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 jointly produced a typology report to address emerging risks in the money or value services sector in a timely fashion. A pilot 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 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 timely detection of risk patterns and trends in customer behavior and transactions.

The Supervisory Authorities in the UAE follow a risk-based approach ("RBA") to anti-money laundering and combating the financing of terrorism ("AML/CFT") supervision. The supervisors seek to identify, assess, and understand the money laundering, terrorism financing, and proliferation financing ("ML/TF/PF") risks facing the UAE's financial sector 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 uses the findings of these assessments to plan its supervised activities in a risk-sensitive manner.

Supervisors perform periodic and event-driven risk assessments of the sectors it supervises as well as of individual regulated entities, for the purpose of applying a risk-based approach to the scope, nature, and frequency of its supervision and monitoring activities. The risk assessment process includes the collection and analysis of both quantitative and qualitative data pertaining to 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 entity-level risk assessments to inform the supervisory approach. Going forward, for each year's supervisory calendar, each supervisor will use the results of both sectoral and entity-level risk assessments, ensuring that supervisory resources are deployed to 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 material changes in management or business activities.

To develop a better understanding of the risks facing supervised entities, UAE supervisors continue maintaining an 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 through its transaction monitoring tools, systems and internal controls, are able to detect these changes to inform supervisors. Further, the private sector is likely to identify these changes, due to their direct contact with clients.

The on-going co-ordination between supervisors through the SSC and other competent authorities in their

[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.

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.

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 a number of 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 short period of time
- Multiple transactions conducted at more than one branch, in a day or over a period of time.

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 conduct transactions behalf of other entities.

3.1. Unusual High Value of Transactions

Customer transfer funds/ exchanges foreign currency in large in volume which is unusual to customer 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 behavior compares to customers with similar profiles.

4.1. Sudden Increase in the turnover

Increase in transaction value or annual turnover compare 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 were carrying large volume of banknotes by hand to our 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 form one particular of the exchange house.

9.1. Concealment of Beneficial Ownership

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

Key Red Flags

- The client is reluctant to provide personal information
- Reluctant to explain business activities and corporate history
- Hide identity of the beneficial owner
- 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 without a legitimate reason to employees.

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

Key Red Flags

- High value salary transaction to employees
- Change in salary amount compare 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, large sum transactions compared to person living standards.

Customer type: Individual
Products use: Money Remittance

Key Red Flags

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

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 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 Publically 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 as to launder 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 apparent reason

17.1 Cash against Credit Card – Cash Advance

Layering of illicit money to avoid audit trail 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 declaration

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

Transactions which are not in line with individual or corporate profile

Customer type: Individuals/Corporate
Product use: All Products

Key Red Flags

- High value of transactions that are not match with client profile
- Unusual transaction amount to expected volume and count
- Transactions to and from unrelated parties

CASE STUDIES:

Case Study 1:

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

Fraudulent IDs: Customers approached different branches of Exchange House A to receive funds through Instant Money services like MoneyGram, Ria etc. These customers were generally from West Africa countries 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 Publicly Exposed Person: Through adverse media checks Customer A, was identified as a Foreign Publicly Exposed Person who operates various companies in the UAE. Customer A approached Exchange House A to purchase a large amount 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 destined to a number countries by professionals in UAE are remitted just below the reporting thresholds to their respective countries. These transactions below the reporting thresholds can be seen either monthly or multiple times during the day, and are being routed from professional works.

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). Further, trade-based money laundering techniques observed differed in complexity and were frequently used in combination with other money laundering techniques to obscure the money trail.

Employment of money mules to structure remittances below Enhanced Due Diligence (EDD) thresholds:
Exchange House A identified instances of remittances to South Asian Countries by a by a group of individuals and customers to different beneficiaries. 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, who are on a visit visa (tourist visas) 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 remittance according to the non-Resident customers is 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 Customers, who are non-resident customers on tourist visas to the UAE, would arrive to 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 from western Africa countries based in developed countries.

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

Case Study 3:

Wholesale Gold Traders accepting large amount of cash from local buyer:

Exchange House C had a customer, whose nationality is from a high risk jurisdiction, whose main business was in wholesale gold trade. The customer would accepting large amount of cash on a regular basis from local buyers to purchase foreign currency from the Exchange House for the purpose of settling 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 them to buyers in UAE.

The customer had local bank accounts. The local banks were receiving high volume of cash from the customer's local buyers. The customer was then buying foreign currency from the Exchange and remit the currency to high-risk jurisdictions to settle their gold suppliers.

Risk 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 out of UAE to high-risk jurisdictions via **non-banking channels.**
- The **gold trader** and the supplier, were owners from high-risk jurisdictions.

Risk Mitigation Steps:

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

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

Case Study 4:

Payment from corporate entities against very old dated invoices (typology detected during COVID-19)

Exchange House D had often receive requests for remittance transactions from corporate clients to make delayed payment against old dated invoices. Exchange House D was informed by these customers that the goods were already delivered or yet to be delivered, but the late payments were being made due to the unavailability of funds. The Exchange House received such requests especially during COVID-19.

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 were already shipped before 6 to 24 months.

Risk Mitigation Steps:

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

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

Case Study 5:

Hawala Service Provider X observed an increase in trading companies that were working as **unlicensed Hawala service businesses.** In particular, this was noted for General Trading companies, Wholesalers, Gold Jewelry Trading companies, Used Car dealers and Electronics and Mobile Trading companies, who were associated with large volumes of cash. It was noted that these unlicensed hawala service businesses were working with customers with limited / no supporting documents.

Case Study 7:

Hawala Service Provider Z observed that freight forwarding companies operating in UAE are making cross border payments to another freight forwarders outside UAE to pay the freight charges of a shipments which is ultimately destined to a high-risk jurisdictions. In most of the cases when they remit, they provide the Hawala Service Provider Hawala with invoices for the freight payment. In some cases, shipment documents are provided as these are advance payments.

Risk Identified:

- The customers who are freight forwarder pays advance payment, rather than paying for completed/ already initiated shipment.
- As per the provided invoice, the type of goods, end user of the goods and the name of the supplier is unknown.
- The invoice without the availability of the shipping information, can be forged.

Risk Mitigations Steps:

As there were no shipment document was available at the point of conducting the payment, the Hawala Service Provider Z took the following measures to mitigate the risk.

- Collect documents issued by the supplier addressed to the party who received the goods.
- Collect documents from end user of the goods address to the shipper for shipment request.
- Collect packing list to confirm the details available in the invoice is matching.
- Screen all the parties mentioned in the documents.

CONCLUSLION

Supervisory Authorities remind FIs to remain abreast 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 carefully design, document and effectively implement its AML/CFT Program 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, results in an inherently higher risk supervised sector.

It summarizes that the sector must continue to enhance its control effectiveness and must implement additional AML/CFT procedures, systems, controls and measures as 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)