflated invoices were used to justify the transfers and mislead banking systems.

-Sequence of Events:
1) The suspects established multiple companies registered in free zones outside the country, where banking operations were subject to limited oversight, and in the names of nominee partners to conceal the identities of the real beneficiaries.
2) These companies were used to receive funds from unknown sources, which were then transferred to external bank accounts using fake commercial contracts and inflated invoices, through complex financial operations without disclosing the beneficial owner.
3) There was no record of any actual commercial activity to justify these transfers, and no import or export records existed.
4) The investigation revealed that the company was used as a front to transfer funds to entities suspected of being involved in terrorism financing.

Legal Nature	Limited liability companies
Sector	Import and export sector
Relevant Stages	✓ **Collection:** Receiving funds from unknown sources without real commercial activity ✓ **Transmission:** Transferring funds to suspicious entities linked to terrorist organizations
Techniques Used -	- Preparation of fake financial statements that understate actual profits - Use of multiple bank accounts to obscure income flows - Registration under multiple trade names to fragment activities and confuse oversight - Collaboration with a certified accountant to produce misleading tax declarations - Prolonging tax evasion by appearing to comply superficially with regulations - Creation of front companies without real activity, used as tools for transferring funds - Registration of companies under nominee names to conceal the identity of the real controller of financial operations - Execution of complex financial transactions to obscure the real financial trail - Abuse of free zones to carry out transfers beyond regulatory oversight - Use of fake commercial activities such as import and export to justify large illicit financial transfers
Red Flags – Indicators	Registration of multiple companies in free zones not subject to adequate oversight Companies transferring large sums of money without supporting commercial activity Financial transfers between companies owned by nominee individuals without real business transactions Import and export companies receiving large transfers without actual activity

	Beneficial owner linked to entities listed on terrorism watchlists
Regulatory Gaps	▪ Weak oversight systems for companies registered in free zones ▪ Inadequate Typology of enhanced scrutiny procedures for companies with high-volume invoicing activities ▪ Lack of integration between legal ownership and banking databases to verify the identity of the beneficial owner ▪ Limited banking follow-up on sequential and complex transfers between commercial entities

✓ **Terrorism Financing through Legal Arrangements**

Decentralized financing represents the most commonly used method by criminals, recorded at 50%.

Unregistered non-profit organizations not incorporated as legal persons and operating as informal trustees under legal arrangements—particularly those active in conflict zones—are the most exploited entities for terrorism financing. Unregistered religious endowments are also misused.

The main objective of these activities is to use non-profit organizations to raise funds for terrorist groups. Similarly, endowments are exploited as a front to transfer funds.

The most commonly used techniques by criminals include: the establishment of fictitious non-profit associations (50%) and the use of endowments to conceal financial flows (40%).

2.4.Identification and Classification of Risk Indicators in the MENA Region

Based on responses from 16 member countries, the methods, trends, and Typologies used in money laundering (ML) and terrorism financing (TF) through legal persons and legal arrangements were classified. This classification is based on actual practices observed in the region and includes key red flag indicators identified to assist supervisory and financial authorities in combating ML/TF.

2.4.1. Indicators for Detecting Risks Related to Money Laundering (ML)

✓ **Legal Persons**

- Use of inactive bank accounts and dormant companies to conduct large-scale financial transfers without actual economic activity.
- Establishment of multi-layered corporate structures to obscure the beneficial owner, complicating the tracking of financial flows.
- Registration of companies with unclear or inconsistent commercial activities relative to their financial flows, indicating potential use as a front for money laundering.
- Large financial transfers to or from companies registered in high-risk countries without a clear economic justification.
- Companies recording no actual imports or exports but receiving substantial financial transfers.
- Use of front companies in financial transactions with unknown entities, suggesting potential money laundering.

✓ **Legal Arrangements**

- Use of trusts to obscure the identity of the beneficial owner, complicating fund tracing.
- Transferring funds between multiple trusts or various accounts within the same financial institution without clear justification.
- Establishment of complex legal arrangements in jurisdictions with high banking secrecy without a genuine business reason.
- Transferring funds from trusts to individuals or accounts of unknown origin without supporting documentation.
- Registration of fictitious legal arrangements or their use as a front to conduct unjustified large financial transactions.

2.4.2. Indicators for Detecting Risks Related to Terrorism Financing (TF)

✓ **Legal Persons**

- Use of shell companies as fronts to transfer funds to individuals or entities suspected of terrorism financing.
- Commercial companies receiving large financial transfers from high-risk countries without genuine economic activity.
- No actual registered activity for the company, yet funds are transferred through it to entities linked to terrorist organizations.
- Registration of companies in loosely regulated commercial sectors, such as import/export, with funds transferred to suspicious entities.
- Unlicensed money exchange companies receiving large transfers from unknown sources, facilitating terrorism financing.

✓ **Legal Arrangements**

- Transferring funds from trusts to individuals in high-risk countries without a clear financial transaction record.
- Frequent changes in trustees or beneficiaries, indicating attempts to obscure real financial activity.
- Legal arrangements making payments to suspicious entities without a clear contractual relationship.
- Transferring funds through financial institutions lacking adequate oversight, contributing to terrorism financing.

2.4.3. Joint Risk Indicators between Legal Persons and Legal Arrangements

Indicators that may signal risks of both money laundering and terrorism financing when observed in companies or legal arrangements:

- Use of inactive bank accounts to conduct large-scale financial transactions without actual economic activity.
- Transferring funds between multiple companies or trusts without clear financial auditing, indicating concealment of the true origin of funds.
- Frequent changes in administrative structure, shareholders, or ultimate beneficiaries, complicating the verification of the beneficial owner's identity.

- Transferring funds from companies or trusts to personal accounts or unknown parties without formal documents explaining the purpose of the transfer.
- Conducting large cross-border financial transactions without clear commercial justification, which may indicate attempts at money laundering or terrorism financing.

2.5. Analysis of Measures Taken by Countries to Detect and Address the Studied Cases

Based on responses from 16 member countries, an analysis was conducted on the measures taken by countries to detect the misuse of legal persons and legal arrangements in money laundering (ML) and terrorism financing (TF). The analysis focused on the methods used and the solutions applied in actual cases.

2.5.1. Measures Taken to Detect Money Laundering (ML)

- Investigation of Shell and Dormant Companies
  - ✓ Country A: Investigations revealed the creation of shell companies for the purpose of money laundering through real estate fraud, where joint-stock companies were registered to collect funds from citizens without executing any actual projects.
  - ✓ Country R: Large financial transfers were detected within companies for which regulatory authorities could not verify any real activity, revealing their use as fronts for laundering money.
  - ✓ Country B: The use of inactive bank accounts and dormant companies to transfer funds abroad in a way that conceals their origin was detected.

- Monitoring Complex Corporate Structures to Obscure Beneficial Ownership
  - ✓ Country D: Investigations confirmed the use of multi-layered companies in money laundering cases, especially where links to political corruption networks were found.
  - ✓ Country T: The creation of holding companies was uncovered, used to conduct large financial transactions without clear operational activity, aimed at tax evasion and concealing the beneficial owner.

- Enhancing Oversight of Commercial Activities Inconsistent with Financial Flows
  - ✓ Country Z: Authorities found that many registered import/export companies had no real operations and were merely used as channels to transfer money abroad.
  - ✓ Country S: Investigations targeted companies offering unlicensed financial services, revealing that most of their activities involved opaque redistribution of funds.

- Auditing Inactive Bank Accounts
  - ✓ Country Dth: Authorities required banks to conduct comprehensive reviews of inactive bank accounts and close any account found to be used for passing suspicious financial transactions.
  - ✓ Country Th: Periodic audits were imposed on corporate bank accounts of inactive companies to prevent their use in money laundering.

2.5.2. Measures Taken to Detect Terrorism Financing (TF)

- Interception of Illicit Financial Transfers via Commercial Companies
  - ✓ Country B: Authorities discovered that import/export companies received large transfers from high-risk countries without actual economic activity, and the funds were passed on to entities linked to terrorist organizations.
  - ✓ Country T: Investigations uncovered the misuse of officially registered commercial companies as fronts to conceal financial flows linked to terrorism financing.
  - ✓ Country R: Local companies received large transfers from foreign countries and redistributed them to individual accounts associated with suspicious entities.
- Addressing Misuse of Unlicensed Money Exchange Companies
  - ✓ Country A: A network of unlicensed money remittance companies was dismantled after receiving large financial transfers and passing them to suspicious accounts without supporting documentation.
  - ✓ Country S: Authorities imposed strict supervisory measures on exchange companies operating without official licenses, as they were found to be used in terrorism financing operations.
- Investigating the Misuse of Inactive Bank Accounts in Terrorism Financing
  - ✓ Country Th: The misuse of bank accounts held by inactive companies as fronts for transferring funds to suspicious entities was uncovered.
  - ✓ Country Z: Authorities discovered that some inactive bank accounts were used to pass funds through repeated transactions between different accounts to finance illicit activities.
- Tightening Oversight on Inauthentic Commercial Activities
  - ✓ Country B: Commercial companies operating in the food sector were discovered to have received large financial transfers without recording any real activity. Upon investigation, it was found that these companies were merely fronts for terrorism financing.

Overall Conclusion

Findings and Key Outcomes

This section is based on the integration of the results of the case analysis on one hand, and the analysis of Member States' responses to the questionnaire on the other, with the aim of presenting a comprehensive analytical conclusion within a structured framework combining field-level practical aspects and broader strategic insights, in order to enhance integrated understanding of how legal structures are misused in contemporary financial crimes.

- **Findings**

Both analyses demonstrated clear alignment in highlighting the patterns and methods used in money laundering (ML) and terrorism financing (TF) through legal persons and legal arrangements.

The analysis revealed significant misuse of shell companies and outdated companies as primary legal persons, with a focus on the most vulnerable sectors, particularly commercial activities, import-export, financial services, and real estate. The data also indicated that the main predicate offenses related to ML include financial fraud, tax evasion, and corruption, with widespread reliance on fake invoices and complex ownership structures.

Regarding terrorism financing, the results showed heavy reliance on licensed companies with no real activity, along with prominent use of informal transfer channels such as the hawala system. The analysis also revealed a noticeable overlap between ML and TF techniques when using legal persons and legal arrangements.

- **Main Outcomes**

The analysis reveals that legal persons and legal arrangements, while being legitimate regulatory tools that facilitate economic and investment activity, are still widely

used in money laundering and terrorism financing due to lack of transparency and oversight. When addressing these challenges, it is important to enhance levels of transparency and supervision without negatively affecting the role of these tools in supporting legitimate economic activity. International cooperation, the Typology of due diligence measures, and intensified oversight of companies and trusts are essential solutions to mitigate these risks in the MENA region.

1. The key outcomes are as follows:
   a. The analysis revealed that ML through legal persons occurs in 45% of cases across multiple jurisdictions, reflecting the cross-border nature of these crimes. Free zones and low-regulation areas are misused in 35% of cases, while shell companies registered in tax havens account for 30%. For TF, 50% of cases involve non-profit organizations operating in conflict zones, while 40% rely on unregistered endowments, and 35% on informal money transfer networks.
   b. The analysis showed that tax crimes, corruption, and financial fraud are the threats most linked to ML through the misuse of legal persons and legal arrangements. Criminals mainly rely on creating shell companies, using nominee directors, and utilizing luxury real estate to conceal the sources of illicit funds. In TF, decentralized financing is the most prominent threat, with funds collected from individuals and NGOs through undisclosed means, exploiting oversight gaps in legal and financial entities.
   c. The data indicates that lack of transparency and varying levels of regulatory effectiveness across regions represent key entry points for the misuse of legal structures in ML and TF. This is due to differences in supervision and implementation levels, creating regulatory loopholes exploited by criminal actors. This is attributed to:
      - The absence of effective systems for collecting and exchanging information.
      - Weak verification procedures for identifying beneficial owners.
      - Inadequate international cooperation and lack of intelligence sharing.
   d. The study found that the following legal persons and legal arrangements are widely used in illicit financial schemes:
      - Shell companies registered in tax havens.
      - Unregistered trusts and endowments.
      - Non-profit organizations operating in conflict zones.
      - Bank accounts of legal entities not subject to effective oversight.
   e. Criminals use several methods to misuse legal persons and legal arrangements, including:
      - Creating shell companies (50%) to justify illicit financial flows.
      - Misusing company bank accounts (40%) to transfer funds.
      - Using companies to purchase high-value assets such as real estate and luxury cars (35%).
      - Relying on nominee directors (45%) to conceal the identity of the beneficial owner.

- Registering companies with fake licenses (40%) to mislead supervisory authorities.
- Inflating invoices between companies (38%) to conceal illicit financial flows. In ML through legal arrangements, the most prominent methods include using fictitious trusts (50%), unregistered endowments (45%), and transferring funds through undeclared accounts (40%).

2. A set of indicators was identified that may signal ML/TF risks, most notably:
   - Using inactive bank accounts to transfer large sums without economic justification.
   - Recording frequent changes in company structure or ultimate beneficiaries, complicating verification.
   - Transferring funds between multiple companies or trusts without clear financial auditing.
   - Using officially registered commercial companies as fronts for TF through large transfers without actual economic activity.
   - Relying on informal money transfer networks to finance terrorist groups.
3. Some countries have taken measures to enhance oversight, such as:
   - Imposing regular audits on inactive bank accounts and companies.
   - Tightening oversight over import-export companies registered without actual activities.
   - Strengthening monitoring of endowment and trust funds to ensure they are not used as a cover for illicit financial activities.

Challenges

The data shows that lack of transparency and difficulties in accessing beneficial ownership information represent major obstacles to efforts to combat financial crimes. In addition, weak international cooperation, the misuse of complex legal structures, and reliance on modern technologies further complicate these challenges. Despite the steps taken to enhance oversight and improve information sharing, there is still a need to strengthen supervisory measures, particularly in free zones and tax havens, and to develop stricter regulatory solutions to protect financial systems from misuse in money laundering and terrorism financing.

▪ Challenges in Accessing Beneficial Ownership Information

The lack of transparency in identifying the beneficial owners of legal entities is a major challenge in combating ML/TF. 45% of countries reported the absence of centralized beneficial ownership registers, hindering immediate access to required information for financial investigations.

Additionally, 40% of countries suffer from weak coordination among supervisory authorities, which reduces the efficiency of financial investigations and impedes international cooperation in tracking suspicious activities. Furthermore, 42% of countries indicated that restrictions on cross-border information exchange and professional secrecy in some financial sectors hinder

the tracking of illicit financial flows and limit the effectiveness of combating cross-border financial crimes.

- **Key Challenges in Detecting and Combating ML/TF**

Despite ongoing efforts, countries continue to face several major obstacles, notably:

- Difficulty in verifying beneficial ownership due to the use of complex corporate structures registered in different jurisdictions.
- Ineffective international cooperation, which hampers the exchange of information on suspicious financial transfers.
- Misuse of modern technologies such as virtual currencies and informal finance in ML/TF operations.
- Weak oversight of unregulated financial sectors, particularly unlicensed money exchange companies used as channels for illegal money transfers.
- Misuse of free zones and tax havens to conceal the origin of illicit funds and exploit lenient regulations in some countries.

- **Remaining Challenges and National Efforts**

Despite ongoing national efforts to combat ML/TF, there are still persistent challenges that require continuous attention, most notably:

- Difficulty in identifying the beneficial owner of legal entities due to complex legal structures.
- Weak effectiveness of financial monitoring tools, especially in tracking cross-border suspicious transactions.
- The need to enhance transparency in legal arrangements to ensure they are not misused for illicit financial activities.

Recommendations

The misuse of legal persons and legal arrangements constitutes a major challenge in combating ML/TF. Transparency, financial oversight, and enhanced international cooperation are among the most important solutions to address these risks. To achieve tangible progress, MENAFATF member countries should update their regulatory policies, apply stricter supervisory mechanisms, and enhance the use of modern technology for early detection of illicit financial activities, by implementing the following recommendations:

- **Enhancing Transparency and Financial Oversight**

Financial transparency is the cornerstone of combating financial crimes, and it is recommended to:

- Establish centralized databases for beneficial owners as a fundamental step in tracking suspicious transactions and limiting the misuse of legal structures, while effectively linking them to other supervisory platforms to enable faster response and improve data

accuracy through integrated mechanisms for continuous updates and alignment with other regulatory data sources.

- Require companies to disclose their beneficial owners and submit periodic reports on their financial movements.
- Strengthen oversight of unregistered trusts and endowments to prevent their misuse in concealing illicit financial flows.
- Use artificial intelligence and data analytics to detect suspicious activities and ensure proactive detection of fraudulent transactions.

- **Tightening Oversight of Companies and Non-Profit Organizations**

Given the role played by these entities in facilitating ML/TF, the following measures should be taken:

- Review newly registered companies, especially in free zones, to verify their actual activities and ensure they are not used as fronts for money laundering.
- Strengthen registration procedures for charities and non-profit organizations to ensure they are not misused for terrorism financing.
- Impose strict transparency standards on informal financial transfers such as cash remittances to ensure traceability of fund sources and their legitimate use.

- **Enhancing International Cooperation and Information Exchange**

Given the cross-border nature of financial crimes, it is essential to:

- Enhance the exchange of financial information between countries, particularly regarding transfers related to companies registered in high-risk jurisdictions.
- Require financial institutions to report any suspicious transactions, especially those related to entities categorized as high-risk.
- Update MENAFATF's risk lists to include the latest methods and technologies used in ML/TF.

- **Tightening Regulatory and Supervisory Measures**

Ensuring the integrity of financial systems is a top priority and includes:

- Conducting regular audits of inactive bank accounts to prevent their use as tools for hiding illicit funds.
- Imposing strict controls over money exchange companies, particularly unlicensed ones used to facilitate illicit financial transfers.
- Monitoring the activities of commercially inactive companies to ensure they are not being used as fronts for money laundering.
- Tightening oversight of cross-border financial transfers, particularly those linked to entities in high-risk jurisdictions.

Table Linking General Recommendations to Detailed Recommendations

General Recommendation	Detailed Linked Recommendations
Updating anti-money laundering and counter-terrorist financing policies	✓ Updating risk lists to include emerging trends and techniques in the misuse of legal persons and legal arrangements.
Enhancing regional and international cooperation	✓ Exchange of information between countries on suspicious transactions. ✓ Cooperation between financial institutions and supervisory authorities to exchange beneficial ownership data.
Strengthening regulatory measures on non-profit organizations	✓ Imposing strict oversight on charitable associations and religious endowments, especially in conflict zones. ✓ Monitoring donations and ensuring their use for legitimate purposes only.
Enhancing financial transparency by mandating beneficial ownership registries	✓ Establishing unified beneficial ownership databases and updating them continuously (periodically and upon any change). ✓ Obliging companies and financial vehicles to disclose, on an ongoing basis (periodically and upon any change), the identities of beneficial owners and prohibiting pseudonyms.
Monitoring international financial transfers linked to high-risk entities	✓ Tightening control over transfers from/to countries classified as high-risk. ✓ Mandatory reporting of suspicious transfers by financial institutions.
Tightening oversight on free zones and tax havens	✓ Reviewing the activities of companies registered in these zones. ✓ Imposing specific transparency standards and monitoring related financial flows.
Combating misuse of shell companies and complex legal structures	✓ Monitoring companies that are commercially inactive or registered under nominee names. ✓ Imposing regular audits on dormant bank accounts linked to such companies.
Raising compliance levels in financial institutions	✓ Imposing strict customer due diligence (CDD) measures on legal entities, particularly in high-risk jurisdictions. ✓ Using data analytics techniques to detect activities.
Regulating the remittance and exchange company sector	✓ Tightening regulations on money exchange companies and prohibiting unlicensed ones from operating. ✓ Tracking informal money transfers and verifying their sources and uses.

Annexes

Annex 1: Typologies Report Questionnaire – November 2023

1-Please Response to the questions below:

Legal persons in the economy	
Nature of Legal persons	*List from countries*
Role of Legal Person	*List from countries*
Sector	*List from countries*
Size of the Legal Person	*List from countries*
Legal Arrangement in the economy	
Nature of Legal persons	*List from countries*
Role of Legal Arrangement	*List from countries*
Size of the Legal Arrangement	*List from countries*

Please answer the following questions to the best of your knowledge (based on your experience, knowledge, statistics, case law or number of suspicious transaction reports):

a. Threats

1-Please select the top 10 ML/TF threats faced by your country (1 = top threat):

	Centralized Terrorist financing threats
7	Decentralization Terrorist financing threats
9	Tax crimes (e.g. tax evasion, tax fraud)
3	Corruption
10	Fraud
4	Trade-based crimes (e.g. avoiding capital controls)
5	National security risk (e.g. foreign ownership of military infrastructure)
6	Circumvention of sanctions and prohibitions
	Illicit trafficking in narcotic drugs and psychotropic substances
	Illicit cross-border transportation of cash
7	Trafficking in human beings and migrant smuggling
8	Environmental crimes (e.g. illegal fishing)
	Other: [PLEASE SPECIFY]

2- Please select the top roles of your country related to the threats above (1 = top role):

	First step of the predicate offense (e.g. drug production, tax evasion)
3	Creation of corporate vehicles for the illegal scheme (e.g. creation of companies)
1	Offering of professional or informal nominee shareholders and directors (i.e. nationals of your country offer their services as nominees for the illegal scheme)
	Opening of financial accounts to transfer funds as part of the scheme
2	Destination country (e.g. illegal funds are kept in your country's financial institutions and freeports, or are illegal funds are used to purchase real estate or other assets in your jurisdiction)
	Physical involvement of cross border inflow and outflow of illegal proceeds
	Other: [PLEASE SPECIFY]

b. Vulnerabilities

3-Please select the top 10 vulnerabilities faced by your country's legal framework and regulations (1 = top vulnerability):

Hiding the owners or controllers (e.g. beneficial owners) – Availability of information	
	No beneficial ownership framework at all
	Inconsistent framework within the country (e.g. free zones have different rules than the rest of the country)

	Inadequate resources allocated to address the issues on identify beneficial owners of foundations, associations and other similar entities.
	Country of incorporation loophole (framework covers only local entities, not foreign ones)
	Type of entity loophole (e.g. only companies are covered, but not other types of legal persons, or only legal persons are covered but not trusts)
	Exceptions from scope (e.g. exceptions for some types of companies, such as state-owned enterprises)
	No provisions at all for exotic foreign corporate vehicles (e.g. Anstalt)
	Inappropriate provisions for foreign entities that share the same name as local ones (e.g. foreign private-interest foundation is treated like a local charity)
	Inactive entities (i.e. dormant entities that fail to file information are allowed to remain in the registry and hold assets)
	Not all relevant elements in the beneficial owner definition (e.g. ownership, control and benefit)
	High thresholds in the beneficial ownership definition (i.e. relevant individuals avoid registration because of the high thresholds)
	Not all parties to the trust or the private-interest foundation need to be identified
	Inappropriate definitions for the type of entity (e.g. “threshold of 25% of shares” applies to trusts)
	Lack of guidance to relevant authorities on beneficial ownership.
	Can we add: absence/misapply of conducting or obtaining record basic information.
	Other: [PLEASE SPECIFY]
Hiding the owners or controllers (e.g. beneficial owners) – Determination of the beneficial owner	
5	Shelf companies
1	Complex ownership structures
	Bearer shares
2	Professional nominees (shareholders or directors)
3	Informal nominees (shareholders or directors), e.g. family members
4	Remote virtual services to set up companies online
	Non-stock companies, companies limited by guarantee
	Use of professional intermediaries in forming legal persons
	Other: [PLEASE SPECIFY]
Hiding the owners or controllers (e.g. beneficial owners) – Accuracy of information	
	Beneficial ownership information is not always updated
	The beneficial owner’s details are usually incorrect
	Inadequate co-ordination and information-sharing among law enforcement and intelligence agencies.
	Other: [PLEASE SPECIFY]
Collection of beneficial ownership	
	Beneficial ownership registries are not fit for purposes (e.g. lack resources for verification)
	AML/CFT framework doesn’t cover all relevant obliged entities (e.g. lawyers are excluded)
	Involvement of obliged entities: they are either wilfully blind or complicit in ML/TF
6	Low awareness or understanding of AML/CFT within obliged entities
	Low enforcement by authorities of the AML/CFT framework (e.g. low audits, no sanctions)
	Other: [PLEASE SPECIFY]
Access to beneficial ownership information	
7	Lack of timely and appropriate access by some authorities
8	Lack of appropriate exchange of information with relevant foreign countries
10	Professional confidentiality (e.g. attorney-client privilege)
	Weaknesses in the competent authorities’ ability to gather and share information.
	Other: [PLEASE SPECIFY]
Hiding the income and assets of corporate vehicles	

	Virtual assets
	Lack of (centralised) ownership and price information of assets (e.g. real estate)
	Involvement of gatekeepers (e.g. lawyer, notary, broker) in real estate purchases
9	Use of lawyer-held or trust accounts
	Use of virtual office, directorship and mailbox services
	Other: [PLEASE SPECIFY]
Hiding the purpose, transactions and relationships of corporate vehicles	
	Shell companies
	Low AML/CFT compliance by obliged entities
	Entities that engage in provision or sale of services (rather than sale of goods)
	Other: [PLEASE SPECIFY]

c. Methods, trends and typologies

4-Please select the top 10 typologies present in your country (1 = top method):

Typology		**Additional details (if typology is selected)**
Where		
1	Multi-jurisdiction splitting (e.g. Company is from country A, shareholder is from country B, beneficial owner is from country C, and corporate assets are located in country D).	Which are the most relevant countries/regions used in the multi-jurisdiction splitting? Country of incorporation: British dependencies, e.g. BVI, Cayman islands. Country of nominees: Cyprus, Malta, Panama Country of Beneficial owner: MENA Location of Assets: MENA, EU, USA
What		
	Shell companies	From which countries/region? [*COMPLETE HERE*]
	Corporate directors	From which countries/region? [*COMPLETE HERE*]
6	Shell companies	From which countries/region? From BVI and Cayman Islands
	Front companies	From which countries/region? [*COMPLETE HERE*]
	Partnerships	From which countries/region and what type of partnerships? [*COMPLETE HERE*]
4	Trusts	From which countries/region and what type of trusts? Discretionary trusts from Cyprus
5	Foundations	From which countries/region and what type of foundations? Private interest foundations from Panama and NL
	Private investment funds	From which countries/region and what type of investment funds? [*COMPLETE HERE*]
	Inappropriate definitions for the type of entity (e.g. “threshold of 25% of shares” applies to trusts)	
	Use of high number of professional gatekeepers (e.g. so	From which countries/region and what type of profession? [*COMPLETE HERE*]

	none of them discover the scheme)	
	Instruments for the beneficial owner to control the nominee director (e.g. power of attorney, waiver, and signed (but undated) termination letter.	Main type of instrument (e.g. power of attorney)? [*COMPLETE HERE*]
3	Use of professional nominee shareholders and directors	From Cyprus, Malta and Panama
	"Nominee beneficial owners" (e.g. use of wealthy nominees who "look" like a real beneficial owner)	From which countries/region? [*COMPLETE HERE*]
2	Informal nominees: deliberate and victims of identity fraud	From which countries/region and what type (e.g. deliberate or victims)? Family members from MENA
	Bearer shares	
How		
7	Complex ownership and control structures	Usual length and types of entities involved? Companies and trusts, usually 5-10 layers
8	Foreign ownership	From which countries/region? Russia, Iran
	Control without ownership: use of power of attorney, contracts and financial instruments	Main type of instrument (e.g. power of attorney, convertible stock, etc.)? [*COMPLETE HERE*]
	Fake IDs	Main countries and type of ID? [*COMPLETE HERE*]
9	Abuse of professional confidentiality	Main country of residence of the professional and type of profession? Lawyers from USA, UK and British dependencies
Hiding or faking income		
	Entities with misleading names	From which countries/region and what type of entity? [*COMPLETE HERE*]
	Fake invoicing	From which countries/region and for what type of service/goods? [*COMPLETE HERE*]
10	Fake loans	From which countries/region? British dependencies and EU countries
	Disguise transfers as legitimate wages	
	Use of lawyers' trust or client accounts.	From which countries/region? [*COMPLETE HERE*]
	Other: [PLEASE SPECIFY]	

d. Risk indicators

5- Please describe between up to 3 local cases (e.g. investigations you have undertaken)

Case 1 (Source: Singapore 2018 report on Misuse Typologies and Best Practices)	
Crime involved (e.g. money laundering, corruption)	Money laundering

Description of the case: Company 1, Company 2, Company 3, Company 9 (and previously Company 8) were subsidiaries of a South Asian Conglomerate Group. All the companies were involved in the commodities industry. The round-tripping transactions occurred within a span of two months. The bank noticed the round-tripping of funds where funds originating from Company 1, Company 2 and Company 3 were passed through several companies and eventually remitted back to Company 1 and Company 3. The round-tripping activities resulted in a high turnover of funds for Company 4, Company 5 and Company 6 (i.e. significant value and volume of transactions passing through the accounts of these companies). The bank was also unable to corroborate the Source of funds from Company 2 and Company 3. In addition, Company 6 did not provide further information and supporting documents for the highlighted transactions. As a result, the relationships of Company 4, Company 5 and Company 6 with the other companies could not be determined.	
Legal entity type	Private limited companies
Industry	Commodity trading
Jurisdictions involved	Singapore (bank account), South-East Asian country 1 (intermediary companies), East-Asian country, Middle Eastern country and Offshore Company Locations (intermediary companies), South-East Asian country 2 and European country (ultimate beneficial owner)
Type of professionals involved	Bank
Red flags	-Round-tripping pattern -High turn-over of funds within a relatively short period of time without any plausible explanations -Unable to corroborate source of funds -Mismatch between transactions and nature of business -Unclear relationships between “connected” companies
Best practices / lessons learnt	-Obtain information about the customer at on-boarding and on an ongoing basis -Obtain corroborative evidence for the underlying transactions, where transactions are not in line with commonly observed transactions and/or industry practice.

Case 2	
Crime involved (e.g. money laundering, corruption)	
Description of the case:	
Legal entity type	
Industry	
Jurisdictions involved	
Type of professionals involved	
Red flags	
Best practices / lessons learnt	

Case 3	
Crime involved (e.g. money laundering, corruption)	
Description of the case:	
Legal entity type	
Industry	
Jurisdictions involved	
Type of professionals involved	
Red flags	
Best practices / lessons learnt	

Annex 2: Summary of Case Studies

Country	A	B	T	Th	J	H	Kh	D	Dth	R	Z	S	Sh	Ṣ	Ḍ	Ṭ	Total
Number	3	0	1	1	3	3	1	3	1	3	3	2	2	3	0	1	30

Country A

Case No. 1

Misuse of a Joint Stock Company in Real Estate Fraud and Money Laundering through a Multi-Layered Scheme

In the context of urban expansion in the North Coast, a businessman owning 30% of a joint stock company established a luxury residential project that attracted more than 2,000 investors, despite lacking permits and not implementing any construction works. The accused exploited his influence to transfer investors' funds to his personal accounts or to purchase luxury assets inside and outside the country under the names of partners and relatives to conceal ownership. As complaints escalated, a parallel criminal and financial investigation was opened, which uncovered a systematic pattern of transferring and laundering funds. This led to asset freezing and the filing of official charges, including fraud, deception, and money laundering, along with initiating procedures to recover the funds and compensate the victims.

Case No. 2

Financial Camouflage through Consulting Firms and Dormant Accounts in Money Laundering and Investment Fraud Operations

Financial investigations revealed the involvement of a brokerage firm in collecting over USD 60 million from local and foreign investors, under the pretext of investing in the stock market, while the funds were transferred abroad through two consulting firms within complex financial channels indicating money laundering operations. It was found that the company was operating in a fictitious manner without conducting any real trading, and the accused relied on shell ownership structures and dormant bank accounts to gradually move and cycle the funds, which helped him evade banking oversight systems. The joint criminal and financial investigation, supported by foreign financial intelligence units, resulted in the freezing of bank accounts, confiscation of assets, and the filing of official charges including fraud, breach of trust, and money laundering using loopholes in institutional systems.

Case No. 3

Camouflaging Terrorism Financing through a Sole Proprietorship for Import and Export as a Financial Front

A sole proprietorship operating in the field of import and export was identified as receiving large and regular financial transfers from a foreign company based in a high-risk country for money laundering and terrorism financing, which raised suspicions and led to the opening of an official investigation. The investigations revealed that the perpetrator established the business to receive funds from a company owned by an individual listed on terrorist lists, under the pretense of importing goods without any actual commercial activity, and these funds were directed to finance terrorist groups within the country. The security and financial investigations, in cooperation with international entities, led to the freezing of the accounts, the arrest of the accused, and his referral to the judiciary on charges of terrorism financing and money laundering, and the foreign company and its owner were listed among the designated entities.

Country T

Case No. 4

Use of Shell Corporate Structures to Operate Complex Financial Crime and Terrorism Financing Networks Across Multiple Jurisdictions.

A series of investigations revealed that individuals used shell companies and legal fronts to conduct suspicious activities, including money laundering, tax evasion, and terrorism financing through complex company networks registered in multiple jurisdictions or under nominee shareholders to

conceal actual ownership. Methods included large financial transfers to inactive companies, sudden closures without liquidation, recycling funds domestically and internationally as fake loans, and misuse of dormant or import companies as fronts for transferring funds from high-risk entities. The investigations, in cooperation with international entities, uncovered the complex financial structures, froze accounts, seized assets, and led to formal charges for money laundering, tax evasion, and terrorism financing, with suspects added to national and international watchlists.

Country Th

Case No. 5

Use of Shell Companies and Nominee Entities to Commit Financial Crimes and Terrorism Financing Through Superficial Legal Structures and Multi-Channel Transfers

Supervisory authorities uncovered a systematic pattern of using shell and historically registered companies for illegal activities including financial fraud, tax evasion, and terrorism financing, through superficial legal structures lacking any real economic activity. Companies were used to obtain financing and then transfer funds abroad, or use multiple entities to minimize tax liability, or conduct small transfers via outdated bank accounts. Import-export companies also received transfers from high-risk foreign entities benefiting individuals linked to terrorist organizations. Investigations led to the exposure of a network of shell companies and nominees, freezing of bank accounts, seizure of illicit assets, and formal charges of fraud, tax evasion, and money laundering and terrorism financing, alongside the issuance of regulatory measures to strengthen oversight.

Country J

Case No. 6

Use of Legal Companies and Complex Structures to Evade Oversight in Money Laundering, Political Corruption, and Illicit Financing via Fintech and Regulatory Loopholes

Investigations uncovered an organized pattern of using legitimate companies, both existing and newly established, to carry out illegal activities including money laundering, political corruption, and illicit currency trading, through complex ownership structures, digital financial technologies, and regulatory gaps. A foreign investor established eight companies in the country which funneled large sums to a prominent political figure, concealing true ownership through multiple layers of shell companies. Other companies conducted split daily transfers via digital banking Typologies or inactive company accounts to carry out organized criminal activities. Joint security and financial investigations, with regional and international cooperation, identified the real beneficiaries, froze accounts, seized assets, and led to official charges of corruption, money laundering, and illicit financing, with recommendations for legislative reforms to strengthen ownership oversight and company data updates.

Case No. 7

Systematic Tax Evasion in the Energy Sector Using False Records and Complex Corporate Structures to Transfer Profits to Unregulated Accounts with the Help of a Certified Accountant

Tax audits in the energy sector revealed that a petroleum import company engaged in systematic tax evasion over nine years by submitting falsified financial data to hide its actual scale of activity. The company used complex corporate structures, multiple bank accounts, and various trade names to split operations and understate declared profits, aided by a certified accountant who intentionally prepared inaccurate reports. The financial investigation revealed profit transfers to unregulated accounts and identified the actual beneficiaries, leading to the accountant's arrest and legal proceedings against the company management, along with heavy fines and recommendations to tighten oversight over sensitive sectors and enhance electronic reconciliation tools.

Case No. 8

Use of a Licensed Import-Export Company to Transfer Funds from a High-Risk Country to Domestic Terrorist Entities via the Hawala System Without Actual Commercial Activity, in a Hidden Funding Pattern Revealed by Financial Investigations

A financial intelligence unit revealed that a licensed import-export company was used as a front to transfer funds to domestic entities linked to terrorist organizations, through regular financial transfers from a high-risk country without any real commercial activity. The investigations showed the company relied on informal transfer channels such as the hawala system to evade oversight, with the funds

redistributed locally to support entities listed on terrorism sanctions lists. The investigations led to the freezing of bank accounts, seizure of remaining funds, and arrest of company officials, with involved entities listed nationally and internationally, and recommendations to strengthen oversight of companies operating with high-risk countries.

Country H

Case No. 9

Use of a Shell Company in Real Estate Fraud to Collect Funds from Citizens and Transfer Them to Personal Accounts and Luxury Assets in a Coordinated Money Laundering Scheme Through a Non-Existent Housing Project

Investigations into real estate fraud revealed a shell company established by an offender to collect funds from citizens via a fictitious housing project marketed with misleading promotional campaigns, without any real construction. After collecting large sums, the funds were transferred to the personal accounts of the perpetrator and family members and used to purchase luxury assets and conduct international financial transfers, indicating an intent to launder money. Investigations began after victims filed complaints, and financial analysis revealed the money flow, leading to arrests, account freezes, asset seizures, initial compensations, and recommendations to tighten oversight on new real estate development projects.

Case No. 10

Use of an Existing Company Without Updating Ownership Information to Execute Suspicious Transfers and Import Goods for Money Laundering Under a Legal Pretext and Lack of Actual Activity

Investigations revealed that an existing company, purchased without updating ownership information, was used for money laundering operations under legal pretense, despite lacking actual commercial activity. The company was used for suspicious financial transfers and vehicle imports to legitimize illicit funds by selling them and recording them as legitimate revenues. Investigations started after a bank flagged unusual activity, and financial investigations uncovered the absence of commercial documents and systematic transaction fragmentation to evade oversight. Outcomes included the arrest of the new owner, account freezes, asset seizures, and charges of money laundering, violation of trade and currency regulations, along with recommendations to tighten control over company ownership transfers and data updates.

Case No. 11

Use of an existing company without updating the new owner's data to conduct suspicious transfers and import goods to launder money under a legal appearance and in the absence of actual activity.

The Financial Intelligence Unit uncovered a sole proprietorship seemingly licensed for import and export, which was in fact used as a legal front to receive funds from a foreign company linked to terrorist financing, without conducting any actual commercial activity. Investigations showed that the financial transfers, originating from a high-risk jurisdiction, were distributed to individuals and entities connected to terrorist organizations within the country. A financial and intelligence investigation was launched in cooperation with international entities, leading to the arrest of the business owner, freezing of the accounts, and seizure of part of the funds used in financing. The entity was also listed among the prohibited lists, with a recommendation to tighten oversight of sole proprietorships dealing with high-risk foreign entities.

Country Kh

Case No. 12

Use of a multinational network of shell companies to transfer large amounts of money without actual activity through interlinked ownership structures and nominee directors, with the aim of money laundering and concealing beneficial owners.

International financial investigations uncovered a complex network of shell companies established in free zones and multiple countries, used to carry out large financial transfers through fictitious contracts and investments without any actual commercial activity, aiming to launder money

and hide the identities of the beneficial owners. The perpetrators relied on interlinked ownership structures and nominee directors. Old companies with active bank accounts were also used to transfer funds abroad via unconventional means. The investigations resulted in freezing international accounts, closing numerous companies, arresting several individuals, and pressing charges of money laundering and creating shell structures, with recommendations to tighten oversight of company registrations and link them to mechanisms for verifying beneficial ownership.

Country D

Case No. 13

Use of registered consulting companies as legal fronts to transfer suspicious funds without actual activity within fictitious networks in tax havens for the purposes of terrorist financing and money laundering from high-risk sources.

Joint investigations revealed the use of a number of officially registered consulting companies as legal fronts to transfer suspicious funds within money laundering and terrorist financing operations using fictitious legal structures and networks registered in tax havens. These companies received large financial transfers from foreign entities without providing actual services, and the funds were quickly routed to entities abroad. It was confirmed that one of the companies received transfers from a high-risk jurisdiction and directed the funds to individuals linked to terrorist entities. The investigations resulted in the freezing of accounts, confiscation of funds, closure of the involved entities, and listing of the accused on national and international lists.

Case No. 14

Use of forged invoices and fictitious relationship between a local and a foreign company to transfer funds to tax havens within a repeated pattern of tax evasion and trade-based money laundering.

Tax and financial investigations in the country revealed the involvement of a local company in using forged and inflated invoices to import electronic components from a foreign company, aiming to justify large money transfers abroad and recycle them through accounts in tax havens, forming a clear pattern of tax evasion and money laundering. It was found that the owner of the Tunisian company was also the actual controller of the foreign company, using nominee names to conceal the relationship. The investigations resulted in account freezing, opening criminal files, recovering part of the funds, imposing fines, and referring the case to court on charges of forgery, tax evasion, and money laundering.

Case No. 15

Use of outdated companies owned by the same person as fronts to transfer suspicious funds without actual activity, within an organized pattern of money laundering via active accounts and low-transparency destinations.

The Financial Intelligence Unit revealed the use of a group of outdated companies, owned by the same person, as fronts to transfer suspicious funds without any real commercial activity, within a pattern suspected to be part of a money laundering scheme. The active bank accounts of these companies were used to receive and transfer large amounts from domestic and international sources without supporting commercial documents, and the funds were traced to entities in low-transparency jurisdictions. The investigations led to account freezing and referral of the suspect to the prosecution on money laundering charges.

Country Dh

Case No. 16

Use of front companies in free zones and outdated accounts to conduct large financial transfers through fictitious contracts and invoices for the purposes of money laundering and terrorist financing, while concealing the identities of the beneficial owners.

Investigations revealed that a group of individuals used inactive front companies or those registered in low-control free zones to conduct money laundering and terrorist financing operations through large financial transfers not backed by genuine commercial activity. Shell companies, fictitious contracts, and inflated invoices were used to hide the identities of the beneficial owners, and funds were

routed among domestic and foreign entities, including bank accounts of outdated companies. It was also discovered that an import-export company received transfers from unknown sources used as a front to fund terrorist organizations. The investigations led to account freezes, asset seizures, and arrests of several involved parties.

Country R

Case No. 17

Use of newly established companies without actual activity as legal fronts to transfer large funds abroad through complex banking channels and low-transparency countries within a suspected money laundering pattern.

Financial authorities uncovered a network of newly established companies operating without actual business activity, used as legal fronts to transfer large sums abroad through complex banking channels, in a pattern suspected to be related to money laundering. The suspects created companies in various sectors without invoices or documented transactions, and these companies received external transfers before either shutting down or moving the funds to accounts in low-transparency countries. The investigations resulted in freezing the accounts, initiating legal proceedings against the company owners, and administratively shutting down some of the entities.

Case No. 18

Use of companies registered under nominee relatives to conceal the real beneficial owner and obtain government contracts and transfer funds abroad, within a coordinated pattern of .evasion, concealment, and money laundering

Investigations uncovered that a businessman registered several commercial companies under the names of relatives to conceal his identity as the beneficial owner and maintain actual control over operations, allowing him to obtain government contracts and major projects through fictitious legal fronts. These companies were later used to transfer funds to foreign entities without showing any direct legal affiliation. The investigations showed that financial decisions and instructions were issued by him, despite the absence of his name in official documents. The results included opening legal cases on charges of forgery, non-disclosure, and money laundering, along with freezing accounts and canceling suspicious contracts.

Case No. 19

Use of inactive and shell companies with active accounts to transfer illicit funds and finance terrorism, in the absence of actual activity and amid regulatory failure to update data and monitor sensitive sectors.

Investigations revealed the abuse of inactive and shell companies in executing illicit fund transfers, including money laundering and terrorist financing, leveraging active bank accounts despite lacking business activity. One company had not updated its data in over five years but continued receiving and transferring funds domestically and internationally, while another, seemingly operating in the food sector, served as a front to transfer funds to entities linked to terrorist organizations. The investigations resulted in account freezes, confiscation of funds, and prosecution of the suspects, with recommendations issued to suspend inactive accounts and reinforce verification of companies' actual operations, particularly in high-risk sectors.

Country Z

Case No. 20

Use of shell companies and fictitious structures to transfer funds via fake investments and government contracts, to conceal the beneficial owner and obscure the source in a repeated pattern of money laundering.

A series of financial investigations uncovered a repeated pattern of using shell or inactive companies as legal fronts to transfer large sums of money domestically and abroad, through fictitious ownership structures designed to hide the real beneficial owner and obscure the origin of the funds. A businessman established these companies in the names of relatives and former employees and obtained fake government contracts and investments, with the money later routed to foreign companies without visible legal ties. The investigations led to freezing accounts, arresting those involved, and initiating proceedings on charges of money laundering and fraud, with recommendations to strengthen verification of actual business activity and beneficial ownership when registering companies.

Case No. 21

Use of an old inactive company to conduct suspicious financial transfers without actual activity or updated data, within a money laundering pattern through accounts linked to high-risk countries.

As part of monitoring bank accounts linked to inactive companies, financial authorities uncovered the abuse of an old company that had not conducted any activity for over five years in executing large financial transfers without updated legal or accounting records, raising suspicions of money laundering. Investigations revealed the absence of any real economic activity and linked the money flows to local and international accounts, some located in high-risk countries, confirming the use of the company as a front to move suspicious funds. This led to account freezing and opening of criminal investigations, along with supervisory recommendations to close unused accounts and regularly update data of inactive companies to prevent their misuse in illicit activities.

Case No. 22

Use of an import-export company as a front to transfer funds from unknown sources to entities linked to terrorist financing, in the absence of commercial activity and with multiple accounts linked to listed entities.

As part of efforts to monitor high-risk financial transfers, authorities discovered suspicious activity from a registered company in the import-export sector, which received large transfers from unknown foreign sources without any real commercial activity or supporting documentation, raising suspicions about its use as a front to transfer funds to entities suspected of terrorist financing. Investigations confirmed the absence of genuine economic activity and revealed that funds were distributed to accounts linked to entities and individuals listed on terrorism watchlists, resulting in account freezing, asset confiscation, and closure of the company, as well as initiating a criminal case against those responsible, with recommendations to tighten supervision over inactive companies or those lacking clear operational data.

Country S

Case No. 23

Use of shell companies in service sectors as fronts for large financial transfers from foreign sources, through fake invoicing and pricing, with central coordination revealed by digital and financial investigations and international cooperation.

The Financial Intelligence Unit uncovered a network of shell companies established in sectors such as import, services, and consulting without any real commercial activity, used to receive large financial transfers from foreign sources without clear economic justification, and the funds were then quickly redirected to foreign accounts. Parallel investigations revealed centralized coordination between these companies, all linked to one businessman, through analysis of transfer patterns, IP addresses, and digital signatures. Fake invoices and false pricing were used to justify the funds, in coordination with international authorities. The findings led to freezing related accounts and referring the case to the public prosecution to open criminal investigations against those involved.

Case No. 24

Use of old and fictitious companies with active accounts to move illicit funds and finance terrorism, within a repeated pattern uncovered by financial and security investigations in coordination with judicial authorities.

Financial and security authorities identified a repeated pattern of using outdated or fictitious companies as legal fronts to move illicit funds, including financing of terrorist-designated entities, where their active bank accounts were misused to receive and transfer large funds without real commercial activity or supporting documents. Parallel and security investigations revealed connections between these entities and suspicious financing networks. Coordination with judicial authorities resulted in freezing the accounts, seizing the funds, and launching criminal proceedings against those involved. The case concluded with recommendations to suspend outdated accounts and tighten due diligence requirements for companies in high-risk sectors like import-export.

Country Sh

Case No. 25

Use of an organized money laundering network involving shell companies registered under nominee names and circular ownership structures in technology and financial service sectors, used to conceal beneficial owners and move funds through fictitious domestic and international transactions.

Extensive financial investigations uncovered a complex money laundering network based on the use of old and shell companies registered under nominee names and organized within circular and interlinked ownership structures domestically and internationally, to mislead regulators and conceal beneficial owners. These companies, especially in technology and financial services, were used as legal fronts to receive large external transfers under the guise of fake services and investments, then redistribute the funds via local and foreign bank accounts. Parallel investigations confirmed the absence of any real business activity, relying on analysis of ownership, contracts, and bank transfers, in cooperation with international authorities. The results included freezing bank accounts and opening criminal investigations, with recommendations to tighten transparency requirements in company structures and mandatory disclosure of beneficial owners.

Case No. 26

Use of shell companies for real estate fraud and terrorist financing through lack of licenses, financial camouflage, and fictitious ownership structures to hide real beneficiaries and obstruct supervision.

Competent authorities uncovered cases involving shell companies in criminal activities, the first being a real estate fraud operation via a fictitious development company that collected funds from over 2,000 citizens without carrying out any real project, using the funds to purchase assets and make personal transfers. The second case involved a network of unlicensed exchange companies operating in unsupervised areas and used to finance terrorist organizations through complex financial transfers. Investigations revealed lack of licenses, misuse of accounts, and use of fictitious structures to conceal beneficiary identities. Actions included arresting suspects, freezing accounts, and closing non-compliant offices, with recommendations to tighten oversight of real estate and money remittance sectors.

Country Ş

Case No. 27

Use of a fictitious real estate company to transfer funds of unknown origin abroad by hiding the beneficial owner and lacking actual activity, within a complex pattern of money laundering and regulatory evasion.

Regulatory authorities uncovered a real estate company officially registered that had not executed any real project since its establishment, despite receiving large financial transfers from unknown sources, which were later routed to foreign bank accounts without legitimate justification. Investigations revealed the company was registered under a nominee with no connection to management, while the real beneficiary remained unidentified, aiding in concealing the perpetrators' identities and complicating fund tracing. The case was initiated following a bank report of unusual transfers, leading to account freezing and opening of a criminal investigation, with recommendations to strengthen supervision over real estate investment companies, requiring them to submit regular operational reports and identify real beneficiaries to ensure transparency and prevent money laundering.

Case No. 28

Use of complex ownership structures and multinational companies to conceal the beneficial owner and circulate funds through different jurisdictions without actual activity, aiming to mislead investigations and launder funds.

Regulatory authorities uncovered a complex network of multi-layered companies created across multiple jurisdictions, including tax havens, aiming to conceal the identity of the beneficial owner and mislead financial investigations. Inactive companies with open bank accounts were used to channel funds without real commercial activity through fictitious contracts and investments. The perpetrator relied on a convoluted ownership web to circulate funds between connected entities, making it difficult to trace their original source. Parallel financial investigations confirmed the absence of any legal or economic justification for these operations, resulting in account freezes, asset seizures, and the opening of criminal investigations. Authorities recommended tightening disclosure requirements for ownership

structures and real beneficiaries, and enhancing integration between commercial and banking registries to ensure transparency and prevent misuse of legal entities.

Case No. 29

Use of unlicensed exchange networks and informal remittance systems for terrorist financing and fund transfers without oversight or documentation amid weak regulatory and supervisory frameworks.

Security and financial investigations revealed a network of unlicensed exchange and remittance companies operating outside legal frameworks, involved in transferring funds to unknown entities, some linked to terrorist organizations listed on national and international watchlists. These companies received large financial transfers without official records or transaction documentation, using informal systems such as hawala, which hindered fund tracking. Investigations led to raids, seizure of equipment and documents, and freezing of related bank accounts, along with arrests of those involved. Authorities recommended tightening licensing conditions, reorganizing the exchange sector, and strengthening supervision to prevent its abuse in terrorist financing and illicit activities.

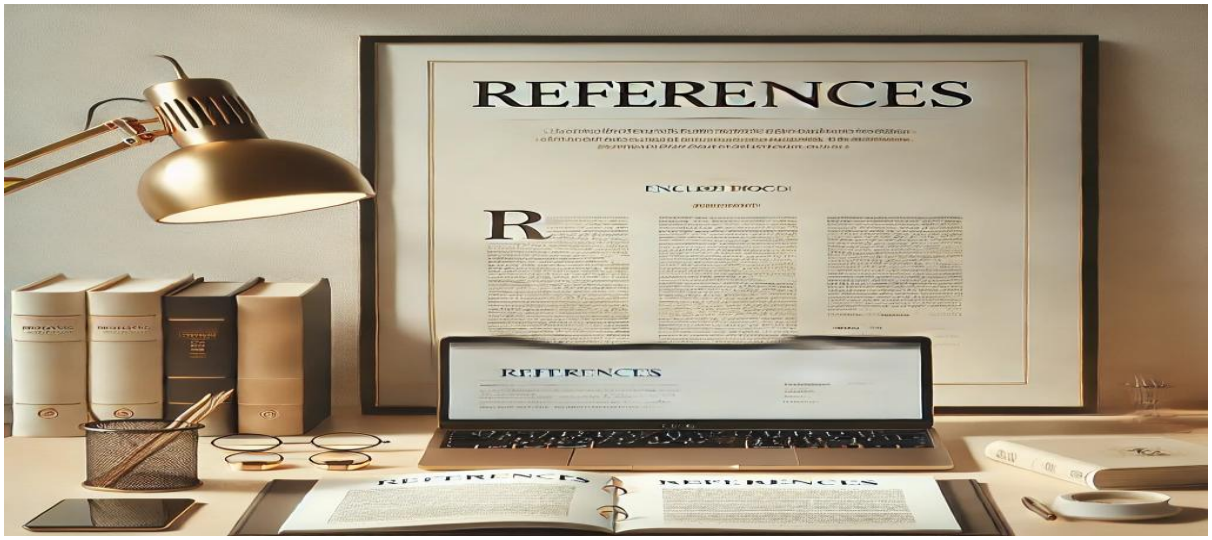
Country Ṭ

Case No. 30

Use of an organized shell company network and interlinked ownership structures for money laundering and terrorist financing through unlicensed entities and fictitious fronts to hide real beneficiaries and transfer funds via multiple fake transactions.

Regulatory and security authorities uncovered a complex network of shell and unlicensed companies systematically used for money laundering and terrorist financing, including inactive import and trading companies, entities registered under nominee names, and active accounts of old companies, along with unlicensed remittance companies. Large amounts of money from unknown sources were routed abroad through fake transactions and interlinked ownership structures created to conceal the real beneficiaries. Investigations, launched after suspicious bank reports, employed financial and intelligence analysis tools and uncovered widespread manipulation of ownership structures and involvement in financing terrorist networks domestically and abroad. The results included account freezes, closure of involved companies, and opening of criminal files, with recommendations to strengthen supervision, require full disclosure of real beneficiaries, and enhance coordination among relevant authorities to combat illicit activities.

References



International Reports and Official Organizations

- Europol. (2020). Financial Crime Threat Assessment. The Hague, Netherlands: Europol.
- FATF & Egmont Group. (2022). Trade-Based Money Laundering – Trends and Techniques. Paris, France: FATF & Egmont Group.
- FATF. (2018). The Role of Professional Money Launderers. Paris, France: FATF.
- FATF. (2019). Best Practices on Beneficial Ownership for Legal Persons. Paris, France: FATF.
- FATF. (2019). Terrorist Financing Through the Non-Profit Sector. Paris, France: FATF.
- FATF. (2020). Trade-Based Money Laundering (TBML): Trends and Developments. Paris, France: FATF.
- FATF. (2021). Misuse of Legal Persons and Arrangements for Money Laundering and Terrorist Financing. Paris, France: FATF.
- FATF. (2021). Money Laundering Through the Automotive Sector. Paris, France: FATF.
- FATF. (2022). Money Laundering and Terrorist Financing Through the Real Estate Sector. Paris, France: FATF.
- Financial Action Task Force (FATF). (2014, updated 2023). Guidance on Transparency and Beneficial Ownership. Paris, France: FATF.
- Global Financial Integrity (GFI). (2021). Illicit Financial Flows and Trade Mispricing. Washington, DC: GFI.
- OECD. (2018). Ending the Shell Game: Cracking Down on the Use of Companies for Tax Crimes and Money Laundering. Paris, France: OECD.
- OECD. (2021). Global Forum on Transparency and Exchange of Information for Tax Purposes. Paris, France: OECD.
- Transparency International. (2021). Assessing Beneficial Ownership Transparency in Corruption Cases. Berlin, Germany: Transparency International.

- UNODC. (2019). Money Laundering Through Trade and Corporate Entities. Vienna, Austria: UNODC.
- UNODC. (2021). Global Report on Corruption and Corporate Crime. Vienna, Austria: UNODC.
- World Bank. (2011, updated 2020). The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets. Washington, DC: World Bank.

Additional Links and Online Sources

- https://www.federalregister.gov/documents/2022/09/30/2022-21020/beneficial-ownership-information-reporting-requirements
- https://www.transcrime.it/en/publications/csabot-beneficial-owners-of-european-companies/
- https://ebra.be/wp-content/uploads/2021/10/EBOCSIII.WP1_Final-Project-Report.pdf
- https://www.taxjustice.net/wp-content/uploads/2019/01/Beneficial-ownership-verification_Tax-Justice-Network_Jan-2019.pdf
- https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html
- https://taxjustice.net/2023/02/07/roadmap-to-effective-beneficial-ownership-transparency-rebot/
- https://www.fatf-gafi.org/en/publications/Methodsandtrends/Concealment-beneficial-ownership.html
- https://www.abc.com.py/policiales/2023/07/20/aparece-el-primer-rostro-conectado-a-la-megacarga-de-cocaina-incautada-en-alemania/
- https://panamapapers.sueddeutsche.de/articles/5718f882a1bb8d3c3495bcc7/
- https://taxjustice.net/wp-content/uploads/2022/07/Trusts-FATF-R-25-1.pdf
- https://taxjustice.net/wp-content/uploads/2019/10/The-transparency-risks-of-investment-entities-working-paper-Tax-Justice-Network-Oct-2019.pdf
- https://star.worldbank.org/publications/signatures-sale-how-nominee-services-shell-companies-are-abused-conceal-beneficia
- https://www.globalwitness.org/en/blog/three-ways-uks-register-real-owners-companies-already-proving-its-worth/
- https://www.globalwitness.org/en/campaigns/corruption-and-money-laundering/anonymous-company-owners/companies-we-keep/
- https://elibrary.worldbank.org/doi/abs/10.1596/978-0-8213-8894-5
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/434546/bis-15-320-enhanced-transparency-of-company-beneficial-ownership-enactment-impact-assessment.pdf
- https://taxjustice.net/2020/07/06/exploring-uk-companies-legal-ownership-chains-to-detect-red-flags-and-verify-beneficial-ownership-information/
- https://taxjustice.net/wp-content/uploads/2022/02/Complex-ownership-chains-Reduced-Andres-Knobel-MB-AK.pdf
- https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf
- https://taxjustice.net/wp-content/uploads/2022/12/State-of-Play-of-Beneficial-Ownership-2022-Tax-Justice-Network.pdf
- https://www.bnm.md/files/Kroll_%20Summary%20Report.pdf.