مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

GUIDANCE FOR LICENSED FINANCIAL INSTITUTIONS ON RISKS RELATED TO TRADE-BASED MONEY LAUNDERING ("TBML") AND TRANSSHIPMENT

26 November 2025

CentralBankUAE
CentralBankUAE
Central Bank of the UAE
CentralBankoftheUAE
Central Bank of the UAE
المصرف–المركزي.امارات
www.centralbank.ae
Central Bank of the UAE:
Download on the App Store
GET IT ON Google Play
المصرف-المركزي.امارات
www.centralbank.ae

AGENDA

1. Purpose, Applicability and Legal Basis
2. Trade and Service-Based Money Laundering
3. Illicit Transshipment
4. Mitigating Factors and Controls
5. International Trade and Trade Finance
6. Q&A

Purpose and Applicability of the Guidance

Purpose

- This Guidance does **NOT** constitute new regulation and does **NOT** introduce new legal obligations.
- It is designed to help CBUAE's LFIs understand the purpose and context of their existing legal obligations, as well as the CBUAE's expectations for how those obligations will be fulfilled.
- LFIs are expected to demonstrate compliance with requirements of the Guidance within one month from its coming into effect.

Applicability

The guidance document applies to **all natural or legal persons that are licensed and/or supervised by the CBUAE** in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, investment companies, payment service providers, virtual asset service providers, payment service providers, registered hawala providers ("RHPs"); and
- Insurance companies, agencies and brokers.

Legal Basis

- **Federal Decree-Law No. (6) of 2025**, Regarding the Central Bank, Regulation of Financial Institutions and Activities, and Insurance Business [which repealed Federal Decree-Law No. (14) of 2018, Regarding the Central Bank & Organization of Financial Institutions and Activities, and its amendments ("CBUAE Law")]

- **Federal Decree-Law No. 10 of 2025**, Regarding the Combating Money Laundering, the Financing of Terrorism, and the Financing of Arms Proliferation. [which repealed Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended ("AML-CFT Law")]

- **Cabinet Decision No. (10) of 2019** concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as amended by Cabinet Decision 24 of 2022 ("AML-CFT Decision") and its amendments.

- **Cabinet Decision No. (74) of 2020** Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74"), and its amendments.

- **CBUAE/BSD Notice No. 1943.2022** Regarding AML/CFT Minimum Standards and Supervisory Expectations.

Increasing Global Trade Volume and the Role of the U.A.E. as a Trading Hub

- Global trade has grown significantly in recent years, reaching a record value of over USD 32 trillion in 2022.
- Ranked as the 11th country in commodity exports in 2022, the U.A.E. is a major trading hub in the Middle East and globally.
- As the volume of trade activities increased in the U.A.E., Licensed Financial Institutions (“LFIs”) in the country are increasingly exposed to global trade by:
    - Providing financing (credit) through trade finance products, and
    - Settling payments for trade transactions, sometimes on an open account.
- The products, services, and customers associated with international (and also domestic trade) exposes the LFIs to TBML.

Trade and Service-Based Money Laundering

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Trade-Based Money Laundering

The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins

TBML Typologies

- Over-and Under-Invoicing of Goods and Services
- Over and Under Shipment of Goods and Services
- Multiple Invoicing of Goods and Services
- Falsely Described Goods and Services
- Use of Shell, Front, or Shelf Companies
- Use of Free Trade Zones
- Illicit Cash Integration
- Third Party Intermediaries
- Back-to-Back Letters of Credit
- Fictitious Documents
- Accounts Used as Pass Through
- Use of RHPs and Alternative Remittance Systems

TBML Typologies

Over and Under Invoicing of Goods and Services

- Illicit actors **misstate the price of goods/services** to transfer value across borders, often requiring collusion between buyer and supplier.
- **LFIs can detect** this by comparing invoice prices to market values using external sources, especially in commodities trading.
- **Example**: A criminal organization under-invoices 1,000 electronic widgets at AED 5,000 each (market value AED 6,000), transferring AED 1 million in value to the buyer.

Over and Under Shipment of Goods and Services

- Value is transferred by **misrepresenting the quantity of goods shipped**, including phantom shipments where no goods are sent.
- LFIs should cross-check quantities across trade documents and **assess consistency** with customer profiles.
- **Example**: Company A ships only 5,000 of 10,000 laptops invoiced, transferring AED 22.5 million in value to Dubai.

TBML Typologies

Multiple Invoicing of Goods and Services

- The same shipment is invoiced multiple times to different financial institutions to receive multiple payments.
- LFIs should scrutinize invoice authenticity and look for anomalies or duplications in documentation.
- **Example**: Company A issues two invoices for the same banana shipment to Companies B and C, laundering AED 150,000.

Falsely Described Goods and Services

- Goods are misrepresented in quality or type, often to disguise controlled or restricted items.
- LFIs should request attestations or further documentation when red flags suggest misdescription.
- **Example**: Company A ships silver worth AED 2.75 million but declares it as bronze worth AED 32,000.

TBML Typologies

Use of Shell, Front, or Shelf Companies

- These entities obscure the true beneficiaries and complicate transaction tracing, **often used by sanctioned or corrupt actors**.
- LFIs should apply strong CDD/KYC and monitor for unusual patterns like dormant accounts suddenly becoming active.
- **Example**: A shell company inflates prices on government contracts to siphon profits through trade.

Use of Free Trade Zones

- FTZs offer reduced oversight and are exploited for smuggling, mislabeling, and re-exporting restricted goods.
- LFIs should assess the rationale for FTZ use and evaluate counterparties' legitimacy and geographic risk.
- **Example**: Navigation equipment is re-exported from an FTZ disguised as kitchen appliances to evade export controls.

TBML Typologies

Illicit Cash Integration

- Criminals **integrate illicit cash into trade** through non-bank institutions, offsetting schemes, or legitimate supply chains.
- LFIs should monitor for unusual cash flows and file reports when suspicious integration methods are detected.
- **Example**: A supermarket owned by a criminal group aggregates drug proceeds via fake POS transactions and uses them to pay for illicit imports.

Third Party Intermediaries

- Unrelated third parties settle trade invoices, often from offshore jurisdictions, to obscure the transaction trail.
- LFIs should question third-party involvement and verify economic justification and documentation consistency.
- **Example**: Company C pays for goods delivered to Company B, raising red flags due to offshore incorporation and inconsistent documentation.

TBML Typologies

Back-to-Back Letters of Credit

- Two LCs are used to conceal the original buyer or seller, often to evade sanctions or obscure fund flows.
- LFIs should conduct due diligence on intermediaries and monitor for rapid, similar-value fund movements.
- **Example**: A broker uses back-to-back LCs to hide the origin of sanctioned oil from Country A, disguising it as originating from Country B.

Fictitious Documents

- Fake or altered trade documents are used to justify illicit fund transfers, often undetectable without red flags.
- LFIs should compare documents for inconsistencies and build internal repositories for document verification.
- **Example**: Company B submits a fake invoice and forged export declaration to support a suspicious wire transfer.

TBML Typologies

Accounts Used as Pass Through

- Accounts are used solely to layer funds and complicate tracing, often in low-risk jurisdictions.
- LFIs should investigate unnecessarily complex transactions and unjustified intermediaries or currency exchanges.
- **Example**: A fake logistics company receives regular payments and provides fake invoices to justify fund transfers.

Use of RHPs and Alternative Remittance Systems

- Hawala and informal systems are used to disguise trade payments, especially when misrepresenting personal remittances.
- RHPs must perform CDD/KYC and verify the legitimacy of business-related transactions.
- **Example**: A hawala network is used to transfer payments for counterfeit goods disguised as family remittances.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Service-Based Money Laundering

The process of disguising the proceeds of crime and moving value by exploiting the trade of services or other intangibles, such as information.

The **intangible nature of services makes it difficult to detect anomalies** in the price of services offered and to prove whether such services have been provided.

Example: A strategic consulting firm located in Country A billed hundreds of hours of advisory services to a company in Country B. The ultimate beneficial owner of both companies was the same person, who was a professional money launderer. Using the consulting firm, the owner transferred large amounts of funds moved from Country B to Country A without being suspected of any wrongdoing.

Vulnerable Economic Sectors

Illicit Transshipment

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Illicit Transshipment

Transshipment involves routing goods through intermediate destinations before reaching the final destination. While often legitimate, it can be exploited to evade sanctions and export controls.

Illicit transshipment involves embargoed or sanctioned jurisdictions.

- **Embargoed jurisdictions**: Certain countries that are subject to embargoes have a comprehensive or near comprehensive prohibition on any export or reexport to such country.
- **Sanctioned jurisdictions**: Countries facing unilateral or multilateral sanctions have numerous categories of goods and services that cannot be provided to, or sourced from, such country.

Common Illicit Transshipment Techniques

- **An illicit actor ships goods from a sanctioned country to a non-sanctioned location**. Illicit actors first ship goods originating in a sanctioned country to a non-sanctioned location. The illicit actors then ship these goods to a third location, with the underlying documentation showing the non-sanctioned location as the country of origin. Sometimes the re-exporter repackages the goods or adds non-sanctioned country seals of origin to the packaging to further obscure the true origin.

- **An illicit actor located in a jurisdiction with fewer export restrictions imports goods, allegedly for use in the country**. An illicit actor located in a jurisdiction with fewer export restrictions imports goods, allegedly for use in the country. The illicit actor then forwards the goods to either prohibited end-users (i.e., users blacklisted by the countries where the goods originated) or to embargoed or sanctioned countries. Often such schemes involve networks of import/export companies registered in jurisdictions world-wide, with goods travelling across multiple jurisdictions before they reach the prohibited end-user or destination.

Common Illicit Transshipment Techniques

- **An illicit actor located in a country susceptible to corruption imports goods controlled for export**. An illicit actor (e.g., import/export company) located in a country susceptible to corruption imports goods. The illicit actor then uses government connections to mislabel the goods or forge customs declarations and reexport goods to a prohibited destination.

- **An illicit actor establishes another company in a third jurisdiction**. An illicit actor subject to sanctions or export control restrictions establishes a company in a third jurisdiction. To disguise the connection, the non-restricted company is registered in the name of residents of the third country and bears a generic name. The company is then used as a transshipment hub, accumulating export controlled or restricted goods and moving them to the prohibited parent company.

- **An illicit actor "peels" part of a shipment while transshipping**. An illicit actor "peels" part of a shipment while transshipping to another non-sanctioned country; as in, the illicit actor delivers a shipment while passing through a sanctioned country (e.g., when a vessel docks in a port in a sanctioned country while enroute to another location).

Common Illicit Transshipment Techniques

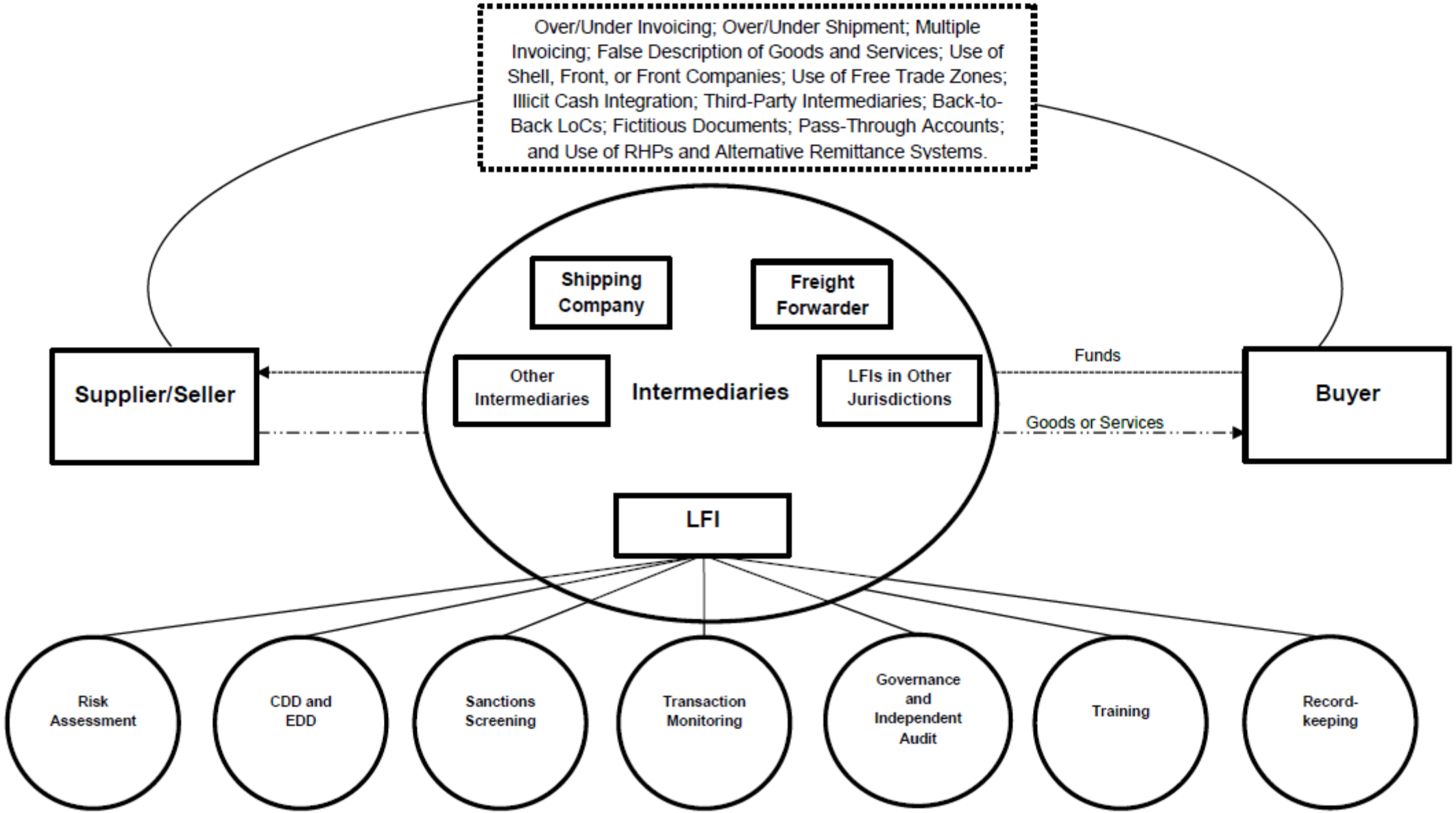
- **An illicit actor exports or reexports under the disguise of transshipment**. An illicit actor exports or reexports under the pretense of transshipment. An illicit actor located in a landlocked country states that it has to ship the goods via a sanctioned country due to difficulties arranging other routes, while in fact, the country in question is the final destination of the goods.

Due to its strategic location and trade volume, the U.A.E. is particularly vulnerable to transshipment abuse, especially involving nearby sanctioned jurisdictions.

LFIs should also consider risks related to landlocked countries. Without direct access to coastal ports, landlocked countries must rely on transit countries to connect them with international markets. Sometimes such transit countries can be subject to restrictive sanctions or export controls, increasing the risk of potential non-compliance for an LFI.

Mitigating Factors and Controls

Mitigating Factors and Controls


Over/Under Invoicing; Over/Under Shipment; Multiple Invoicing; False Description of Goods and Services; Use of Shell, Front, or Front Companies; Use of Free Trade Zones; Illicit Cash Integration; Third-Party Intermediaries; Back-to-Back LoCs; Fictitious Documents; Pass-Through Accounts; and Use of RHPs and Alternative Remittance Systems.
Shipping Company
Freight Forwarder
Supplier/Seller
Other Intermediaries
Intermediaries
LFIs in Other Jurisdictions
Funds
Goods or Services
Buyer
LFI
Risk Assessment
CDD and EDD
Sanctions Screening
Transaction Monitoring
Governance and Independent Audit
Training
Record-keeping

Mitigating Factors and Controls

Enterprise-wide Risk Assessment and Risk-based Approach

- LFIs must identify, assess, and understand ML/TF risks, **including those related to trade**, and apply proportionate AML/CFT measures.
- Risk assessments should cover customers, intermediaries, geographies, products/services, delivery channels, and operations.
- **Trade-related risks** should be evaluated through standalone assessments or integrated into enterprise-wide frameworks.
- LFIs must document, regularly update, and report risk assessments to senior management.
- Risk assessments should be dynamic, reflecting changes in business operations, customer base, and external threats.

Mitigating Factors and Controls

CDD and EDD Measures

General CDD Measures

- LFIs must conduct CDD at onboarding and throughout the customer relationship, including identifying beneficial owners.
- CDD should establish the nature of the customer's business, **trade activities**, and expected transaction behavior.
- LFIs must screen customers and related parties against sanctions lists and internal watchlists.
- Any material misrepresentation by a customer should lead to rejection, exit, and reporting to the FIU.
- **Ongoing monitoring** is required to detect deviations from expected behavior and update CDD records accordingly.

EDD Measures for Heightened Trade-related Risks

- EDD is mandatory for PEPs, high-risk countries, and correspondent relationships; it is also expected for **high-risk trade scenarios**.
- LFIs should identify dual-use or high-risk goods and screen for vague or suspicious descriptions.
- **Additional steps** may include verifying source of funds, reviewing vessel data, and using third-party authentication services.
- Open account trade and complex goods require enhanced scrutiny and possibly tailored due diligence questionnaires.
- Ongoing monitoring should detect changes in customer behavior and trigger further CDD or EDD as needed.

Mitigating Factors and Controls

Targeted Financial Sanctions Obligations

- LFIs must screen customers and transactions against the UAE Local Terrorist List and the UN Consolidated List.
- **Screening should include** SWIFT messages, trade documents, and all relevant parties in a transaction.
- Confirmed matches require immediate freezing of assets and reporting via the goAML Confirmed Name Match Report (CNMR).
- Partial matches must be escalated and reported as Partial Name Match Reports until resolved.
- LFIs should consider including sanctions clauses in trade finance instruments to allow non-payment in case of a true sanctions hit.
- LFIs should ensure an employee cannot proceed with a trade-related transaction unless an appropriate screening unit within the LFI has cleared all sanctions-related alerts.

Mitigating Factors and Controls

Transaction Monitoring and Suspicious Transaction/Activity Reporting

Transaction Monitoring

- LFIs must monitor all transactions to ensure consistency with customer profiles and detect suspicious activity.
- **Monitoring systems should be risk-based, scalable, and capable of handling trade-specific risks and typologies.**
- Automated systems are preferred, but smaller LFIs must ensure effective manual or hybrid controls.
- External data (e.g., vessel routes, commodity prices) can enhance monitoring effectiveness.
- Monitoring should be regularly tested and updated to reflect evolving risks and customer behavior.

Suspicious Transaction/Activity Reporting

- LFIs must file STRs/SARs when they suspect transactions involve criminal activity or TBML.
- Investigations should include reviewing CDD, trade documents, open-source intelligence, and transaction history.
- STRs should also be filed for high-risk behaviors like refusal to provide information or unexplained trade structures.
- Filing STRs supports law enforcement in identifying and disrupting financial crime networks.
- LFIs should consult the CBUAE's STR guidance and use the goAML platform for submissions.

Mitigating Factors and Controls

Governance and Independent Audit

- AML/CFT programs must be supported by strong governance and the “three lines of defence” model.
- Senior management must oversee and support AML efforts, including TBML and transshipment risk management.
- Compliance teams must have independence, authority, and resources to operate effectively.
- Independent audits should regularly assess the design and effectiveness of AML controls.
- Audit findings must be reported to senior management and followed by remediation of identified gaps.

Mitigating Factors and Controls

Training

- LFIs must implement tailored training programs based on their risk profile and exposure to TBML and transshipment.
- Training should be current, periodic, and include real-life case studies and emerging red flags.
- All relevant staff, especially those in high-risk roles, must receive training.
- Training should cover internal controls, reporting obligations, and suspicious activity detection.
- Attendance and knowledge assessments should be documented and refreshed regularly.

Mitigating Factors and Controls

Record-keeping

- LFIs must retain records of risk assessments, CDD, transactions, and STRs for at least five years.
- Records must be organized to allow for transaction reconstruction and regulatory access.
- Trade-related documents should be stored in structured databases to support AML/CFT and TFS compliance.
- Records must be made available to competent authorities upon request.

International Trade and Trade Finance

Trade Finance Products

Non-Documentary Trade Finance Products & Open Account Trade

- Financial products related to trade transactions that requires a smaller subset of documents, if any.
- **Open Account Trade:** When the supplier ships goods to the buyer and the corresponding documents are exchanged directly between them, followed by a bank transfer to settle the balance.
- **Import and Export Factoring:** The process of purchasing account receivables from a supplier/exporter in one country and collecting the invoice value later from the buyer/importer in the second country.
- **Forfaiting**: Akin to factoring except that the LFI assumes the risk of non-performance.
- **Structured Trade Finance:** Financing provided to parties to trade transactions to cover the costs during the production and delivery.
- **Countertrade:** A reciprocal form of international trade in which goods or services are exchanged for other goods or services rather than for hard currency.

Trade Finance Products

Documentary Trade Finance Products

- Performance or non-performance based, in which the payment related to trade is due once the documents proving performance of lack of performance are presented.
- **Letters of Credit (LC)**: A letter from an LFI guaranteeing that the LFI will make a full payment to the supplier once the supplier presents the documents that confirm their performance and that would allow the buyer to receive the ownership of goods and services.
- **Standby LC**: A secondary payment method which will only be called upon when one of the parties to a standby LC fails to perform against their contractual obligations in a trade.
- **Bank Guarantee**: An undertaking from an issuing LFI to pay to a beneficiary if one of the parties to a contract has failed to perform against their contractual obligations in a trade. Bank guarantees have a wider application compared to standby LCs and are not limited to securing a performance under a trade-related transaction.
- **Types of documents available**: Air waybill, bill of lading, certification of inspection/quality, certificate of origin, customs bond, insurance certificate, invoice, packing list, contract, etc.

Trade Finance Products Vulnerabilities

LC and Bank Guarantee Vulnerabilities

- LCs and bank guarantees are especially vulnerable to the risk of TBML as they can create the illusion of legitimacy for an otherwise illicit transaction. At the same time, LCs involve the most detailed documentation that an LFI may collect under a trade transaction (bank guarantees may have less detailed documentation), allowing LFIs to carefully review the transactions for suspicious activity, red flags indicating TBML, or indicators of potential sanctions evasion.

Trade Finance Products Vulnerabilities

Open Account and Cash In Advance Vulnerabilities:

- Considering hundreds of millions of wire transfers processed by global banks daily, it may be hard for an LFI to identify trade conducted on an open account, even in instances where the transfer references an invoice or a type of good. Thus, manual intervention and review becomes impossible unless a transaction triggers an alert, e.g., in case of a transaction monitoring or sanctions or watch list screening that would then allow an analyst to review the payment and request supporting documentation, if necessary.
- Thus, millions of transactions a day are settled on open account between buyers and sellers without any oversight from LFIs. While the majority of such settlements do not relate to any illicit activity, some illicit actors will abuse trade on open account and may even conduct test transactions to verify if certain types of transfers may trigger compliance review from various banks.

Trade Finance Products Vulnerabilities

Import and Export Factoring Vulnerabilities

- An Import/Export Factoring Company may undertake less stringent CDD/KYC and trade-related controls than a typical bank. Factoring Companies also often advertise their services as an alternative to banking, targeting companies that may have previously been denied banking services (although under banking may be caused by numerous reasons unrelated to illicit activity).
- A bank or an Import/Export Factoring Company participating in a transaction will receive fewer documents than in a documentary trade transaction. The documents may be limited to, for example, an invoice and a bill of lading, making it difficult to understand the trade transaction and all the parties and goods involved in the underlying trade activity.

Import and Export Factoring Vulnerabilities

- Similar to factoring, a forfaiting company will have limited visibility into the underlying trade transaction and would collect fewer documents than in a documentary trade finance. Thus, a forfaiting company is unlikely to detect illicit activity.

Trade Finance Products Vulnerabilities

Structured Trade Finance Vulnerabilities

- **Warehouse Financing Vulnerabilities**: LFIs that engage in warehouse financing should pay attention to the valuation of the inventory in trade since over-valuation may be used by illicit actors to gain funds that would otherwise not be available to them. Similarly, warehouse financing may be used to cover “phantom shipments”, referred to in Section 2.2.2. Over- and Under-Shipment of Goods and Services, and/or involve commodities trade, which is particularly susceptible to TBML. LFIs should consider conducting additional due diligence on the warehouse(s) and the supplier of the goods to make sure they are legitimate and operating businesses. Finally, in warehouse financing, the financing LFI may have little visibility into the origin of the goods or the underlying documentation that supports the trade transaction.
- **Pre-Export Finance Vulnerabilities**: In pre-export finance, an LFI has visibility only into one aspect of a trade transaction (i.e., activities by a borrower before shipment of goods). Therefore, in this scenario, it is harder for an LFI to identify any red flags or verify whether the borrower used the financing for the specified purpose. Thus, CDD/KYC measures play a particularly important role in pre-export finance, as further discussed in Section 4.2. CDD and EDD Measures.

Trade Finance Products Vulnerabilities

Countertrade Vulnerabilities

- Countertrade is the least transparent form of a cross-border trade since the parties do not involve any LFIs, and thus, are not subject to CDD/KYC, transaction monitoring or other transaction checks. It may also take place in a country with weak AML/CFT and recordkeeping regulations, making it nearly impossible to reconstruct the transaction or understand the parties involved.

Annex 1. TBML and Illicit Transshipment Red Flags

- Red flags relating to payments and trade transactions – 23 red flags.
- Red flags relating to jurisdictions – 10 red flags.
- Red flags relating to goods – 11 red flags.
- Red flags relating to corporate structures used – 16 red flags.

Note: these lists are non-exhaustive.

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Conclusion and Questions

Thank You

CentralBankUAE
CentralBankUAE
Central Bank of the UAE

CentralBankoftheUAE
Central Bank of the UAE

المصرف–المركزي.امارات
www.centralbank.ae

Central Bank of the UAE:

Download on the App Store
GET IT ON Google Play

المصرف-المركزي.امارات
www.centralbank.ae