National Anti-Money Laundering and Combating Financing of Terrorism and Financing of Illegal Organizations Committee

United Arab Emirates

TYPOLOGIES

IN THE MONEY OR VALUE TRANSFER

SERVICES SECTOR

EMERGING RISKS IN THE UAE

Supervisory Authorities' Sub-Committee
June 2022

Abstract

"This Typology Report (the "Report") has been put together, as part of understanding the Money Laundering ("ML"), Terrorist Financing ("TF"), and Sanctions risks identified by the money or value transfer services in the UAE".

TABLE OF CONTENTS:

INTRODUCTION

The Supervisory Authorities Sub-Committee (SSC), the Financial Intelligence Unit (FIU) in the UAE and the Executive Office for AML/CFT have produced a joint typology report to address emerging risks in the money or value services sector. A pilot group of Exchange Houses and Registered Hawala Service Providers (RHP) were selected to collaborate on an operational initiative that aims to share certain practices observed in the market amongst financial institutions, and to engage actively with competent authorities when such typologies are identified.

Risk-based supervisory interventions through onsite examinations, workshops, operational public private partnership (PPP) engagements and frequent dialogue with the private sector have improved the UAE's understanding of risks, particularly where supervisors observe the sector's proactive approach to monitoring risks, and the timely detection of risk patterns and trends in customer behaviour and transactions.

The Supervisory Authorities in the UAE follow a risk-based approach (RBA) to AML/CFT supervision. They seek to identify, assess and understand the ML/TF/PF risks facing the UAE's financial services, including the money or value services sector (supervised sectors) and, in coordination with other competent authorities in the UAE, to take action and apply resources aimed at ensuring that these risks are mitigated effectively.[1] To this end, the supervisors perform periodic and event-driven risk assessments, both of supervised sectors and of individual regulated entities, and use the findings of these assessments to plan their supervised activities in a risk-sensitive manner.

Supervisors also perform periodic and event-driven risk assessments of individual regulated entities, applying a risk-based approach to the scope, nature and frequency of these supervision and monitoring activities. The risk assessment process includes the collection and analysis of quantitative and qualitative data on the regulated entity, the inherent risks to which they are exposed, and the effectiveness of their counter-illicit finance policies, procedures, systems, and controls. Sector-wide assessments are also performed on a risk basis to identify groups of regulated entities that may face the same threats and vulnerabilities.

Supervisors use the results of these entity-level risk assessments to inform their overall supervisory approach. In future, each supervisor will use the results of both sectoral and entity-level risk assessments in their supervisory calendar, ensuring that supervisory resources are deployed to the areas of greatest risk and that any need for additional resources is promptly identified and addressed. The risk profiles of regulated entities are reviewed periodically, including where there has been a material change in circumstances, such as in management or business activities.

To develop a better understanding of the risks facing supervised entities, UAE supervisors continue ongoing engagement with the private sector, and gather data and statistics to detect and respond to such trends. As ML/TF typologies emerge and evolve rapidly, the private sector is able to detect changes through direct contact with clients and its transaction monitoring tools, systems and internal controls, and can inform supervisors accordingly.

The ongoing coordination between supervisors through the SSC and other competent authorities in their engagement with the private sector ensures clear expectations on risk management. This report highlights trends and case studies observed in the Money or Value Transfer Service sector (i.e. Exchange Houses and Registered Hawala Service Providers) for the year 2021-2022.

[1] The SSC consists of the Central Bank of the UAE (CBUAE), the Dubai Financial Services Authority (DFSA) of Dubai International Financial Centre (DIFC), the Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market (ADGM), the Securities and Commodities Authority (SCA), the Ministry of Justice and the Ministry Economy. (collectively the "Supervisory Authorities").

[2] Financial Action Task Force ("FATF"), *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2012; updated October 2020), Recommendation 1, p. 10.

GLOSSARY:

ANTI MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM	AML/CFT
ENHANCED DUE DILIGENCE	EDD
FINANCIAL INTELLIGENCE UNIT	FIU
KNOW YOUR CUSTOMER	KYC
MONEY LAUNDERING	ML
PROLIFERATION FINANCING	PF
PUBLIC PRIVATE PARTNERSHIP	PPP
PUBLICALLY EXPOSED PERSON	PEP
REGISTERED HAWALA SERVICE PROVIDERS	RHP
RISK-BASED APPROACH	RBA
SUPERVISORY AUTHORITIES SUB-COMMITTEE	SSC
TERRORISM FINANCING	TL
TRADE BASED MONEY LAUNDERING	TBML
UNITED ARAB EMIRATES	UAE

TYPOLOGIES AND RED FLAGS:

Common Typologies detected in the Exchange House and Hawala sector

Based on the review of products, services, processes, procedures and statistical analysis of all products and transactional data, the UAE identified the following financial crime typologies and red flags:

1. Structuring	2. Use of Third Parties/smurfing	3. Unusual High Value of Transactions	4. Sudden Increase in the turnover
5. Trade based money laundering	6. Fabricating transaction receipts	7. Carrying large value of foreign currency	8. Sudden increase in Turnover from one particular branch
9. Concealment of Beneficial Ownership	10. High value or change in salary (WPS) transactions to employees	11. Numerous remittances to same or different beneficiaries	12. Receiving money from many senders
13. Remittance to and from high-risk countries	14. Large Cash Deposits	15. Corruption through Publically Exposed Persons	16. Frequent Currency Conversion
17. Cash against Credit Card – Cash Advance	18. Cash Couriers	19. Transactions that are inconsistent with the customer's profile	

1.1. Structuring

Segregating large volume of transaction into small transactions to avoid scrutiny and detection.

Customer type: Individual/ Corporate
Products use: Currency Exchange and Money Remittance

Key Red Flags

- Multiple low value remittance or currency exchange transactions.
- Small value of frequent fund transfers made over a short time.
- Multiple transactions conducted at more than one branch within a day or more.

2.1. Use of Third Parties/Smurfing

- Transactions carried out by third parties (for example relatives and family members) on behalf of another person are aimed at concealing the sender and/or receiver.
- Transactions carried out by third party (entity) on behalf of other corporate entity.

Customer type: Individual/Corporate
Products use: Currency Exchange/Money Remittance

Key Red Flags

- Third Parties conducting numerous transactions on behalf of other individuals.
- Multiple transactions conducted by third parties at more than one branch, in a day or over a period of time.
- Corporate clients conducting transactions behalf of other entities.

3.1. Unusual High Value of Transactions

Customer transfer funds/exchanges foreign currency in large volumes, which is unusual for the customer's general economic activity.

Customer type: Individual/corporate
Products use: Currency Exchange/Money Remittance

Key Red Flags

- High value of cash transactions.
- Transaction does not match with the customer's profile or the entity's economic activity.
- Unusual transaction behaviour compares to customers with similar profiles.

4.1. Sudden increase in turnover

Increase in transaction value or annual turnover compared to previous years.

Customer type: Individual/Corporate/Exchange houses
Products use: Currency Exchange/Money Remittance

Key Red Flags

- Sudden increase in the value or annual turnover without an apparent reason.
- Unusual/high turnover from corporate clients and exchange houses, in contrast with others.

5.1. Trade based money laundering

Manipulating invoices by overstating the value of goods.

Customer type: Corporate
Products use: Remittance

Key Red Flags

- Invoice value greater than value of goods.
- Difference in the information of Origin, description, and value of goods.

6.1. Fraudulent transaction receipts

Difference in quality of receipts, font size, printing, and logo size.

Customer type: Exchange houses
Products use: Currency Exchange

Key Red Flags

- Representative of exchange house used fabricated transaction receipts to exchange illegal foreign currency.

7.1. Carrying large value of foreign currency

Customer type: Exchange houses
Products use: Currency Exchange

Key Red Flags

- Representative/employee of exchange house carried large volume of banknotes by hand to an exchange house.

8.1. Sudden increase in turnover from one particular branch

Customer Type: Exchange Houses
Product Use: Currency Exchange

Key Red Flags

- Volume/Turnover of transactions has been increased from one particular exchange house.

Customer: Corporate
Products: Foreign Currency/Money Remittance/WPS

Key Red Flags

- The client is reluctant to provide personal information, their business activities and corporate history.
- Hiding the identity of the beneficial owner.
- Disguising the nature of their business dealings with third parties.

10.1. High value or change in salary (WPS) transactions to employees

Placement of cash into the financial system; the client is paying significantly higher wages than usual to employees without a legitimate reason.

Customer type: Corporate
Product use: Wage Payments Service (WPS)

Key Red Flags

- High value salary transaction to employees.
- Change in salary amounts, compared to previous months - large cash transactions.

11.1 Numerous remittances to same or different beneficiaries

Customer conducts numerous money remittances to same beneficiaries in different values in a short period of time.

Customer type: Individual/Corporate
Products use: Money Remittance

Key Red Flags

- Customers sending money to same or different beneficiaries

12.1 Receiving money from many senders

Receiving funds form high number of senders over short period of time, with large sum transactions compared to a person's usual living standards.

Customer type: Individual
Products use: Money Remittance

Key Red Flags

A customer is the beneficiary of a high number of remittances (often in relatively small amounts) during a short time.

13.1 Remittance to/from high-risk countries

Remittance to high-risk countries

Sending money to high-risk jurisdictions.

Customer type: Individual/Corporate
Products use: Money Remittance

Key Red Flags

- Transfers to countries that have weak AML controls or high exposure to corruption.
- Transfers to high-risk countries or tax havens.

Remittance from high-risk countries

Receiving money from high-risk jurisdictions

Customer type: Individual/Corporate
Products use: Money Remittance

Key Red Flags

- Transfers from countries that have weak AML controls or high exposure to corruption.
- Transfers from high-risk countries or tax havens.

14.1 Large Cash Deposits

Placement of unusual amounts of cash into the financial system.

Customer type: Individuals/Corporate
Product use: Foreign Currency/Remittance/Wage Payments Service (WPS)

Key Red Flags

- High value of transactions by paying cash to introduce illegal money into financial system.

15.1 Corruption through Publicly Exposed Persons

Customer type: Individuals/Corporate
Product use: Foreign currency exchange/Remittance

Key Red Flags

- Use of Corporate Vehicles and Domestic Financial Institutions to launder money.

16.1 Frequent Currency Conversion

Converting one currency into another to launder the proceeds of crime.

Customer type: Individuals/Corporate
Product use: Foreign currency exchange

Key Red Flags

- Frequent local or foreign currency exchange in short period of time, without an apparent reason.

17.1 Cash against Credit Card – Cash Advance

Layering of illicit money to avoid audit trails by taking multiple cash advances after overpaying.

Customer: Individuals
Product: Cash against Credit Card

Key Red Flags

- Multiple cash advance on credit card in a month, credit card bill payment followed by cash advance withdrawal.

18.1 Cash Couriers

Concealing the movement of currency from one jurisdiction to another.

Customer type: Individuals
Product use: Foreign currency exchange

Key Red Flags

- Bringing cash from other country without a relevant declaration.

19. 1 Transactions that are inconsistent with the customer's profile

Transactions which are not in line with an individual's or corporate profile.

Customer type: Individuals/Corporate
Product use: All Products

Key Red Flags

- High value of transactions, that do not match the client profile.
- Unusual transaction volumes and amounts.
- Transactions to and from unrelated parties.

CASE STUDIES

Case Study 1

Exchange House A operating in the UAE detected unusual customer behaviour and trends through its Know Your Customer ("KYC") programme.

Fraudulent IDs: Customers approached different branches of Exchange House A to receive funds through Instant Money services such as MoneyGram, Ria, etc. These customers were generally from West Africa and used fraudulent identification documents. When probed for further information during the customer due diligence process, the customers would often raise a number of red flags (e.g. show signs of frustration, anger and hesitation to provide any supporting documents or answers to the questions asked) and would instantly leave the branch.

Adverse Media Reports/Foreign PEP: Through adverse media checks, Customer A was identified as a Foreign PEP with various companies in the UAE. Customer A approached Exchange House A to purchase a large number of foreign currencies. The purpose of the purchase according to the Customer A, was due to travel expenses and chartering a flight. Upon investigation, it was found that the purchase of the foreign currencies required by the Customer A was higher than the actual cost of chartering the luxurious private jet (as per market information), and when asked for additional information, the customer did not provide a rationale that was in line with the purpose of purchasing large foreign currencies.

Cross Border Remittances below the reporting thresholds: Transactions just below the reporting thresholds are remitted by professionals in the UAE to their respective home countries. These transactions can be seen either monthly or multiple times during the day and are being routed from via professional systems.

Trade Based Money Laundering (ghost-shipping techniques): Misrepresentation of the price, quantity or quality of imports or exports, or port of discharge (to show it is being discharged to the UAE). Observed TBML techniques differed in complexity and were frequently used in combination with other ML techniques to obscure money trails.

Employment of money mules to structure remittances below Enhanced Due Diligence (EDD) thresholds: Exchange House A identified instances of remittances to different beneficiaries in South Asian countries by a group of individuals and customers. Upon investigations, it was revealed that micro-structuring was used to remit below the EDD threshold.

Case Study 2:

Remittances sent or received by non-residents

Exchange House B operating in the UAE detected remittances sent or received by non-residents

Non-resident customers, mainly women on a tourist visit visa to the UAE, would remit funds to either one or multiple beneficiaries from the UAE. These remittances would occur multiple times during their one-time visit to the UAE. The purpose of these remittances, according to the non-resident customers, was to provide funds to family members and friends. Upon investigation, it was identified that the non-residents would often approach different branches and use multiple remitters to send funds to common beneficiaries in high-risk jurisdictions, which could indicate the use of layering proceeds of crime laundered by criminally-controlled individuals.

1. A group of non-resident customers on tourist visas to the UAE, would arrive at an Exchange House branch. One or two members of the group would approach the counter to receive funds from outside the UAE. When inquired about the sender's relationship, the standard response provided would be "in-laws". Based on review of such transactions, it was observed that the nationality of the senders would typically be West Africans based in developed countries.

2. Remittances would be sent to high-risk countries known for drugs trafficking and other predicate crimes related to ML, by unrelated senders to a single person. Upon review, the purpose stated by the senders was mainly to provide support and financial aid to families in these countries. The funds were remitted through instant money services.

Case Study 3

Wholesale Gold Traders accepting large amounts of cash from a local buyer

Exchange House C had a customer from a high-risk jurisdiction, whose main business was in wholesale gold trade. The customer would accept large amounts of cash on a regular basis from local buyers to purchase foreign currency from the Exchange House to settling the bills of foreign suppliers. Exchange House C understood the customer's business to purchase scrap gold from sellers in a high-risk jurisdiction. After refining the scrap gold into gold bars, they would sell the subsequent products to buyers in the UAE.

The customer's local bank accounts received large quantities of cash from the customer's domestic buyers. The customer then bought foreign currency from the exchange to remit to high-risk jurisdictions to settle their gold suppliers.

Risks Identified

The Exchange House's monitoring process of foreign currency detected the following red flags:

- The **gold traders** were accepting high volume of cash from the local buyers.
- The purchased currencies were transferred from the UAE to high-risk jurisdictions via **non-banking channels.**
- The **gold trader** and the supplier were from high-risk jurisdictions.

Risk Mitigation Steps

The Exchange House collected the following documents as a part of its risk mitigation measures and KYC programme:

- Cash receipts for the payments.
- Proof of shipment of the gold.
- Customs clearance and documents of the shipped gold.
- Currency export evidence, including customs clearance.
- A complete list of the company's buyers and sellers, including their ownership details.

Case Study 4

Payment from corporate entities against outdated invoices (typology detected during COVID-19)

Exchange House D often received requests for remittance transactions from corporate clients to make delayed payment against outdated invoices. These customers informed the Exchange House that the goods had already been delivered, or were yet to be delivered, and the late payments were being made, due to the unavailability of funds at the time. The Exchange House received such requests especially during the COVID-19 pandemic.

Risk Identified

During the processing of these transactions, Exchange House D observed the following red flags:

- The due date mentioned in the presented invoice, the payment was delayed for 12 to 24 months; and
- The goods had already been shipped 6-24 months previously.

Risk Mitigation Steps

As part of its risk mitigation measures and KYC programme, the Exchange House requested a new invoice/statement from the beneficiary. In absence of this, the Exchange House collected the following documents:

- Communication from the beneficiary regarding the due date and the invoice;
- Bill of lading and customs clearance document if the goods are already shipped;
- Recent customer bank statement; and
- Clarification statement from the customer regarding delayed payment.

Case Study 5

Hawala Service Provider X observed an increase in trading companies working as **unlicensed hawala service businesses.** In particular, this was noted for general trading companies, wholesalers, gold jewellery trading companies, used car dealers and electronics and mobile phone trading companies, which were associated with large volumes of cash. It was noted that these unlicensed hawala service businesses were working with customers with limited or no supporting documents.

Case Study 6

Hawala Service Provider Z observed that freight forwarding companies operating in UAE made cross-border payments to other freight forwarders (outside the UAE) to pay the freight charges for shipments ultimately destined for high-risk jurisdictions. In most of the cases, the companies gave the hawala service provider invoices for the freight payment, some of which were advance payments.

Risk Identified

- The freight forwarder customers made advance payments, rather than paying for shipments completed or already initiated.
- The type of goods, end user or the supplier's name were not listed on the invoice.
- An invoice without relevant shipping information can often be forged.

Risk Mitigations Steps

As there were no shipment documents available at the point of payment, hawala service provider Z took the following measures to mitigate the risk, collecting documents:

- Issued by the supplier addressed to the party receiving the goods;
- From end user of the goods, addressed to the shipper and requesting shipment;
- Recording a packing list, to match the details on the invoice.
- Screen all the parties mentioned in the documents.

CONCLUSIONS

The Supervisory Authorities remind FIs to remain aware of all regulatory obligations under the UAE Federal Decree Law on AML/CFT and Financing of Illegal Organisations, and its Implementing Regulation, Instructions, Guidelines, Notices, and Rules ('AML Legislation').

The mitigation of ML/FT crimes and effective control measures remain a key priority for the UAE. Exchange Houses must design document and implement its AML/CFT Programme carefully and effectively, based on the Standards outlined in Chapter 16 [i] at a minimum.

The Central Bank of the UAE, in particular, has conducted a granular sectoral risk assessment for its supervised sectors (i.e. Exchanges Houses and Registered Hawala Service Providers). Factors such as customers from high-risk segments (including free zones, general trading companies and non-resident customers), intrinsically high-risk products offerings (cross-border wire transfers, instant money transfer service, currency exchange), exposure to cash settlements, and correspondent relationships in high-risk jurisdictions, carry an inherently higher risk in these supervised sectors.

In summary, the financial sector must continue to enhance the effectiveness its controls, and must implement additional AML/CFT procedures, systems, controls, and measures appropriate to the risk profile of its business[ii].

If any further concerns arise or assistance is required, kindly contact your respective Supervisory Authority

[i] Chapter 16 of Standards Version 1.20 of Nov 2021 amending version 1.10 of Feb 2018.pdf (centralbank.ae)
[ii] CBUAE Sectoral Report - Money Laundering and Terrorism Financing Risk Assessment.pdf (centralbank.ae)