FERG
مجموعة مؤسسات الصيرفة والتحويل المالي
FOREIGN EXCHANGE & REMITTANCE GROUP
U.A.E. - ف.ع.م

www.ferguae.org

NewsExchange

FERG Newsletter Q1 - 2019

The History

Foreign Exchange and Remittance Group [FERG] is a non-profit organization formed based on the initiative of the Central Bank of UAE. The FERG comprises of companies engaged in the business of money exchange and remittances from large sized companies with over 100 branches, to single branch outlets to come on a common platform and work towards mutual benefit.

The initiative to form the Foreign Exchange & Remittance Group (FERG) started in the year 2001, wherein, some of the large and leading exchange companies decided to come together and hold regular meetings to discuss current market situations, opportunities and threats facing the exchange industry. This initiative gained momentum with the Central Bank Governor calling a meeting of all leading exchange companies in January 2004 to discuss the challenges facing this Industry. One of the important outcomes of the meeting with the Governor was the initiation of the Steering Committee, comprising of 10 leading exchange companies, who relentlessly worked towards bringing in most of the exchange companies to a common platform.

Over the next couple of years, the Steering Committee held regular meetings and took up issues with various regulatory and government authorities such as, Central Bank of the UAE, Reserve Bank of India, Dubai Police, Human Resources Committee for Emiratization, etc., with an objective to facilitate easier operational norms & to create a conducive business environment for the money exchange industry in the UAE. In the course of time more exchange companies joined the Committee as Rotating Members to strengthen and make it more vibrant.

FERG is registered with Dubai Chamber of Commerce & Industry (DCCI) since October 2008. Currently 69 exchange houses are the members of FERG, who aggregately cover over 90% money exchange and remittance business in the UAE.

Office Bearers 2019 - 2020

Mr. Mohamed Ali Al Ansari
Chairman

Mr. Osama Al Rahma
Vice Chairman

Mr. Adeeb Ahamed
Secretary

Mr. Rajiv Raipancholia
Treasurer

Mr. Harish Pawani
Joint Treasurer

Vision & Mission

To foster the development of a dynamic, innovative and stable foreign exchange and remittance industry that contributes to the economic and social wellbeing of our customers and position UAE as the market leader in money exchange and remittance business.

Goals & Objectives

To become a strong & united Group to voice the views & opinions of our members and create awareness about the role of exchange companies in transferring millions of dollars across the world through official channels in a safe, secure and economical way within the regulatory frame work of the Central Bank and Government of UAE.

Mr. Mohammed Anwar
HOD Compliance & AML Department

Al Ansari Exchange
FERG AML Sub Committee

EFFECTIVE RISK MANAGEMENT PROCESS

Definition

Risk management refers to the exercise of identifying potential risks associated to each job function, analyzing it, evaluate the existing controls and assess residual risks to ensure all risks have been mitigated effectively or taking precautionary measures to reduce/curb inherent risks.

In General Concept

No risks must be ignored, throughout the process it must be communicated and consulted accordingly with internal/external stakeholders, hence it assists in identifying the parties involved in risk assessment process and to engage the parties in risk treatment, monitoring and periodical review of risks.

Interestingly, if a specific risk management process is effective, it is more likely to go unnoticed. On the contrary when it is absent/fails, the impact is often highly visible and experienced across the entire organization and the consequences will result in negative manner.

Risk Management Process

Identification of Risk

Identify the risks that might have an impact on the objectives of the business/job function. It includes identifying sources of risk, areas of impact and their causes and consequences.

In this step, consider asking the following questions to yourself to have a clear view in identification of risks:

- **What might go wrong?**
- **How could it happen?**
- **Where could it happen?**
- **Why might it happen?**
- **What could be the impact of risks?**
- **How much is within the control?**

There are two techniques to identify risks – Identification of Retrospective Risks and Identification of Prospective Risks:

In general terms, risks that have previously occurred, such as compliance breaches, incidents, audit remarks, etc. are known as retrospective risk and on the other hand risks that have not yet happened, but it might happen any time in the near future are known as prospective risks.

Sources to identify retrospective risk – Audit reports, incident register, client remarks, etc.

Source of identify prospective risk – Review of policies, procedures and internal controls, GAP analysis, meeting/discussion with key employees or stakeholders.

Analysis of Risk

Upon identification of risks, develop a detailed understanding of risks. This process includes:

Identification of existing controls – Firstly determine whether the controls which are in place is effective to mitigate the impact of risks or not. Secondly assessment of likelihood and severity of the risks and risk rating; which helps in determining whether the identified risks are acceptable or requires further treatment.

Assess the likelihood – it can be described as rare, unlikely, possible, likely and almost certain.

Assess the severity – it can be described as insignificant, low, medium, high and extreme.

Evaluation of Risk

This step is to decide whether the identified and analyzed risks are acceptable or unacceptable. Communication/consultation and discussions within the involved parties are very vital in this step as this is a decision making situation.

Risk Appetite – it can be described as the amount and type of risk that an organization/business unit is willing to take in order to meet their strategic objectives.

Risk Tolerance – it can be described as the organization's/business unit's willingness to bear the risk after risk treatment to achieve its strategic objectives.

A risk is considered as acceptable or tolerable if the decision has been made not to treat it, however such risks may still needs to be monitored.

Aforementioned three steps constitutes the risk assessment phase of the risk management process.

Treatment of Risk

This step is also called as risk response – is the process of developing strategy to reduce the likelihood and severity of the identified risk. Devise an action plan to implement risk treatments to control the risk. Risk treatment must be applied on the root cause of such risks, or else such action would be ineffective and promote a false belief within the organization/business unit that the risk is controlled.

This step includes:

- **Desirable treatment for identified risks**
- **Treatment options to reduce the likelihood and severity of risk**
- **Evaluate treatment options**
- **Proper documentation of treatment plans**
- **Implement commonly agreed treatments**
- **Assess residual risk after risk treatment**

During the course of risk management process and afterwards, involved parties must constantly communicate and consult each other or with internal/external stakeholders in an effective manner and continuous monitor and review of risks; considering the evolving environment of the organization/business unit.

EFFECTIVE STR / SAR WRITING

Ms. Gurminder Kaur
Head Compliance

Al Rostamani International Exchange
FERG AML Sub Committee

Suspicious Activity/Transaction Reports (SAR/STR) acts as one of the enablers for the Financial Intelligence & Law Enforcement Units to take actions on perpetrators of Money Laundering and Terrorism Financing. SARS serve to safeguard the interest of Financial Institutions and help them in avoiding regulatory fines, penalties and other legal consequences.

As the name suggests a Suspicious Activity Report is not a judgment but a suspicion that a violation or a crime may have occurred. Let us delve into what makes a SAR effective or ineffective. An effective SAR is a timely SAR, has clarity, and provides relevant and complete description about the parties, transaction, dates, amount and more. Whereas an ineffective SAR lacks all these components and does not enable the Intelligence to take actions but is merely another document which goes into the database.

Having a SAR form makes it easier to fill and not miss out on any of the vital information that may be essential to a subsequent investigation. The “5Ws” & “H” should be remembered while drafting a SAR namely, Who, What Where, When & How.

The SAR must be crisp and convey the suspicion clearly and not just a mention of what is unusual. To explain it further, the report should tell us who is the customer; the beneficiary i.e. the party/s against whom the suspicion of a violation or crime is. Is the customer a legal or juridical person, i.e. is the customer an individual or a company, ID details, nationality, address of the customer should be provided. This helps the Law Enforcement Authorities for further investigations. Is it the remitter or the beneficiary? When the violation or a transaction which arose the suspicion has occurred, give the date; if time is of importance to the case, give details about that too.

A well drafted report should provide the details from where the customer has availed and usually avails the service; i.e. the branch details. Is it a single transaction or a series of transactions (if series provided a statement of the suspected customer as an attachment) which gives rise to the suspicion. What is the service used; does it involve remittance, instant money or a forex transaction/s?

Has the customer approached you to process a transaction and during the initial phase you have discovered the red flags and denied your company’s services; in such cases as well you should be reporting your suspicions as an “attempted” case.

The “How” is the most important in the SAR; it describes the modus operandi of the customer which violates or serves as the red flag on the basis of which a SAR is reported. Describe as precisely as possible as to how the company/individual operates, the series of events which gave rise to the suspicion. The “How” is the story which an investigator should be able to visualize about the customer’s activity and your suspicion clearly.

In addition to the SAR a KYC against whom the SAR has been raised should be provided; where the SAR is against a company the KYC should provide details of the Owners/ Partners/Directors/Authorized signatories/Representatives.

Lastly, what action has the exchange house undertaken; is the customer still active, has the customer been put in the internal watch list and other actions undertaken as per the risk appetite of the exchange house should be mentioned.

It is advised to add the company/individual to the internal watch list for heightened monitoring in case the customer approaches the exchange house again, this shall serve as an alert to do enhanced due diligence, reject or report to FID. A linked STR can be raised against company/individual where we have got further information and instances where the company/individual has again availed a service which is potentially suspicious. We must remember to provide the earlier filed SAR reference number stated in the FID portal in the linked SAR.

An intelligent and a timely SAR thus serves an important role in the fight against Money Laundering & Terrorism Financing.

Mr. Abdulkarim Farook
Group Chief Compliance Officer

Wallstreet Exchange
FERG AML Sub Committee

IMPORTANCE OF INDEPENDENT REVIEW OF AML / CFT AND SANCTIONS COMPLIANCE

FATF Recommendation 18 (Internal Controls and Foreign Branches and Subsidiaries) stipulates the following:

Financial institutions' programmes against money laundering and terrorist financing should include:

- **The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;**
- **An ongoing employee training programme; and**
- **An independent audit function to test the system.**

As per the FATF Recommendation stated above, it is important not only to implement an AML/CFT compliance function but also to test through independent audit that the said function effectively addresses all the AML/CFT requirements. It is important to assess whether the said policies, procedures and systems are effective in combating money laundering/terrorist financing and meeting all the legal and regulatory requirements in this regard.

The Basel Committee on Banking Supervision in its AML/CFT Guidelines highlighted the three lines of defense in the context of AML/CFT: the first line of defense are the business units in charge of identifying, assessing and controlling the risks of their business, Compliance is the second line of defense responsible for ongoing monitoring of the fulfillment of all AML/CFT requirements and Internal audit is the third line of defense, plays an important role in independently evaluating the risk management and controls, and discharges its responsibility to the audit committee of the board of directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with AML/CFT policies and procedures.

The above requirements related to independent review to test the effectiveness of AML/CFT policies, procedures and controls is stipulated in our AML/CFT Executive By-law (Cabinet Decision No. (10) of 2019).

The key aspect of the review process is that it must be conducted in an independent manner and at regular intervals to provide an impartial assessment of the compliance function. EHs must be able to demonstrate the independence of the reviewer (auditor)by ensuring that the following conditions are met:

It should be completed by a person who was not involved in undertaking any of the functions or measures being reviewed, including the design, implementation or maintenance of the AML/CFT and sanctions compliance program, and who was not involved in the development of EHs risk assessment or related internal controls. In essence, EHs must be satisfied that an independent reviewer is not assessing their own work, and that there are appropriate divisions in place to avoid any conflicts of interest or threats to the independence of a reviewer. Independent reviews also provide an opportunity to assess whether previous audit issues have been addressed.

EHs would be vulnerable to abuse by criminals and terrorist financiers and incur reputational risks including payment of huge amount of fines due to having systems, controls and procedures not commensurate with the ML/TF and sanction risks facing the company.

To summarize, AML/CFT and sanctions compliance function must be reviewed on a regular basis to assess its effectiveness and the assessment must be conducted by a party (internal or external) who was not involved in any manner in the design/implementation of the AML/CFT policies, procedures and controls, in order to carry out an impartial assessment without any bias or self-interests.

Ms. Anuja Thakur
Head Compliance

UAE Exchange
FERG AML Sub Committee

THE ROLE OF A COMPLIANCE OFFICER IN TODAY'S WORLD

Financial Crime Compliance remains an extremely important topic for regulators, governments and financial institutions. Whilst it is the responsibility of the entire institution to make money laundering as difficult as possible, it is the "Compliance Officer", who is considered the gatekeeper, controller and custodian of the firm's AML framework.

This is a critically important position within any financial service, when it comes to the identification, detection, escalation, reporting, managing and training of staff on Anti Money Laundering procedures. It is the personal responsibility of the Compliance Officer to ensure this all happens as effectively and efficiently as possible.

The role of the compliance officer has been defined as, "to provide oversight of the day-to-day operations for compliance by the firm and develop its AML policies, procedures, systems and controls". However, the role of a Compliance Officer in today's financial world is significantly far more challenging, as they have to deal with stringent changes within the regulatory framework on one hand and the threats of money launders masking their funds through financial systems with exquisite intelligence on the other.

As the future of the financial landscape moves towards digitalization and smart technology, the ability to quickly adapt to the new challenges of compliance governance around innovation is another key challenge for the Compliance officer.

During the past decade the overall compliance framework has in itself, undergone an overhaul with regulators moving swiftly towards the "Risk Based Approach" than the traditional rule-based approach. To successfully implement a "Risk Based Approach" a compliance officer has to develop in depth understanding of the Financial Institution's business, it's nature, scale, diversity of products, customer base and geographies of operations. Equally, a Compliance officer must have an ability to understand and interpret the regulations and translate their applicability to the Financial Institute and develop demonstrable evidence of adherence to the same.

In order to assess the money laundering risk, the Compliance Officer should not only have an understanding of criminal methodologies but an understanding of the behavior and business practices of the firm and it's customer base. Compliance Officer has to strategically calibrate their firm's anti-money laundering program to suit their compliance obligations, delicately poising it between the dangerous legal liabilities of under-compliance, and the costly burdens of over-compliance.

Considering the above, the Compliance Officer must hold a senior position within the firm, with an ability to have access to all relevant information to make informed decisions and to be free to act on his/her own authority. Their position should also allow them to design, implement, and enforce their firm's compliance systems and procedures. They should be a part of the senior management team of the firm. They should be provided in depth knowledge about the firm's business model, MIS/data, product capabilities and risks. They should have adequate resources, time and staff. They should be provided with sufficient training to keep themselves upskilled with market trends and threats.

The Compliance Officer is akin to the "traffic control team" within the aviation industry, they may not fly the planes, neither built them or fuel them, but they bear the huge responsibility of guiding the pilots towards safe aviation operations, ensuring the all threats are effectively identified and mitigated.

Mr. Sarfraz Gill
Chief Compliance Officer

Orient Exchange
FERG AML Sub Committee

RISK OF DE-RISKING PRACTICES AND MITIGATION MEASURES

"De-risking" is very common now a days and it refers to financial institutions exiting relationships with and closing the accounts of clients considered "high risk." There is an observed trend to-ward de-risking of money service businesses, foreign embassies, nonprofit organizations, and correspondent banks, which has resulted in account closures in the US, the UK, and Australia. Low profit, reputational concerns, and rising AML/CFT scrutiny contribute to de-risking, which can further isolate communities from the global financial system and undermine AML/CFT objectives.

It has observed that financial institutions have moved to a "de-risking" approach in their operations. While de-risking – eliminating or significantly limiting – business lines, products, geographies, and/or clients that pose an increased risk to AML-compliance efforts may seem prudent, it also poses significant growth challenges for financial institutions. Over the past several years, institutions have sought to reduce risk by eliminating portfolios, counter-parties, or entire lines of business. However, these moves may run counter to their ability to achieve strategic business objectives. These decisions may be overly broad since they may not be focused on those risks that may pose the biggest risks to the bank: high-risk customers, politically exposed persons, and regions such as emerging markets.

This is also noticed that one sector that has traditionally been perceived as high risk is MSBs. MSBs are non-bank institutions that provide financial services such as money transmission, currency exchange, or check cashing, often with much lower fees than traditional banking institutions and without the requirement to maintain a formal account. However, limited and varying levels of regulatory oversight, as well as challenges to conducting customer due diligence (CDD) in many recipient payout locations and jurisdictions, have raised concerns about AML/CFT vulnerabilities. Even if MSBs are in full compliance with the sending jurisdictions' regulations, transactions are often perceived as risky when the recipient jurisdiction lacks adequate AML/CFT frameworks or borders jurisdictions that are subject to sanctions, have limited governance capacities, or are experiencing conflict.

The FATF expressed several concerns due to de-risking, such as;

- De-risking can introduce risk and opacity into the global financial system, as the termination of account relationships has the potential to force entities, and persons into less regulated or unregulated channels. Moving funds through regulated, traceable channels may facilitate the implementation of anti-money laundering/countering the financing of terrorism (AML/CFT) measures.

- It is central to our mandate to ensure that the global AML/ CFT standard is well understood and accurately implemented, and that countries and their financial institutions are provided with support in designing AML/ CFT measures that meet the goal of financial inclusion.

The risk-based approach should be the cornerstone of an effective AML/CFT system, and is essential to properly managing risks. The FATF expects financial institutions to identify, assess and understand their money laundering and terrorist financing risks and take commensurate measures in order to mitigate them. This does not imply a 'zero failure' approach.

By taking a fresh look at inherent as well as perceived risks, financial institutions can become risk intelligent, even before they conduct a formal AML risk assessment. Boards and senior executives should consider several key questions in managing risk appropriately:

Does the company possess a culture of compliance that exists throughout the organization or are there silos present that inhibit a more integrated compliance approach?

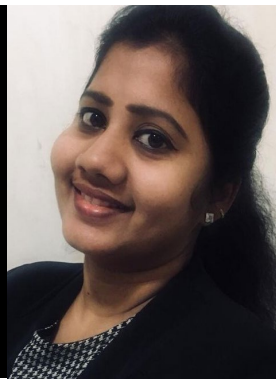
- **Has management established appropriate incentives to incorporate AML compliance objectives across the organization?**
- **Does senior management set the tone through active engagement and involvement in AML risk mitigation?**
- **Are the company's policies and procedures aligned with the business' operating model, and its various lines of business?**
- **Does management possess a holistic view of its customers across geographies?**
- **Are the company's various reporting, technological, and other systems integrated geographically?**
- **Is our ongoing compliance monitoring and testing sufficient to identify potential weaknesses?**

This article has been written to share research results, to contribute to public debate and to invite feedback on development and humanitarian policy and practice. It does not necessarily reflect the policy positions of the FERG or its associates who are jointly publishing it. The views expressed are those of the author and not necessarily those of the individual organizations.

UNDERSTANDING COMPLEX OWNERSHIP STRUCTURES – IMPORTANT? WHY?

Ms. Jayanthi Mohanasundaram
Compliance Officer

Lulu International Exchange
FERG AML Sub Committee



After the release of Panama and Paradise papers, public awareness had increased regarding creative techniques used by criminals to hide cash in Corporate structures such as shell& offshore companies.

Corporate vehicles - Corporations, Trusts, Partnerships, etc play a major role in modern economies. Though majority of them serve legitimate purposes, some are misused for illegal purposes including Money Laundering, Terrorist Financing, Bribery, Corruption, Tax Frauds, etc. The concern arising from the potential misuse of corporate vehicles by criminals can be significantly reduced by understanding the UBOs, source of assets and their business objectives.

Financial Action Task Force(FATF) and Regulators across the globe, are working together to curb the exploitation of complex corporate structures and other incorporations of disputable ownership. Just Know-the-Customer is not the only important risk mitigation tool for Financial Institutions(FI), but is increasingly becoming a mandatory legal requirement and a methodology to execute legal and profitable business with.

Who are the UBO's?

FATF defines UBO (Ultimate Beneficial Owner) as natural person(s) who ultimately owns/controls a customer, and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person/arrangement. Under the new FinCEN rules regarding CDD requirements, collecting, maintaining and reporting of beneficial ownership information is a mandatory requirement for FIs. The Regulations of CBUAE also specifies that the collection of the ownership and UBOs of a legal entity is mandatory during any business relationship.

Hence, comprehensive identification& verification of corporate structures and UBOs has become vital.

Challenges in identifying UBO's

It is not sufficient to just find out who the UBOs are, but to understand what level of compliance risk they present to the organization. Some of the critical challenges faced by FIs:

- Complicated layers of structures – multiple layers of ownership increase the number of entities to be verified; difficulties to detect changes in profiles or suspicious patterns.
- LaxLaws and Regulations – jurisdictions of incorporation with weak controls in place, the so called "Secrecy/Tax Heavens", are used.
- Lack of standardized documentation – Supporting documentation to validate ownership may vary across countries, making knowledge for appropriate documents for EDD a complex process.
- Flexibility to change ownership – FIs may not be aware of changes in ownership after establishing relationship.
- Differing types of shares issued – the knowledge of any "un-named" type of shares issued by the corporate is very difficult, and most of the times the bearer shares holders may not be even registered at all.

Why identifying the UBOs is important?

Money Laundering/Terrorist Financing remains the top concern globally for financial services. Any lapses in Know-your-customer, beneficial ownership or sanctions compliance would result in huge penalties/fines by Regulators.

Section 3 and Chapter 3 of the CBUAE's Cabinet Decision No.(10) of 2019 concerning the implementing regulation of Decree Law no.(20) of 2018 on AML/CFT strengthens the requirement on FI's to identify the UBOs conducting financial transactions, in order to avoid non-compliance and possible penalties at both account opening and ongoing. The lack of identification of UBO's and/or anonymity in account or transaction maintenance can inhibit severe Law Enforcement.

Financial crime in general, including ML&TF, can expose a country's economy to financial instability. For criminals trying to bypass AML/CFT measures and controls, corporate vehicles are used as an attractive & effective way to disguise their criminal proceeds, before introducing them formally into the financial system. Therefore, the FIs must take reasonable measures and actions to determine the true identity of all customers, the beneficial owners, and ultimate beneficiaries whom request their services.

To overcome this challenge, strong AML/CFT Compliance and Sanctions Programs with adequate knowledge about the risks involved become critical to the FIs; in order to understand the highly complex, multi layering and hidden structures of corporate entities created to hide the identity of UBOs, they use new technologies such as Artificial intelligence and Machine Learning that help to identify identities of those who exercise ultimate effective control over legal/incorporated entities.

Combating Money Laundering and Terrorist Financing is our responsibility!!!

Mr. Mohan Marimuthu
Compliance Manager

Al Fardan Exchange
FERG AML Sub Committee

ML / TF RISK ASSOCIATED WITH HAWALA & OTHER SIMILAR SERVICE PROVIDERS

Hawala is a trust-based system used to transfer funds across countries and continents. It is often reliant on ties within specific geographical regions or ethnic communities, which arrange the transfer and receipt of funds or equivalent value, without any requirement for identification of remitters. These movements of value may be settled through trade or cash businesses engaged in remittance activities. They often operate in areas of expatriate communities.

The term 'Hawala' is often used to describe a number of different Informal Value Transfer Systems which have similar properties and operate in similar ways, although they are not strictly 'Hawala'. Accordingly, in 2013, the Financial Action Task Force (FATF) came up with the wider term 'Hawala and Other Similar Service Providers' or HOSSPs to describe this activity. HOSSPs are a subset of Informal Value Transfer Services (IVTS); other forms, apart from Hawala, include Hundi, Chinese underground banking and Black Market Peso Exchange.

The most common reasons for existence of HOSSPs are cheaper & faster money transmission, cultural preference, lack of banking access in remittance receiving and sending country, higher confidence in Hawala and other similar service providers than in the banking system, evade currency controls and international sanctions, evade taxes, transfer or conceal criminal proceeds.

Completely unregulated HOSSPs operators are particularly vulnerable to Money Laundering/Terrorist Financing risks because they permit funds to be sent with little or no CDD requirements, allowing a money launderer or terrorist financier to freely send funds with limited risk of being identified.

There are several reasons why HOSSPs continue to pose a money laundering and terrorist financing vulnerability like lack of supervisory will or resources, settlement across multiple jurisdictions through value or cash outside of the banking system in some instances, the use of businesses whose primary focus may not be regulated as financial institutions, the use of net settlement or cover payments, to settle through the banking system that makes it difficult to track individual transfers, the commingling of criminal and illicit proceeds and the masking of illicit proceed transfer that appears to be trade.

Hawaladars (those that operate 'Hawala') often run parallel businesses other than money transfer, particularly general trading companies, currency exchange, travel agencies or telephone shops. Grocery stores are a typical venue for hawaladars and other similar services providers to conduct their remittance business. Many of them also provide import –export business – which creates an enabling environment for value settlement – in particular over-under invoicing when remitting funds to other geographic locations. By running an additional business such as a travel or ticket agency or freight forwarding, criminal HOSSPs can derive an additional benefit that provides them with a ready supply of customer identity documents, which can be 'hijacked' and used to generate false customer records which are used to mask the receipt of criminally derived cash.

The most frequent methods of settlement used by hawala and other similar service providers are simple reverse Hawala, triangular settlement with network of service provides, value settlement through trade transactions including over invoicing and under invoicing and settlement through cash transport.

UAE Government and CBUAE are taking stringent steps to curb the illegal Hawala operators. In early 2017, Department of Economic Development (DED) raided 25 shops in Dubai for illegal money transfers to Bangladesh. DED has quoted that "First of all, such illegal channels deny accurate information on the flow of cash [and thus harm the economy]. Secondly, they deprive authorised money exchanges and banks of their deserved share of business, and thirdly, customers depending on such illegal channels risk losing their hard-earned money". DED has further urged consumers not to be tricked by such unscrupulous operators and alert the DED of any illegal business activities they come to notice. Consumers can contact the DED on the Ahlan Dubai number 600 54 5555

Thank you for your support

Capital Banking Solutions
EXPERIENCE INNOVATION

idetect

KPMG

AJMS | INTERNATIONAL MANAGEMENT CONSULTANCY

pwc

WesternUnion WU

FERG
مجموعة مؤسسات الصيرفة والتحويل المالي
FOREIGN EXCHANGE & REMITTANCE GROUP
U.A.E. - ش.م.ع

+971 4 3772896
info@ferguae.org
www.ferguae.org
ferguae
ferg