Frequently Asked Questions (FAQs) On Anti-Money Laundering and Countering of Terrorism& Proliferation Financing (AML/CFT/PF)

SECP

SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN

Sixth Edition

Updated – November 2024

SECP is pleased to publish this updated version of Frequently Asked Questions (FAQs) on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT). The purpose of these FAQs is to facilitate understanding of SECP's regulated persons (RPs) under the AML/CFT regime, and to meet evolving regulatory expectations for anti-money laundering and sanctions compliance. This batch is specially focused on topics relating to Customer Due Diligence (CDD), Politically Exposed Persons (PEPs), Targeted Financial Sanctions (TFS) and other AML/CFT related obligations.

Note: The following FAQs have been prepared for illustrative purposes only. The FAQs do not constitute legal advice or have any legal merit on the subject. In the event of any inconsistency between these FAQs and any laws, rules or regulations the provisions of such laws, rules or regulations shall prevail.

1- What should be the frequency for updating customer due diligence (CDD) information with respect to existing customers?

SECP Regulation 19 (Ongoing Monitoring) requires a regulated person to conduct ongoing due diligence on the business relationship by undertaking reviews of existing records and ensuring that documents data or information collected for CDD purposes is up to date.

In this regard, it is advised that using the risk rating that the regulated person has assigned to each customer at the time of customer onboarding, the due diligence of existing customers should be carried out as under:

- CDD information of customers categorized as "High Risk" shall be reviewed/updated each year.
- CDD information of customers categorized as "Medium Risk" shall be reviewed/updated at least once in every three years while CDD information of customer categorized as "Low Risk" shall be reviewed/updated at least once in every five years.
- RE may determine the respective frequency for review/update of customers falling in different risk categories and include the same in their internal policy.
- Moreover, CDD information of customers shall be updated immediately whenever material information regarding the customers becomes known or there is a suspicion of money laundering or terrorist financing or there are doubts about the veracity or adequacy of previously obtained data.

2- Should we rate all such customer as High Risk whose sectoral vulnerability have been rated as high in the National Risk Assessment irrespective of the RP's internal risk tolerance/assessment based on various parameters such as amount invested, CDD performed and documents obtained?

At the outset it should be noted that a sectoral vulnerability can't be construed as a final risk rating for a specific client. Risk categorization of a customers is based on combination of factors such as customer, product, geography and delivery channel, which varies on a case by case basis. Furthermore, SECP Regulation 4 *Risk Assessment*, requires the regulated person to take appropriate steps in accordance with section 7F *Risk Understanding* of the AML Act 2010 ("AMLA"), to identify, assess and understand its money laundering, and terrorism financing risks for customers, geographic areas, products/services, transactions and delivery channels. An assessment of all four factors will result in an applicable rating. NRA provides guidance for overall sector while risk rating of each client is dependent upon Internal Risk Assessment by every entity after accommodating combination of abovementioned four factors.

As a rule of thumb, National Risk Assessment (NRA) allows a country to identify, assess and understand its money laundering and terrorist financing risks at the national/sectoral level. Once these risks are properly understood, appropriate AML/CFT measures that correspond to the level of risk identified may be applied using the risk-based approach (RBA) as prescribed by FATF Recommendation 1.

For additional guidance please refer to Chapter II Risk and Mitigation, SECP AML/CFT Regulations 2020. Link: SRO 921 (I)/2020 Securities and Exchange Commission of Pakistan (AML/CFT)

Regulations, 2020 | SECP and section 5 of SECP AML/CFT Guidelines 2021.

3- Is the Wealth Statement reported to Tax Authorities with a client's Income Tax Return helpful for enhanced verification of the Source of Wealth (SoW) and Source of Funds (SoF) of a customer?

While the Income Tax Return and Wealth Statement provide some insight into a customer's financial position, however, they do not fully establish the source of wealth or funds. These documents primarily serve as evidence regarding potential predicate offenses like tax evasion. To conduct a thorough verification of SoW and SoF, the reporting entity should assess whether these documents provide sufficient information about the SOW and SOF. In cases where these documents do not provide sufficient evidence or do not establish the SOW and SOF, additional specific information and documents on the SoF and SoW, ensuring transparency of the origin of assets should be obtained. Examples of such circumstances include receipt of funds subsequent to the filing of wealth statement, liquidation of any fixed asset for the purpose of investment etc.

Further, for high-risk customers or transactions, it is essential to apply additional measures in line with global best practices and FATF recommendations. Examples of these enhanced CDD measures include:

i. Obtaining additional customer information, such as occupation, asset volume, or publicly available data, and regularly updating customer identification and beneficial owner identification data.
ii. Gathering more details on the intended nature of the business relationship, including its duration and purpose.
iii. Seeking explanations for intended or completed transactions to assess whether they align with the expected profile of the customer.
iv. Securing senior management approval before initiating or continuing business relationships in high-risk cases.
v. Implementing enhanced monitoring, increasing scrutiny on the customer's transactions, and flagging patterns for further review.
vi. Requiring the first payment to be made from a bank account in the customer's name, which is subject to equivalent Customer Due Diligence (CDD) standards.

These additional measures, combined with the wealth statement, provide a more comprehensive and reliable method of verifying the customer's source of wealth and funds, thereby strengthening the overall integrity of the process.

4- Can we offer a low risk product with Simplified Due Diligence to a high-risk customer?

At the outset, it may be noted that the risk categorization of a customers is based on combination of factors such as customer, product, geography and delivery channel. If a high-risk customer intends to purchase a low risk product, he/she will be subjected to Enhanced Due Diligence (EDD) measures. Please note that under apply simplified Regulation 23, the RPs may due diligence after lower risks have been identified through proper risk assessments, but not when there is suspicion ofML/TF.

As per Regulation 6 of SECP AML/CFT Regulations 2020, *"The regulated person may take simplified measures to manage and mitigate risks, if lower risks have been identified. Simplified measures should not be permitted whenever there is a suspicion of ML/TF'*. Based on the aforementioned, high risk customer can only be offered low risk product after performing EDD.

5- What should be the time-frame for categorizing an individual as PEP after he/she has been relieved from assigned services?

FATF Recommendation 12 defines a PEP as someone who is or has been (but may no longer be)

entrusted with a prominent public function. FATF Guidance on PEPs recommends an open-ended approach (i.e., "once a PEP – could always remain a PEP"). Accordingly, handling of a client who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits.

The risk-based approach requires that financial institutions and DNFBP's assess the ML/TF risk factors of a PEP who is no longer entrusted with a prominent public function, and take effective action to mitigate this risk. Possible risk factors include:

- the level of (informal) influence that the individual could still exercise and the seniority of the position that the individual held as a PEP; or
- whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

In line with risk-based approach outlined above, the period for which a PEP, family members and close associates of a PEP, who is no longer entrusted with a prominent public function will be dependent on an assessment of the risk posed by that specific PEP.

6- What are the factors a financial institution should consider while performing Enhance Due Diligence (EDD) against PEPs to manage risks and mitigating controls with respect to a particular PEP?

Once identified, PEPs, their family members, and close associates may represent additional risk that requires appropriate management. The precise nature and magnitude of that risk and commensurate risk mitigations, however, may vary widely. Factors that affect risk relating to PEPs may include but not limited to the following:

a) the perceptions of corruption and financial transparency in the PEP's country of citizenship;
b) the nature of the political exposure;
c) the nature of the relationship with the PEP, in the case of family members and close associates;
d) the elapsed time since the PEP held the position(s) that qualified him to be a PEP;
e) the nature of the claimed sources of funds and the ability to fully and confidently verify those sources and their legitimacy;
f) has business interests, which are related to his/her public functions (conflict of interest);
g) involved in public procurement processes; where the PEP holds several (related or unrelated) prominent public functions that may enable influence to be exerted at several key decision-making points in a process, especially relating to payments;
h) holds a prominent public function in sectors known to be exposed to corruption; or
i) holds a prominent public function that would allow him/her to exert a negative impact on the effective implementation of the AML/CFT framework in the country.

7- Can a self-declaration form suffice for identifying a Politically Exposed Person (PEP) in order to perform relevant CDD obligations?

Please note that solely relying on self-declaration by a customer may not be an appropriate customer due diligence (CDD) measure in terms of AML/CFT Regulatory framework. RPs should undertake steps to not only identify but also verify that the self-declaration is valid.

Moreover, many customers would not be able to determine if they are indeed a PEP, or not, for example because the customer may not be aware of the definition of a PEP, family member or close associate of a PEP as defined in SECP Regulations 3(g), (m) and (q).

To establish PEP status, RPs should actively engage with customers and obtain information relevant to establish different elements of the PEP definition. To do this effectively, well-trained staff and effective information gathering using 'PEP search softwares' or through public databases such as Election Commission, parliamentarian's tax directories, public website/disclosures by Public sector organizations and other public search portal etc. should be used and document for record keeping purposes.

8- If the client makes payments through banking instruments to an NBFC, insurance service

provider or a securities broker or any other SECP regulated person (RP) for the execution of transactions in its account, then can we assume that the said client payments should not be subject to further KYC/CDD inquiries by the RP, since it is presumed that the same is already inquired from the client by its respective bank?

While routing of funds through banks is considered a safe mechanism under the risk factor of 'Delivery channel', however it may please be noted that risk assessment and rating of a customer depends on the other three factors as well namely customer, product, and geography.

It is important to note that as per FATF, AML/CFT obligations are imposed separately on every financial institution that is providing financial services. Hence in this case, banks are not responsible for the obligations of a SECP RP, and the responsibility for compliance with the AML/CFT Regulations will rest with the SECP RP.

In case the bank shares the KYC documents or information of a customer (For example in the case of Roshan Digital Accounts-RDA) to facilitate the process of customer onboarding at the RP's end, SECP regulations allow a mechanism for third party reliance on CDD. RPs may avail this facility after complying with the relevant requirements as specified in Regulation 24, Reliance on Third Parties". So, if banks share their CDD, and the RP is in compliance with requirements of Regulation 24, the RP can rely on it, otherwise, the RP must carry out its own customer due diligence measures.

9- Can a Regulated Person be engaged with technology solution provider for facilitating the process of KYC/CDD e.g. Technology solution for Facial/Biometric ID Verification, Screening solution providers etc. Can we treat reliance on such service providers being "Reliance on Third party" under Regulation 24?

RPs may use the services of a technology solution provider or outsourcing agency for verifying customer against the identity evidence provided, for example by using biometric solutions like facial recognition and liveliness detection to identify and authenticate during the onboarding process. However, it is important to consider the application of 'third party reliance' in such cases.

Please note that the FATF Recommendation 17 requires that a Third-party reliance can only be made in case the "Third party" is:

- a financial institution i.e. should be subject to CDD and record-keeping requirements in line with Recommendations 10 and 11, and be regulated, supervised or monitored
- have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures;

This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity. Hence the interpretive note to the Recommendation 17 states that it does not apply to outsourcing or agency relationships. Guidance in this regard is provided in 'FATF Guidance on Digital Identity'. Link: Documents - FATF Digital Identity Guidance.

10- What should be appropriate course of action for a client who continuously decline the provision of KYC/CDD information required in KYC form?

As required under section 7A of AML Act, every financial institution/ Regulated Person/Entity (RP/RE) has to conduct CDD while onboarding a customer into a business relationship. In case any RP is unable to complete CDD, section 7D of AML Act allows that "*the RP:*

a) shall not open the account, commence business relations or perform the transaction; or shall terminate the business relationship if any ; and
b) shall promptly consider filing a Suspicious Transaction Report in relation to the customer.

Where a reporting entity forms a suspicion of money laundering or terrorist financing, and

reasonably believes that performing the CDD process will tip-off the customer, the reporting entity shall not pursue the CDD process and shall file a STR"

Further, SECP AML/CFT Guidelines 2021 requires that in case of an existing customer, the RP *"will block accounts without identity document (after serving one-month prior notice) for all withdrawals, until the subject regulatory requirement is fulfilled. However, upon submission of attested copy of identity document and verification of the same from NADRA or biometric verification the block from the accounts shall be removed.*

For customers whose accounts are dormant or in-operative, withdrawals will not be allowed until the account is activated on the request of the customer. For activation, the regulated person shall conduct NADRA Verisys or biometric verification of the customer and obtain attested copy of customer's valid identity document (if already not available) and fulfil the regulatory requirements."

11- What factors a Regulated Person/Entity should consider while identification of geographic areas that may fall into High Risk Geography?

The high-risk geographies have already been communicated several times in outreach sessions and through risk assessment exercises. The National Risk Assessment (NRA) 2019 has provided a detail of high-risk geographies at the overall national level beside identifying characteristics of customers from towns and cities near porous borders areas and some other areas that may pose high risk for money laundering and terrorist financing. Determination of risk from a particular client will be based on a complete evaluation of the risk profile of the customer, not only in terms of geography, but also other components of risk that include type of customer, product/ services, and delivery channel being used.

The assessment of such areas should be based on following metrices:

Foreign Geographies	**Local/Domestic Geographies**
▪ FATF's monitored jurisdictions with respect to ML ▪ Countries sharing porous borders with Pakistan ▪ High Risk Foreign Jurisdictions for Transnational TF Risk ▪ Countries on FATF's Public Statement ▪ Countries having a Hostile Relationship with Pakistan	▪ Residence of designated and proscribed persons in a particular area ▪ Terrorism hit areas / No. of terrorist attacks ▪ Locations of attempted transactions by proscribed/designated person ▪ No. of Terrorism related STRs ▪ Bordering areas with hostile nations ▪ Negative media reports ▪ Sectarian violence ▪ No. of high risk NPOs and Madrassas

12- Why there is no objective straight-line AML/CFT requirement for all types of customers, why it has been subjective for the RPs to use their judgement under the AML/CFT Regulations for onboarding the clients?

The straight-line approach being referred is commonly known as 'Rule based approach' which is highly discouraged by FATF. The FATF emphasized that all FIs should follow risk-based approach wherein, money laundering and terrorist financing risk posed by any customers is subject to risk assessment by the regulated entity. Please note that for all clients onboarded digitally or face to face, the regulated entity is responsible for ensuring compliance with SECP's AML/CFT Regulations 2020. Therefore, it is required under SECP AML/CFT Regulations 2020 that RPs should formulate their "compliance program" in line with risk-based approach.

In order to provide guidance, RPs should go through a Good Practice Note on "Essential Elements of a Sound AML/CFT program" issued by International Finance Corporation (the World Bank Group) [link: https://bit.ly/3rJZN8q]. This guidance note provides comprehensive features of a compliance program of a financial institution. Further, in the context of SECP Regulated regime, please go through section 13 of SECP AML/CFT Guidelines to provide useful guidance to RPs for developing a better compliance framework.

13- Why no separate AML CFT Regulations being introduced for low risk sector/product?

Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is considered appropriate where there is little opportunity or risk of your services or customer becoming involved in money laundering or terrorist financing. SECP AML/CFT Regulations 2020 allows RPs to carry out Simplified Due Diligence (SDD) subject to the condition that ML/TF risk has been assessed as low.

A brief about SDD measures are already provided on SECP Website please refer to link: https://www.secp.gov.pk/faq/what-are-the-simplified-due-diligence-measure/

14- Should an individual be construed/ considered as an associated individual under the Sanctions regime merely on basis of familial/ blood relationship with a designated/ proscribed person?

The last para of Regulation-25 of SECP AML/ CFT/ CPF Regulations requires RPs to identify associates meaning individuals and entities acting on behalf of, or at the direction of designated/ proscribed persons using risk screening databases, watch lists, publicly known information or linkages on the basis of Government or regulatory sources, reliable media information, or regulated entity's own analysis, etc. However, a person, merely on the basis of his/ her relationship with the designated/ proscribed person, which is a naturally ascribed status, cannot be penalized.

15- In case screening of database leads to potential match with designated person, what are the actions required from the SECP RE?

As per Section II (2.4.1.1.i.v. & 2.4.1.1.i.vi.) of the MOFA Guidelines on the Implementation of UNSC Resolutions concerning TFS, Travel Ban, and Arms Embargo and Section II (4.6.1.1(a)vi.) of MOFA Guidelines on the Implementation of the UNSC Resolutions concerning TFS on Proliferation Financing, SECP RE is required to immediately place a temporary freeze on the assets of the potential match and convey this information to SECP for onwards sharing with the focal point at the Ministry of Interior for verification.

16- Which are the relevant authorities for verification of potential match under ATA, 1997?

Depending on the basis for proscription, the relevant authorities are as under:

Sanction Regime	Authority
Schedule-I of ATA, 1997	Secretary, Ministry of Interior
Schedule-IV of ATA, 1997	Home Secretary of the relevant province or Chief Commissioner, ICT

****