

All Pakistan Gems Merchants and Jewelers Association
AML & CFT Guidelines, 2018

Definitions

- (a) “**AML Act**” means the Anti-money Laundering Act, 2010 ;
- (b) “**Beneficial owner**” means the natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercise ultimate effective control over a person;
- (c) “**Business**” means any shop, branch, display center, etc. of member business engaged in sale / purchase, trading, import / export, investment and any other activity related to all kind of jewelry, precious metals and gems.
- (d) “**CTR**” means a report on transaction in cash exceeding such amount as may be notified pursuant to the AML Act;
- (e) “**Customer**” means a any person / entity conducts sale/purchase, import/export, investment with your business
- (f) “**FMU**” means the Financial Monitoring Unit of Pakistan established under section 6 of the AML Act;
- (g) “**person**” includes an individual, association, authority, company, firm, institutions, partnership, society, trust or other entities;
- (h) “**politically exposed persons**” or “**PEPs**” means any person entrusted with a prominent public function by the State of Pakistan, a foreign country or an international organization and includes Heads of state or government, and members and senior officials of legislature, judiciary, executive, military and regulatory authorities, and senior executives of corporations, departments or bodies that are owned or controlled by the state;
- (i) “**STR**” means a report on suspicious transactions of one or more kinds specified under section 7 of the AML Act; and
- (j) “**UNSCR**” means the United Nations Security Council Resolution.

AML/CFT Measures

1. The Business, including all its owners and employees, shall,-
 - (a) comply with the provisions of the AML Act and the rules and regulations issued thereunder for reporting STRs and CTRs in the context of money laundering or financing of terrorism;
 - (b) implement appropriate internal policies, procedures and controls for meeting the obligations specified by the AML Act and the rules and regulations issued thereunder; and
 - (c) make use of technology and upgrade their systems and procedures in accordance with the nature of risks of money laundering and financing of terrorism and shall establish criteria for management of alerts for such risks.
2. An STR shall be generated based upon suspicion and regardless of the amount of transactions under consideration.
3. A CTR shall be generated for a transaction in cash of Two Million rupees (PKR 2,000,000) or above any other threshold notified pursuant to the AML Act and regardless of any suspicion.
4. The basis of decision to file an STR or CTR with FMU shall be documented and kept on record together with all internal findings in relation to the suspicion.
5. The owner and employee of the Business shall,-
 - (a) scrutinize any transactions that are not consistent with the history or profile of the customer.
 - (b) pay special attention to unusually large transactions and unusual patterns of transactions and examine the background of such transactions, as far as possible, and record the findings for any further inspection and investigation;
 - (c) not disclose to any person the fact of filing of an STR or CTR with FMU, except where so required by law.
6. Some of the red flags related for formation of suspicion to generate STR are provided in FATF report on Money laundering / terrorist financing risks and vulnerabilities associated with gold. The link of the report containing red flags is provided at the end of these Guidelines.

Customer Due Diligence (CDD) / Know Your Customer (KYC)

7. Every customer shall be identified for establishing business relationship and, for the purpose, following information shall be obtained, verified and recorded:
 - (a) Full name as per identity document;
 - (b) CNIC/Passport/NICOP/POC/ARC number;
 - (c) Registration/incorporation number of business;
 - (d) Residential address, telephone numbers and e-mail;
 - (e) Business address, telephone numbers and e-mail;
 - (f) Date of birth;
 - (g) Date of registration/incorporation of business;
 - (h) Nationality or place of birth;
 - (i) Place of registration/incorporation of business;
 - (j) Nature of business, locations involved and type of counter-parties;
 - (k) Sources of earnings.
8. The Business shall verify identity documents of the customers from relevant authorities and bodies, including through NADRA's Verisys system, and, where necessary, use other reliable, independent sources and retain copies of all reference documents used for identification and verification. The Business may call for the original identification documents from the customer for this purpose and stamp the copy of document(s).
9. The Business shall be responsible for verification of the identity documents and the customer shall neither be obligated nor the cost of verification be charged to the customer.
10. Where the customer is represented by an authorized agent or representative or agent, or where customer is a legal person, the Business shall identify the natural persons who act on behalf of the customer and verify the identity of such persons and the authority of such natural persons shall be verified through documentary evidence, including specimen signature of the persons so authorized.
11. Where beneficial owners of a customer are involved, all reasonable measures shall be taken to obtain information to identify and verify the identity of the beneficial owners.
12. The verification of the identity of customers and any beneficial owners shall be completed before business relations are established.

13. In exceptional cases, business relationships may be established without prior verification, if the deferral of verification of the identity of the customer and any beneficial owners is required in order not to interrupt the normal conduct of business operations and the risks can be effectively managed.
14. In relation to legal persons,-
 - (a) all reasonable measures shall be taken to identify and verify (i) the ownership and control structure of the customer and (ii) the natural persons who ultimately own or control the customer; and
 - (b) the information about the purpose and intended nature of their business relations shall be obtained.
15. The Business shall periodically review the adequacy of information obtained in respect of customers and any beneficial owners and ensure that the information is kept up to date, particularly, for high-risk categories of customers.
16. The Business shall establish criteria for identifying and assessing risks that may arise in relation to new products, services, business practices and delivery mechanisms, including the review of existing products and services on an on-going basis.
17. In the case of joint customers, the CDD/KYC measures specified in this Chapter shall be performed on all the joint Customers as if each of them was an individual customer.
18. The Business shall perform the CDD/KYC measures in relation to its existing customers as may be appropriate having regard to assessment of materiality and risk and without compromise on identity and verification requirements.
19. The Business shall not provide any services / products to the individuals and entities proscribed under the Anti-terrorism Act, 1997 (XXVII of 1997), or designated under UNSCR 1267, UNSCR 1373 or other instrument of the United Nations, and to those persons who are associated with such individuals and entities, whether under the proscribed or designated name, or with a different name.
20. The Business shall monitor their relationships on a continuous basis and ensure that no relationship with the proscribed or designated, individuals and entities exists and where, any such relationship is found, the same should be immediately reported to FMU and other actions shall be taken as per the applicable law.

21. In relation to politically exposed persons (PEPs) and their close associates or family members, the Business shall:

- (a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP;
- (b) obtain approval from the senior management to establish or continue business relations where the customer or a beneficial owner is a PEP or subsequently becomes a PEP;
- (c) establish, by appropriate means, the sources of wealth or beneficial ownership of funds; and
- (d) conduct enhanced monitoring of business relations with the customer.

22. In relation to non-governmental organizations (NGOs), non-profit organizations (NPOs) and charities, the Business shall:

- (a) conduct enhanced due diligence of the customer;
- (b) obtain senior management's approval while establishing business relationship;
- (c) ensure that the business relationship may not be used for unlawful objects;
- (d) issue the instruments in the name of the relevant NGO, NPO or charity, as given in its constituent documents;
- (e) subject to the authorized agents or representatives of the customers to comprehensive CDD/KYC; and
- (f) ensure that the authorized agents or representatives may not be affiliated with any proscribed individual or entity, whether under the same name or a different name.

23. The Business shall not provide any service or product on basis of forged documents or in fictitious name.

Record Keeping

24. The Business shall maintain all necessary records on transactions, both domestic and overseas, including the results of any scrutiny or analysis for a minimum period of five years from completion of the transaction.
25. The records shall be sufficient to permit reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any customer involved in the transactions so as to provide, when necessary, evidence for action at law.
26. The records may be maintained in paper or electronic form or on microfilm.
27. The records of identification data obtained through CDD/KYC process, including copies of identification documents, application forms, KYC forms, verification documents and other documents along with business correspondence, shall be maintained for a minimum period of five years after the business relationship is ended.
28. The Business shall retain such records for longer periods of time where transactions, customers or instruments are involved in litigation or the same are required by a Court of law or other competent authority.
29. The Business shall satisfy, on timely basis, any enquiry or order from the relevant authorities, including law enforcement agencies and FMU, for supply of information and records as per law.

Internal Controls, Compliance and Audit

30. The Business shall formulate detailed procedures and controls in the light of AML/CFT policy approved by the Board / Owners of the Business.
31. The policies, procedures and controls shall include, amongst other things, CDD/KYC measures, record retention, detection of suspicious transactions and obligation to file STRs and CTRs with FMU.
32. In formulating policies, procedures and controls, the Business shall consider the threats of money laundering and financing of terrorism that may arise from the use of new or developing technologies, especially those having features of anonymity or inconsistency with the spirit of CDD/KYC measures.
33. The AML/CFT measures provided in these guidelines shall be applicable to the Business outside Pakistan to the extent that laws and regulations of the host country permit and, where the AML/CFT requirements in the host country differ

from those in Pakistan, the Business shall apply the higher of the two standards to the extent that the law of the host country so permits.

34. The Business shall invariably ensure compliance of all the relevant laws, rules and regulations pertaining to AML/CFT and devise appropriate mechanism including but not limited to the appointment of fit and proper personnel for this purpose.
35. The Business shall maintain an independent audit function that is adequately resourced and able to regularly assess the effectiveness of internal policies, procedures and controls, and its compliance with regulatory requirements.

Training

36. The Business shall develop and implement training programs for the officers and employees concerned with AML/CFT measures, on regular basis, in order to effectively implement such measures.
37. The trainings of officers and employees shall enable them to understand new developments, techniques method and trends concerning money laundering and financing of terrorism.
38. The training should include the responsibilities relating to AML/CFT measures, especially requirements relating to CDD/KYC and analysis of unusual transactions and alerts generated thereof for possible reporting of STRs and CTRs.
39. The Business may acquire or develop comprehensive AML/CFT training programs, including the online training programs and tests, under a comprehensive plan with clear timelines for its implementation.

Following are some important links for information and necessary action of the members:

FMU:

<http://www.fmu.gov.pk/index.html>

CTR Form:

[http://www.fmu.gov.pk/docs/Currency Transaction Report Form.pdf](http://www.fmu.gov.pk/docs/Currency_Transaction_Report_Form.pdf)

STR Form:

[http://www.fmu.gov.pk/docs/Suspicious Transaction Report Form.pdf](http://www.fmu.gov.pk/docs/Suspicious_Transaction_Report_Form.pdf)

Red Flag Indicators:

As mentioned in FATF report on Money laundering / terrorist financing risks and vulnerabilities associated with gold:

<http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-risks-vulnerabilities-associated-with-gold.pdf>

FATF (Financial Action Task Force):

<http://www.fatf-gafi.org/>

Asia / Pacific Group on Money Laundering:

<http://www.apgml.org/>

UNSC 1373 Proscribed individuals/entities Lists:

NACTA – National Counter Terrorism Authority, Pakistan

<https://nacta.gov.pk/>

Consolidated UNSC 1267 SROs

<http://www.mofa.gov.pk/contentsro1.php>