AML/CFT **Snapshot**

By: Nesar Yosufzai
Certified Financial Crime Specialist
Certified Anti Money Laundering Specialist

Note: 03 | April 2018

Anti-Money Laundering and Counter Financing Terrorism Notes to Insurance Sector of Afghanistan

Money Laundering is the process to conceal or disguise the proceeds of crime such as drug trafficking, corruption, illicit arms trafficking, extortion, fraud, insider trading, organized crime, and other predicate offenses and to make them appear legal. According to the International standards, including Financial Action Task Force Recommendation, Palermo Convention, and European Union Directives, jurisdictions should criminalize money laundering and enable its competent authorities to confiscate the proceeds of crime.

The existence of legal and regulatory framework to combat money laundering and terrorist financing is the crucial and an integral element of a sound anti-money laundering and terrorist financing regime. Financial Action Task Force recommends that countries should criminalize money laundering and terrorist financing with a view to include the widest range of predicate offenses.

Although Afghanistan is not a financial center, the proceeds of drug, corruption and bribery, illegal extraction of mines, tax evasion, forgery, contraband, human smuggling, and usurpation of lands are shaped pieces of money laundering.

Afghanistan's first Anti-Money Laundering and Proceeds of Crime law was passed in 2004 with the purpose to prevent the use of financial institutions for money laundering and terrorist financing. Mutual Evaluation of Afghanistan had been undertaken in 2011[1], identified significant deficiencies in the legal and regulatory framework of anti-money laundering regime. Since then, Afghanistan has adopted the new anti-money laundering and terrorist financing laws and regulations to assimilate with FATF recommendations and other conventions.

LEGAL FRAMEWORK

1: Anti-Money Laundering and Proceeds of Crime Law

The Anti-Money Laundering and Proceeds of Crime Law (AML-PC) was adopted and published in official Gazette # 1142 in July 2014. The law was then amended in April 2015.[2] The purpose of the AML-PC law is to protect and promote the financial integrity of Afghanistan and fight against the use of financial institutions and designated non-financial businesses and professions (DNFBPS) including Insurance Companies (ICs), for money laundering, proceeds of crime, the proliferation of weapons of mass destruction and the financing of terrorism. The amended AML-PC law meets the action plan items agreed with the International Cooperation Review Group of Financial Action Task Force (ICRG/FATF)[3]. The law defines the predicate offense as:

> *"Predicate offense means any criminal acts resulted in funds or properties, whether directly or indirectly irrespective of whether the offense is committed inside or outside the country. These offenses shall include all categories of offenses prescribed by FATF standards, including piracy in the high sea."*

The categories of offenses listed by FATF are;

- *"Participation in an organized criminal group and racketeering;*
- *Terrorism, including terrorist financing;*

- *Trafficking in human beings and migrant smuggling;*
- *Sexual exploitation, including sexual exploitation of children;*
- *Illicit trafficking in narcotic drugs and psychotropic substances;*
- *Illicit arms trafficking;*
- *Illicit trafficking in stolen and other goods;*
- *Corruption and bribery;*
- *Fraud;*
- *Counterfeiting currency;*
- *Counterfeiting and piracy of products;*
- *Environmental crime;*
- *Murder, grievous bodily injury;*
- *Kidnapping, illegal restraint and hostage-taking;*
- *Robbery or theft;*
- *Smuggling; (including in relation to customs and excise duties and taxes);*
- *Tax crimes (related to direct taxes and indirect taxes);*
- *Extortion;*
- *Forgery;*
- *Piracy; and*
- *Insider trading and market manipulation."*[4]

In addition to the definition of the predicate offense provided in AML-PC law, another set of dominating laws in Afghanistan criminalizes most of the predicate offenses listed above.

Money Laundering Offense: The money laundering offense defined in article # 4 of the Anti-Money Laundering and Proceeds of Crime law, criminalizes money laundering in compliance with recommendation # 3 of the FATF and meets the international standards, particularly the elements of article # 6 of the United Nations Convention Against Transnational Organized Crime (Palermo Convention).[5] In general, the money laundering offense includes; (i) the conversion or transfer to conceal the illicit origin of the property, (ii) concealing the true nature of the property, (iii) possess and use of the property derived from predicate offenses, (iv), engage, participate, attempt or enter into arrangement knowing that the property is derived from illicit activity, and (v) assisting, organizing, supporting or facilitating another person to do so.

An important element of the money laundering offense is "knowledge" which may be inferred from the objective of factual circumstance. As Afghanistan had few money laundering convictions, hence use of the legal principles to infer "willful blindness" or "deliberate avoidance of the knowledge of facts" would be an exercising gap for investigators and prosecutors.

2: Counter Financing of Terrorism Law

Counter Financing of Terrorism (CFT) law had been passed in September 2014 and then amended in April 2015[6]. The CFT law criminalizes terrorist financing in compliance with recommendation # 5 of the FATF. The purpose of this law is implementing the International Convention for the Suppression of Financing of Terrorism (1999) and its successor conventions, prevent the provision of funds or property for terrorist acts, terrorist organizations, or terrorist (s); and Implement UN Security Council Resolutions on combating the financing of terrorism and the financing of proliferation of weapons of mass destruction.

In addition to the CFT law, the new penal code also criminalizes terrorist financing. Terrorism offenses defined in the new Penal Code include acts such as suicide attack, crimes against persons, use of explosive or lethal devices, dissemination or destruction of the nuclear or radioactive materials, destruction of infrastructure, acts against the airport, ship or fixed platform safety, control over an aircraft or ship, hostage taking for terrorism purposes and the establishment of terroristic organization and its membership. The above acts against the Government of the Islamic Republic of Afghanistan or foreign country, national and international organizations are criminalized. The punishment for accomplice, accessory, starter, and conspirator are the same as principle offender.

INSURANCE SECTOR

Why is AML/CFT Program essential to an Insurance Company?

Insurance is a contract which is represented by a policy that an individual or entity receives financial protection against losses from an insurance company. Insurance Policy is used to hedge against the losses that may result from damage or liability for damage.[7] Insurance Company (IC) is a business that provides financial coverage in the form of compensation against losses, injury, treatment, and damages. Insurance companies are risk takers and calculate the risk of occurrence and determine the premium which should be paid by the insured person. Insurance companies are vulnerable to money laundering and terrorist financing due to their nature of the business. ICs should avoid the potential use of their businesses by criminals for the purpose of money laundering and terrorist financing. Some of the indicators for the life insurance, annuities, and other policies are; (i) early termination without business reason or looking to a free cancellation period, (ii) overpayments, (iii) purchase of the product inconsistent with customer needs, (iv) structuring, (v) injecting the proceeds of crime into the system, (vi) unusual payments, and misuse of the product by agents or broker as they have sale motive rather than being compliance staff or unwitting.

Insurance companies are exposed to reputational, operational, legal, and concentration risks. The key side effect of the reputational risk is the loss of confidence and integrity in the market. Inadequate or failed internal processes, people, system, and fraud are the exposures of operational risk. In the event, IC doesn't have adequate AML/CFT compliance program, there might be the high-risk of lawsuits and adverse judgments against the IC which is also flagged as the legal risk. Without proper due diligence and risk assessment, concentration in risky products, sector, and geography are the main streams of concentration risk. Board of directors and AML/CFT compliance officer of the IC should make sure that their organization is not exploited by money launderers and terrorist financiers.

Insurance Sector of Afghanistan

The insurance sector of Afghanistan is very small and limited.

A total number of four insurance companies are present in the country offering the travel, personal accident, fleet motor, fleet aviation, construction, cargo, transit, property, and professional indemnity types of insurances. Afghanistan Insurance Authority (AIA) was established in 2005 which had been housed in the Ministry of Finance. AIA is the licensing and supervisory authority of the insurance companies in Afghanistan. Cornerstones and responsibilities of the authority are; (i) issuing product licenses, (ii) issuance of license to insurance companies, brokers, agents, survivors, loss adjusters, audit companies and insurance consultants, (iii) avoid illegal insurance activities, (iv), on-site and off-site supervision of insurance companies, (v) to appoint external audit company for insurance companies, (vi) to propose amendments to the insurance law, and (vii) drafting regulations, policies and procedures to the sector.[8]

The legal basis for having AML/CFT program in the Insurance Company

Based on the article # 5 of the Anti-Money Laundering and Proceeds of Crime Law, Insurance Company is called "Reporting Entity". Relevant articles of the law are compulsory applicable on ICs. In the event of non-compliance, the penalties and enforcement actions specified in article # 24 of the law are enforceable by competent authorities.

The international standard for having AML/CFT program in the Insurance Company

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standards.[9] Based on the FATF 40 recommendations, insurance companies should comply with relevant recommendations. In the event, insurance sector is not covered in the AML/CFT legal framework of the country, this might be considered as a deficiency during the

mutual evaluation of the country. To meet the best international practices, Afghanistan legal and regulatory framework is now in par with FATF standards.

AML/CFT GUIDANCE NOTES

This article is not the interpretation of legal framework or bypasses the legal responsibilities of the insurance companies. This is only a non-exhaustive list of notes which can be considered by insurance companies. Most importantly, IC should have their own AML/CFT policies and procedures which should be approved by the board of directors. The policies, procedures, and guidelines should assess the adequacy of the AML/CFT program in line with the risk and context of each business.

1. AML/CFT Compliance Program

The fourth group of Financial Action Task force recommendations (9-23) describes preventative measures both for the financial and non-financial businesses and professions, including ICs. This set of recommendations covers the customer due diligence and record keeping, secrecy laws and tipping off, correspondent banking and MVTS, new technologies, reporting of suspicious transactions, reliance on third parties and internal controls, high-risk countries and additional measures for specific customers and activities.

The AML-PC law and the FATF standards require all financial institutions, including ICs to develop effective frameworks, preventive measures, systems, controls, and practices to manage their potential money laundering/terrorist financing (ML/TF) risks. Financial institutions should have adequate controls and procedures in place to know their customers with whom they are establishing business relationships. Adequate due diligence on new and existing customers is an important part of these controls.

In general, a good AML/CFT compliance program includes the following pillars;

- Policies, procedures, and internal controls;
- Compliance function;
- Comprehensive training program; and
- Independent audit function.

The program should also include the role of the board of directors and identified deliverables for internal control measures. FATF requires that financial institutions, including ICs should have internal controls in place aimed to minimize money laundering and terrorist financing risks. Article # 19 of the dominant Anti-Money Laundering and Proceeds of Crime law of Afghanistan requires reporting entities, including ICs to develop programs for the prevention of money laundering and terrorist financing.

2. AML/CFT Policy and Procedure

The existence of AML/CFT policies and procedures are very important for ICs. Policy is the general voice of the organization and high-level controls. Procedure (s) is to explain how the policy will be implemented in practice. The existence of policies and procedures are vital components of the combating abilities for ICs. Even though simplified processes should be the outcome of comprehensive risk assessment, the AML/CFT policy should describe if there are areas of simplified approaches, waivers or exemptions.

The policy should be approved by the board of directors, reviewed regularly and updated as necessary at least every two years. The voice should be given to all sections and employees of the organization that policy implementation will cover all including any global presence. Employees should be required to comply with AML/CFT standards in an ethical manner. Any failure in this part may push the ICs into the reputational risk and doing business dilemma.

The policy should reflect the responsibilities of all stakeholders and list all the criminal, civil, and disciplinary actions and penalties which will harm the IC as well as employees. The Standard Operating Procedures (SoP) should be detailed, cover all day to day operations and working practices. All vulnerable areas should

be served with adequate control. The internal controls may vary, including management reports and built-in safeguards. If necessary; dual control, maker and checker, and/or second review or approval should be incorporated into the SoP. Internal control measures should at least form the, (i) senior management oversight, (ii) policy approval, (iii) customer identification, verification, acceptance and rejection of customer, (iv) SAR/STR reporting, (v) record keeping, (vi) thresholds and limits, (vii) staff screening, (viii) dual control, built in safeguards and electronic parameters set in electronic platform.

3. AML/CFT Compliance Function

Anti-Money Laundering and Proceeds of Crime Law of Afghanistan requires ICs to ensure implementation of the legislation. It is highly recommended that ICs should have an independent compliance department with adequate resources, including staff to ensure implementation and to enforce combating indicators. Chief Compliance Officer (CCO) should have required qualifications and relevant expertise. Board of directors appoints the CCO and approves his/her sufficient authority to implement the day to day compliance functions. In some instances, the CCO might be approved or provided with "No - Objection" by the supervisory authority to ensure the criteria of being fit and proper person. Being a responsive function, CCO is administratively hung under executive board, but the line of reporting is vectored to the board of directors unless otherwise described differently in approved AML/CFT policy. CCO is responsible for coordinating and monitoring the day to day compliance issues of the IC. Although the compliance function within each IC might look differently in terms of size and structure of the department; main responsibilities of CCO leading the compliance functions shall be, (i) risk assessment of the products, customers, and delivery channels, (ii) to ensure that policies, procedures, and internal control measures are complete and up to date, (iii) leading and coordinating the implementation of policies and procedures, (iv) monitor changes to the laws, regulations, circulars, and guidelines issued by the AIA or any other competent authority, (v) develop and implement knowledge adequacy program for compliance, customer facing, and other AML/CFT related staff, (vi) investigating the money laundering red flags, parameters, alerts, and filing the STR/SAR within three working days after the formation of suspicion to the Financial Intelligence Unit, (vii) responding to supervisory authority, Financial Intelligence Unit and any other competent law enforcement agency or government body, and last but not the least (viii) to ensure implementation of the AML/CFT legislation, circulars, and instructions issued by competent bodies.

A dedicated stand-alone compliance department should at the minimum, include the sub-units of, (i) Know Your Customer (KYC), (ii) Sanction Screening, (iii) Transaction Monitoring, (iv) Investigation, and (v) Program Management.

The staff of the compliance department needs to be knowledgeable, experienced, and should have high values of ethical standards. "Enemy within the Organization" is a concern for ICs as well, therefor ICs should ensure to have the proper employees' onboarding and regular screening. If necessary, ICs should conduct the due diligence on third parties as well. Anti-Money Laundering and Proceeds of Crime Law of Afghanistan (Article # 19) requires the reporting entities, including ICs to adopt adequate screening procedures to ensure high standards when hiring employees.

As criminals are adopting new methods of money laundering and may try to own the financial institution as the front business or laundering machine; therefore, it is very important for the AML/CFT supervisory authority to set the requirements identifying the fit and proper person mainly for the executive officers, high-level managerial

positions, or any other person or legal entity who exercises influence or degree of control over the management and/or ultimately owns the business.

4. AML/CFT Training Program

International standards suggest that reporting entities should have an ongoing and written training program. Training is an important component of a good and effective compliance program. Anti-Money Laundering and Proceeds of Crime Law of Afghanistan (Article # 19) also requires the reporting entities, including ICs to conduct ongoing trainings for the officials and employees. Ongoing awareness and training will demonstrate the seriousness of ICs about AML/CFT standards. Staff should be regularly updated about their statutory obligations and mandates. Staff should know that each can be individually liable for the failure to perform their duties in accordance with the dominant legislation in the country. The training contents, coverage, frequency, levels, and completeness should reflect the knowledge needs. As a minimum, AML/CFT training should cover the operation, customer facing, compliance, audit staff, and senior management. Audit as the third-line of defense should make sure about the relevancy, frequency, contents, and evaluation results of the training during the process of regular audits. A good training plan should describe, (i) what to train, (ii) who to train, (iii) how to train, and (iv) when to train.

5. Independent Audit Function

In order to ensure the effectiveness of the AML/CFT compliance program, the internal audit within the ICs should test the program. Internal audit should attest the overall effectiveness, controls, transactions, assess employees' knowledge, adequacy, accuracy and completeness of training, process of identifying suspicious activity, timely reporting, and effective corrective actions.

Recommendation # 18 of FATF and article # 19 of the Anti-Money Laundering and Proceeds of Crime Law of Afghanistan require the reporting entities, including ICs to have internal audit arrangements to check compliance with legal and regulatory requirements and effectiveness of the measures taken place to apply the mentioned legislation. Audit function should be independent; compliance department or its staff shouldn't be involved in the audit process as the audit will assess the implementation of planned activities including functions being carried out by the compliance department as well. Internal audit department or cell of the ICs should directly report to the board of directors or its sub-committee defined and approved by the board. Chief Internal Auditor should be assigned by the board. If needed or instructed by AIA or any other competent authority, external auditors might be selected by the AIA to review the adequacy of the compliance program including AML/CFT controls. ICs should constantly keep their eyes open in deterring money launderers and terrorist financiers from making use of them or exploiting their products or delivery channels. Please note that an excel file titled "AML/CFT Compliance Check-List" is also prepared to summarize the key functions of internal audit and other parts of this article. These notes or the check-list are not mandatory obligations and just for guidance.

6. Sanctions Implementation

Implementation of sanctions by reporting entities is essential not only for their domestic obligations as well as international. Failure to comply with sanctions may result in penalties and reputational risk. In accordance with the Counter Financing Terrorism Law, Anti-Money Laundering Law, Standing Freezing Order of the Attorney General's Office, and relevant procedures; ICs shall continuously comply with the freezing order, avoid any type of transaction with designations and immediately freeze the cash, bank account, movable and immovable assets and any other type of funds, properties and transactions.

As per the standing freezing order, frozen funds and properties should be immediately reported to the Office National Security Council and Attorney General's Office through the relevant regulatory bodies. As per the Counter Financing Terrorism Law and CFT Regulation, any person who makes available, directly or indirectly, any funds, property, economic resources or financial and/or other related services available to or for the benefit of designated persons shall commit an offense. Meanwhile, whoever fails to implement the freezing order shall commit an offense as well.[10]

ICs should obtain the domestic and international sanctions list from the competent authorities and screen their customers not only on-boarding but also on real-time basis. It is highly recommended that this process be made through the electronic platform and prioritize "False Negative" and "False Positive" matches respectively.

Sanctions screening should be implemented before the establishments of the business relationship and on on-going basis. The reason to have it on real-time basis is that national and international sanctions get updated on a regular basis. Most of the financial organizations do prefer to have the electronic platform for screening purpose.

7. Customer Due Diligence (CDD)

Customer due diligence is also an integral element of the compliance program. An effective customer due diligence and verification process, improves the combating abilities of ICs. Financial Action Task Force (Rec 10) requires reporting entities to undertake customer due diligence when; (i) establishing business relations, (ii) carrying out occasional transactions, (iii) above the applicable designated threshold, or (iv) there is suspicion of money laundering or terrorist financing, and (v) the institution has doubt about the veracity or adequacy of previously obtained documents.

Based on the article # 12 of the dominant Anti-Money Laundering and Proceeds of Crime Law, ICs should conduct the following measures on the beneficiaries of the life insurance and other investment products and policies:

- *"For beneficiary (ies) that are identified as named natural or legal persons or legal arrangements – taking the name of the person; and*
- *For beneficiary (ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary."*

ICs should conduct due diligence of customers with whom they are dealing. An important step of due diligence is to develop customer identification, acceptance, rejection, screening, and verification policies and procedures. It is recommended that customers information should be regularly updated based on their risk profile. In order to allocate the resources and prioritize the vulnerabilities, it is also recommended that customer due diligence should be conducted on risk-based. As minimum, customer due diligence should cover the followings:

- Identifying and verifying of customer's identity and documents using reliable sources. E-IDs and online registries are very helpful in the process of verification. Verification can be carried out using the "Documentary" and "Non-documentary" process. This piece of CDD is crucial. In general, verification of the identification should take place at the time of onboarding and relationship is established, verification may also take place or allowed after the insurance contract is signed with the policyholder if the money laundering and terrorist financing risks are

managed effectively and shall be before the payout is made.

- If the customer is acting on behalf of others', reasonable steps should be taken to identify and verify the subject behind.
- Information about the nature of business and intended purpose of the relationship.
- Identify the beneficial owner (s).
- Risk scoring of the customer. The general categories are "High, Medium, and Low". As an example, Politically Exposed Person (PEP) is a high-risk customer due to its access to the public fund and resources. The indicators which are important for risk scoring are the type and the background of the customer, beneficial owner, source of payment, means of payment, nature of the activities, source of wealth, source of fund, business relationship, role and involvement of third parties, and any other indicator which is found material during the risk assessment.
- Customer identification requirements for the natural person could be; full name of the individual, including alias and family name, father name, business name if sole trader, gender, marital status, national identification (Tazkira or Passport), complete address, nationality, date of birth, occupation and organization, income and source of income, phone number, latest photo, assets, signature or fingerprint, and any other information described in policies and procedures. These requirements could be listed as mandatory and optional considering the type and category of customer.
- Customer identification requirements for the legal person could be; legal name of the business, certificate of incorporation, nature of business, tax identification certificate or clearance certificate, articles of association, partnership agreements if any, trust deed, complete address, phone, mobile and fax number (if available), name and contacts of board members, identification of board members, shareholders and senior management, authorization documents, signature or fingerprint, and any other information listed in policies and procedures. These requirements could be listed as mandatory and optional considering the type and category of business.

Enhanced Due Diligence (EDD): Financial Action Task Force requires countries to conduct money laundering and terrorist financing risk assessment. Financial institutions and designated non-financial businesses and professions are not exempted from the requirements to apply enhanced due diligence measures when high-risk scenario is identified.

Article # 11 of the Anti-Money Laundering and Proceeds of Crime Law mandates reporting entities to conduct enhanced due diligence measures where the risk of money laundering and terrorist financing is identified. In addition, article # 12 of the above-mentioned law requires reporting entities to conduct enhanced due diligence in circumstances that have been identified as high risk. It is also recommended to apply enhanced due diligence to all complex, unusual, or large transaction which has no apparent economic purpose.

In terms of differentiating the customer due diligence and enhanced due diligence, additional information, including but not limited to the sources of fund and wealth, approval of senior management, enhanced on-going monitoring, requiring verified certification from competent authorities, enhanced due diligence on the veracity and validity of identification and/or registration

documents, structure of the corporate business and beneficial owners, and other relevant information can be collected to support the enhanced due diligence objectives.

Politically exposed person: Financial Action Task Force defines domestic PEP as; *"Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.*

Article # 15 of the current Anti-Money Laundering and Proceeds of Crime Law also requires reporting entities, including ICs to have appropriate risk management systems to determine whether the customer or beneficial owner is a politically exposed person or not, obtain senior management approval, and conduct enhanced monitoring of the business relationship.

Board of directors should also approve a client acceptance policy with regard to PEP. This part of the policy will impact the reputation of the organization, especially when any money laundering scam is identified by law enforcement agencies.

Simplified Customer Due Diligence: Financial Action Task Force recommends that financial institutions and designated non-financial businesses and professions should identify, assess and take effective actions to mitigate their money laundering and terrorist financing risk.

Where countries identify higher risks, they should ensure that their combating regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions. A key model to identify the products for the financial inclusion is the national money laundering and terrorist financing risk assessment. Internally, the financial and non-financial institutions can also assess their risk and identify the low-risk products, customers, and delivery channels.

Article # 11 of the current Anti-Money Laundering and Proceeds of Crime Law allows the reporting entities to conduct simplified approaches of due diligence where the risk of money laundering and terrorist financing is identified as low. This is critically important to observe the quality of assessment which labels the products, customers and distribution channels as the high, medium and low risk.

Overlooking to the quality of assessment, may misguide the practitioners. In regard to ICs, AML/CFT regulator can look into the compliance program, risk and context of each insurance company separately. In some jurisdictions, the regulator sets the thresholds and identify the product (s) which can be allowed for simplified due diligence. Simplified CDD shall not be applied if there is suspicion of money laundering or terrorist financing or specific higher risk scenario (s).

Based on the international best practices, including FATF recommendations, it is possible to rely on third parties for customer due diligence, but the ultimate responsibility of due diligence remains with the IC relying on third parties.

8. Reporting STR/SAR

Although Currency Transaction Report (CTR) or Large Cash Transaction Report (LCTR) are reporting requirements in some jurisdictions, reporting suspicious transaction is very important to combating money laundering and terrorist financing both for financial and non-financial businesses and professions.

Filing STR/SAR is the final output of the compliance program in financial and non-financial businesses and professions, including

ICs to minimize the money laundering and terrorist financing risks. FATF recommends that if a financial and non-financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required by law, to report promptly its suspicions to the financial intelligence unit. The word promptly is reflected in domestic legislation within three working days as the ceiling.

Based on the article # 18 of the Anti-Money Laundering and Proceeds of Crime Law, reporting entity should report the suspicious transaction where the reporting entity suspects or has reasonable ground to suspect that the transaction or the attempt is proceeds of crime, or be used for money laundering or terrorism financing or related to terrorists or used for terrorism as soon as practicable but no later than three working days to the financial intelligence unit.

Reporting entity should report STR/SAR even if it becomes evident after the completion of the transaction. The reporting entity shall immediately report the updates and additional information which may confirm or invalid the suspicion. Reporting entities and their staff are prohibited by law not to disclose to the relevant customer or any other person that STR/SAR is filed with the Financial Intelligence Unit. Any violation would be subject to criminal penalty.

Board of directors, senior management, compliance and other staff of the ICs including internal audit should know that reporting STR is a legal obligation, the violation might be considered a criminal act. It protects the organization from allegations of collusion, supports the law enforcement agencies and the financial intelligence unit to investigate and prosecute criminals and protects the reputation of the organization.

STR should be investigated internally by the "Investigation Unit" of the Compliance Department of the IC. Once the suspicion is formed, it should be reported immediately. About the details of the process, search the public domain or website of the Financial Intelligence Unit for a collection titled "How to File a Good STR?".

The reporting templates are available on Financial Transactions and Reports Analysis Center of Afghanistan (the Financial Intelligence Unit) website.[11]

9. Record Keeping

Record keeping requirements apply to the designated non-financial businesses and professions including ICs. Based on the international best practices, ICs should keep the records for at least five years. The regulator can ask the ICs to keep the records for longer period especially records and documents which form the suspicion of money laundering and terrorist financing.

Based on article # 16 of the Anti-Money Laundering and Proceeds of Crime Law, reporting entities should maintain records on attempted or executed transactions for at least five years following the execution or attempt of the transaction or longer if required by the competent authorities. Record keeping requirement includes the records on identification and verification through the CDD and EDD measures, STR supporting documents, files and business correspondence.

10. Enforcing Compliance

In addition to criminal penalties mentioned in Anti-Money Laundering and Proceeds of Crime Law, article # 24 of the mentioned law empowers the Financial Intelligence and other competent supervisory authorities to enforce compliance.

The unit and any other supervisory authority can impose the following sanctions;

- Issuance of warning letters;
- Issuance of suspension orders;
- Revocation of business license;

- Impose the fine ranging from AFN 50,000.00 to 500,000.00 for every infraction;
- Order to conduct the external audit at cost of IC which will be selected by the competent authority.
- Remove the administrator or any other employee;
- Cease engaging in certain actions or practices; and
- Take corrective actions.

There are rooms for the contest, which should be dealt with by the Financial Disputes Resolution Commission (FDRC)[12].

This summary of AML/CFT Notes, should not be considered as the exhaustive list or legal obligations. ICs should consult with the relevant competent bodies for their legal obligations. ***

ENDNOTES:

[1] IMF, 2011. "Islamic Republic of Afghanistan: Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism." https://www.imf.org/external/pubs/ft/scr/2011/cr11317.pdf

[2] DAB, 2015. "Amendments of Anti-Money Laundering and Proceeds of Crime Law." http://dab.gov.af/Content/Media/Documents/AMLLawEnglish121201510361265555333325325.pdf

[3] ICRG, 2012. "Action Plan." http://apgml.org/my-apg/default.aspx

[4] FATF, 2012. "The FATF Recommendations." http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[5] UN, 2000. "United Nations Convention Against Transnational Organized Crime." https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

[6] DAB, 2015. "Counter Financing of Terrorism Law." http://dab.gov.af/Content/Media/Documents/CFTLawEnglish121201511382982955332532 5.pdf

[7] Investopedia, 2018. "Insurance." https://www.investopedia.com/terms/i/insurance.asp

[8] MOF, 2018. "Insurance Affairs Department." http://mof.gov.af/en/page/14369/dm-amin/insurance-department

[9] FATF, 2018. "Financial Action Task Force." http://www.fatf-gafi.org/

[10] AGO, 2016. "Standing Freezing Order." http://fintraca.gov.af/assets/Freezing%20Orders/Standing%20Instruction_(Freezing%20Order)_English(1).pdf

[11] FinTRACA, 2018. "Website." http://fintraca.gov.af/Default.html

[12] FDRC, 2018. "Website." http://fdrc.gov.af/