FintEdu

UNLEARN. LEARN. RELEARN

UAE AML - Identifying, dealing and reporting suspicious transactions

Theresa Karunakaran

3rd June 2024, Monday | 03:00 pm – 04:00 pm GST | Zoom

Identifying dealing with and reporting Suspicious Transactions

ML/TF Penalties levied in 2023 by Global Regulators

Penalties for non compliance with AML,KYC sanctions etc totaled $ 6.6 billion

Highest value of fines $4.3 billion on Binance
Crypto and Payments firms account for the rise in penalties accounting for 69% and 21% of global penalties-Fenegro

“Binance turned a blind eye to its legal obligations in the pursuit of profit. Its willful failures allowed money to flow to terrorists, cybercriminals, and child abusers through its platform,” Secretary of the Treasury Janet L. Yellen

Understanding Money Laundering

- The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source - FATF

Stages in Money Laundering

- **Placement**

Act of introducing illegal profits into the financial system

- **Layering-**

The second stage where the Ml engages in a series of transactions Distancing the Money Launderer from the source of funds by making a series of conversions or movement of funds

- **Integration**

The process through which the funds renter the legitimate economy

Why do we need to guard against ML/TF

Lax controls impact

- The integrity of the Financial System
- Discourages foreign investments
- Acts as a deterrent to technology exports to developing countries

FATF recommendations

- The FATF sets standards and promote effective implementation of legal, regulatory and operational measures for combating ML/TF
- Each country frames the legal framework for AML/CFT
- India for instance has the Prevention of Money Laundering Act 2002 and PML(Maintenance of Records)Rules 2005
- UAE - the Anti Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Laws,related Cabinet decision,Supervisory Guidance to Licensed Financial Institutions(LFI)

First things first –Foundations of a robust AML Programme!

- Customer Due diligence –Identifying and verifying the customer and beneficial owner using reliable and independent sources of identification
- Know Your Customer-Identifying the customer before the commencement of an account based relationship, while dealing with an individual who is a beneficial owner, authorized signatory or power of attorney holder related to any legal entity
- Know Your Customer’s business –nature of business,location,geographical risk covering customers as well as transactions,types of products/services offered,delivery channels used for delivery of products/services,types of transactions undertaken etc
- Know your Customer’s customer

Accounts of Politically Exposed Persons

- Reasonable measures are taken to establish source of funds/wealth
- Approval to open an account is taken at level of Senior Management
- All such accounts are subject to enhanced monitoring on an on going basis.

The Risk based approach
Risk management

- Customers may be categorized as Low,Medium and High
- Risk categorization based on parameters such as customer identity, social/financial, nature of business activity status, nature of business activity, services, delivery channels
- Review of Risk categorization of accounts at least once in 6 months
- KYC updation
- 2-8-10 years depending on risk category.of High,Medium and Low

Transaction Monitoring

- Red Flag Indicators flagged by Regulator/FIU
- Setting appropriate threshold limits for generation of alerts
- Examination and disposal of alerts-3 LOD
- Reporting of Suspicious Transactions
- Quality Assurance.

Suspicious Transaction Reports

Defining a **Suspicious Transactions:**

- Transactions related to funds for which there are reasonable grounds to believe that they are earned from any felony or misdemeanor or related to the financing of terrorism or of Illegal organizations, whether committed or attempted

- A suspicious transaction refers to any transaction, attempted transaction, or funds for which an LFI has ***reasonable grounds*** to suspect as constituting—in whole or in part, and regardless of the amount or the timing - any of the following:

 The proceeds of crime (Money laundering and related predicate offenses, or financing of terrorism or illegal organisations);

 Being related to the crimes of money laundering and related predicate offences, the financing of terrorism or illegal organisations; and

 Being intended to be used in an activity related to such crimes

Suspicious Transaction Reports

The legal basis for the requirement to submit STRS to FIU

- Enshrined in Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and Financing Illegal Organisations Legislation
- Related Cabinet Decisions for its implementation,including
- Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions

STRs

Minimum statutory obligations on LFI

- Put in place indicators to identify suspicious transactions

- Report suspicious activity to the FIU and cooperate with relevant authorities,
- Not disclose the information or data in an STR

The 3 Lines of Defence

- **First LOD**
- Relationship managers,business executives,back office operation functionaries
- Central to timely escalation of suspicious activity
- Trained to regulatory requirements within the scope of their role
- Red flags associated with their customers, products, services, delivery channels, and geographies; and
- Tthe appropriate escalation procedure both to their management and to the second line of defense without compromising their responsibility to report suspicious transactions

The 3 LoD

- **The Second LoD**
- Compliance employees-Provides policy advice, guidance, assurance, oversight, and challenge to the first line of defense.
- Oversees investigation programme,both manual and automated
- Monitors risks relating to LFI and reporting directly to senior management on the LFI’s risk exposure, including through financial crime-related metrics.
- LFI required to appoint Compliance Office or Money Laundering Reporting Officer
- MLRO responsible for reviewing, scrutinizing, and reporting STRs and other reports pertaining to suspicious activity
- MLRO is primary source of contact with law enforcement agencies,
- Liaising with regulators and external bodies on financial crime issues in order to share knowledge, report cases, develop best practices, and where possible, to improve coordination within the financial sector.

3 LoD

- **Third LoD**
- Internal audit ,external auditors ,independent testing functionetc
- Responsible for evaluating the design and operational effectiveness of an LFI’s compliance program controls, including technical compliance with AML/CFT policies and procedures
- Independently identifies gaps,deficiencies,weakness in LFI ‘s operational controls
- Risk-based auditing assists an LFI’s Board of Directors and senior management in identifying areas of weakness, prioritizing those areas for remediation, and ensuring the provision of adequate resources, oversight, and training for affected employees

Reporting of STR

- The quality of STRs, SARs, and other report types is imperative for increasing the FIU's analytical function to identify vulnerabilities and threats to the UAE financial system and
- Develop an overall understanding of money laundering and the financing of terrorism and illegal organisations' risks based on emerging trends and patterns
- LFI should review alerts for potential suspicious activity
- Have policies and procedures that document the process for deciding whether to close the alert or to promptly report the transaction as suspicious and
- Should include guidance on capturing detailed descriptions for the manner in which the alerts were either disposed of by reporting or closure of the alerts

Filing an STR or SAR

- STR: If, during the establishment or course of the customer relationship, or when conducting transactions on behalf of a customer or an occasional customer, an LFI suspects transactions are related to money laundering, related predicate offenses, or the financing of terrorism or illegal organisations, then the LFI should submit an STR to the FIU within the timelines
- □ SAR: If, during the establishment or course of the customer relationship, an LFI suspects any activity or an attempted transaction (i.e., a non-executed transaction) can be related to money laundering, related predicate offenses, or the financing of terrorism or illegal organisations, then the LFI should submit a SAR to the FIU
- Additional Information File(AIF)/Additional information File with Transactions(AIFT)-Reports required to be submitted to the FIU based on their request on the AML platform

Filing an STR/SAR

- Filing STR/SAR using go AML portal
- AML Report
- Investigative narrative report which sets out

Introduction-The general description of the violation, name of the subject against whom filed, any previous STR

- **Body:**Includes narrative as to why STR was filed,

Involved parties

Suspected transactions in chronological order,source and destination of funds, reasons for the suspicion and why the transaction is determined to be illegal/suspicious,modus operandi

- **Conclusion**

Any planned/initiated mitigating steps, including information about any follow-up actions conducted by the LFI (e.g., intent to close or closure of accounts, ongoing monitoring of activity, etc

Filing an STR

- **Can an LFI file a defensive STR?**

Defensive STR is filed for transactions or activity(ies) that LFIs do not deem truly suspicious in order to reduce the risk of regulatory penalties for non-filing of STRs or SARs

- CBUAE considers defensive STR or SARs as indicative of an inefficient transaction monitoring system and an LFI's weak system of internal controls.
- The UAE FIU has noted instances where SAR or STRs are reported due to the LFI not receiving supporting documents that would justify the transaction
- LFIs to conduct a thorough investigation and available retrievable documents included in the STR/SAR

Timelines for filing STRs , SARs

- **Dispositioning of alerts**-recommendation on and decision on whether to file SAR/STR-Within maximum of 35 business days from the date of automated alert generation
- **Filing of a follow up STR or SAR for a complex investigation** the LFI should submit an initial STR within 15 business days of alert generation – SAR/STR to be labelled "Complex investigation". Follow-up SAR/STR to be submitted within 30 business days of filing the initial STR
- **Filing STR/sAR on continuing activity-** Upon filing STR/SAR pertaining to an account holder, LFIs are expected to implement enhanced monitoring on such account holders
- . In the case of continued suspicious activity detected against such account holder, LFIs are expected to expeditiously file an STR/SAR continuing activity with the FIU
- -

Life after filing STR!

- Maintain confidentiality,no tipping off!
- Review related customer accounts,relationships to identify if any further suspicious transactions have taken place,implement EDD,monitoring of such accounts,classify as High Risk
- Obtain Senior Management’s approval for continuing the relationship and the EDD measures
- Review on continuing the business relationship,

If the answer is Yes,

- document reason/rationale for taking the decision
- The EDD process,
- Restricting the customer’s use of certain products or services.

Placing restrictions and/or additional approval requirements on the processing of the customer’s transactions (for example, transaction size and/or volume limits, or limits to the number of transactions of certain types that can be executed within a time period.

Best practices

- Planning an Annual AML /CFT Risk Assessment and mitigation exercise
- Incorporating threat areas identified by FIU/Supervisors in the Annual Risk Assessment
- Analysing implications of changes in Risk categorization of customers, impact on lines of business ,products
- Launch of new products/technologies-assessing AML implications

Case Study -On the Binance Trail!

- Binance did nor register with FinCEN as a money services business
- It did not implement comprehensive KYC protocols or monitor transactions
- Never filed a SAR with FinCEN
- Facilitated trillions of dollars of transctions on its platform
- Generated over $1.6billion in profit

US DoJ Press Release dated Nov 21,2023

0

On the Binance Trail!

- Lack of AML controls lead to
- Illicit actors using Binance's exchange in various ways, including conducting transactions for mixing services that obfuscated the source and ownership of cryptocurrency;
- transferring illicit proceeds from ransomware variants; and moving proceeds of darknet market transactions, exchange hacks, and various internet-related scams.
- Binance did not implement controls that would prevent U.S. users from trading with users in Iran; and, because of this intentional failure, between January 2018 and May 2022, Binance willfully caused over $898 million in trades between U.S. users and users ordinarily resident in Iran.

Choose the correct answer

Binance was levied a fine of $4.3 billion because

a.It had generated $1.6 billion in profit

b.It did not register with FinCEN as a Money Service Business

c.It did business in Crypto currency without getting the requisite authorisation

d.a & b

e.b & c

Choose the correct answer!

Binance transactions were not detected earlier

a. It did not have an AML monitoring system

b. It did not file SARs

c. All of the above

Thank you!