By Special Messenger

Government of Pakistan
Central Directorate of National Savings
ISLAMABAD

F.6(1) AML-IMPL/STR-Instructions/2020 November 27, 2020

Subject: **RED FLAG INDICATORS FOR CENTRAL DIRECTORATE OF NATIONAL SAVINGS (CDNS).**

I am directed to refer to the subject.

2. The National Savings (AML and CFT) Supervisory Board has prepared red flag indicators **(Annex-A)** in consultation with Financial Monitoring Unit (FMU) to identify the suspicion that could be indicative of money laundering and terror financing. Accordingly, CDNS being a reporting entity is required to promptly report such suspicions to FMU in terms of Sec-7(1) of Anti money laundering Act 2010(ALMA). It is pertinent to mention that failure to promptly report Suspicious Transaction Report (STR) shall attract substantial penalties as per AMLA, 2010 and the AML/CFT Sanction Rules,2020.

3. In this context, all Regional Directorates are instructed to make sure that NSCs are properly reporting STR in case of observance of any red flag while conducting the financial activities. Furthermore, exclusive training sessions will be conducted regarding the subject in near future.

4. For any query or information please feel free to contact at 051-9215401 and email to cdnsamlcell@savings.gov.pk.

5. This issues with the approval of the DG, National Saving.

Enclosure: As above.

Zaheer Abbas
Director (V&M)

→ **All Regional Directors.**

Copy to:

1. Director (Operation), Director (PD&M), Director (Legal), CDNS Islamabad.
2. Director, DIA Islamabad.
3. Principal TINS, Islamabad.
4. SO (CDNS), Finance Division, Islamabad.
5. Assistant Director (AML and CFT Supervisory Board), CDNS, Islamabad
6. Webmaster, CDNS Islamabad (With the request to upload the same on website).
7. PA to DG CDNS, Islamabad.

Scanned with CamScanner

Financial Monitoring Unit

RED FLAGS FOR STR REPORTING BY CENTRAL DIRECTORATE OF NATIONAL SAVINGS (CDNS)

PREPARED BY NATIONAL SAVINGS (AML & CFT) SUPERVISORY BOARD IN CONSULTATION WITH FMU

Introduction

CDNS is required to report Suspicious Transaction Report (STR) to the Financial Monitoring Unit (FMU) under Chapter –VII of the **National Savings (AML and CFT) Regulations**(S.R.O.956(I)/2020)(http://www.finance.gov.pk/budget/NS_AML_CFT_Regulations_2020.pdf) if CDNS suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity or money laundering or related to terrorist financing, including attempted transactions, regardless of their value or amount, as per the format prescribed by FMU and as required under AML Act.

Protection for the Reporting Entities and their Officers

Under Section 12 of AML Act 2010, "The reporting entities and their officers……shall not be liable to any civil, criminal or disciplinary proceedings against them for furnishing information required under this Act or the rules and regulations made hereunder in good faith."

Red Flags for CDNS

In order to identify some of the circumstances that could be suspicious in nature or that could be indicative that money is being laundered (ML) or used for terrorism financing (TF) purposes, below are some red flags which are specially intended as an aid for CDNS.

Red Flags for Client Behavior

1. Client is overly secretive or evasive (e.g. of who the beneficial owner is, or the source of funds).
2. Client is actively avoiding personal contact without sufficient justification and insists on interacting through another person or professional.
3. Client appears to be a third party / benamidar where beneficial owner is unknown.
4. The amount of funds being invested by client do not match with his/her socio-economic profile.
5. Forged or suspicious documents are submitted by client.
6. Client linked to adverse news / under investigation for any criminal activity.
7. Client is designated/proscribed under UNSCRs 1267, 1373 (4th schedule of ATA, 1997), other relevant UNSCRs, listed on OFAC or proscribed under the domestic laws like listed on FIA Redbooks, etc.
8. Client is Politically Exposed Person (PEP) or its family member or close associate and is linked to adverse news / under investigation for any criminal activity.
9. Same client using different locations, counters, or tellers in a single day.
10. Persons belonging to a same family conducting transactions frequently.

11. Group of related persons make deposits in same branch to avoid reporting or monitoring.
12. Client belongs to high-risk areas as identified in NRA.
13. Client is found to be of the origin or has links with high-risk countries (e.g. countries designated by national authorities or FATF as non-cooperative countries/ territories or the ones which have inadequate measures to prevent money laundering and the financing of terrorism).
14. When two entirely unrelated persons apply for joint investment (type-A or type-B) without having any plausible justification.
15. Client exhibits unusual concern with compliance with AML/CFT reporting requirements or other (AML/CFT) policies and procedures.

Red Flags for Transactional Pattern related to all products (including certificates, accounts, and prize bonds) wherever applicable

1. Nominee is not a close relative or change in nominee (for instance, to include non-family members).
2. Third party check is provided for investment.
3. Purchase of a long-term investment product followed shortly thereafter by a request to liquidate the position to get back the invested amount.
4. Overall investment quantum, account balance or transactional activity is not in line with customer's business, known means or stated purpose of product.
5. Client is frequently purchasing savings certificates / prize bonds through unusual payments in cash which do not commensurate with his/her profile.
6. Unusually high levels of investments or unusually large transactions in relation to what might reasonably be expected of clients with a similar profile.
7. When transactions are conducted without any apparent legitimate or economic reason.
8. Where multiple deposits are made by unrelated individuals.
9. Large cash is deposited followed by early withdrawal.
10. Where large deposits and withdrawals are made routinely, and the end of day balance is very low or nil.
11. When customer insists to buy multiple savings certificates / prize bonds through structured/broken cash transactions to avoid CTR reporting threshold (PKR 2.0 Million and above).
12. Two or more customers (Linked/associated with each other) working together to break one cash transaction into two or more transactions to evade the CTR reporting requirement.

13. Purchase of higher denomination Prize Bonds against cash without providing any plausible justification.
14. Encashment of higher denomination Prize Bonds without any plausible justification.
15. When customer is frequently converting one product into another (especially in the name of unrelated third party) without any plausible justification.
16. Numerous prizes are repeatedly/very frequently being claimed by the customer against wining prize bonds during a short span of time.

Immediate Actions to be taken by the concerned officers

In line with requirements of National Savings (AML and CFT) Regulations (S.R.O.956(I)/2020), if the Responsible Officer(s) observes one or more of these red flags, he/she will perform Enhance Due Diligence (EDD) and update the Know Your Customer (KYC) / Customer Due Diligence (CDD) information available with CDNS. Responsible Officer will make further inquiries or investigations from the customer with documentary evidence which shall be stored in line with record keeping requirements. In case customer is not able to provide documentary evidences to satisfy Branch Manager or the Branch Manager has reason for suspicion, a Suspicious Transaction Report (STR) shall be promptly filed with FMU: (https://goamlweb.fmu.gov.pk/PRD/Home).

Warning for Non-Compliance

Under Section 33 of AML Act 2010, “Whoever willfully fails to comply with the STR requirement as provided in section 7 or give false information shall be liable for imprisonment for a term which may extend to five years or with fine which may extend to five hundred thousand rupees or both.

Under Section 34 of AML Act 2010, officers, and management of CDNS are prohibited from disclosing, directly or indirectly, to any person that the STR has been reported. Violation is a criminal offence and shall be punishable by a maximum term of five years imprisonment or a fine which may extend to two million rupees or both (http://www.fmu.gov.pk/docs/Anti-Money-Laundering-Act-2010-amended-upto-Sep.%202020.pdf)

Note: The above red flags are in addition to the red flags published by FMU or international stakeholders i.e. FATF / APGML/ Egmont Group, on their websites from time to time.

Financial Monitoring Unit	www.fmu.gov.pk
Financial Action Task Force	www.fatf-gafi.org
Asia-Pacific Group	www.apgml.org
Egmont Group	www.egmontgroup.org

Disclaimer:

These red flags are developed for guidance purpose and may appear suspicious on their own; however, it may be considered that a single red flag would not be a clear indicator of potential ML / TF activity. However, a combination of these red flags, in addition to analysis of overall financial activity and client profile may indicate a potential ML / TF activity. While every effort has been made to ensure the accuracy and check all relevant references/ resources, errors and omissions are possible and are expected. Financial Monitoring Unit (FMU), its officers and its stakeholders are not responsible for any mistakes and/or misinterpretation.