CONSOLIDATED FATF STANDARDS ON INFORMATION SHARING

Relevant excerpts from

the FATF Recommendations

and Interpretive Notes

June 2016

FINANCIAL ACTION TASK FORCE

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 recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website: www.fatf-gafi.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and bounderies and to the name of any territory, city or area.

Contents

ACRONYMS

AML	Anti-money laundering
CDD	Customer due diligence
CFT	Counter-terrorist financing
DNFBP	Designated non-financial business and profession
FIU	Financial intelligence unit
INR.	Interpretive Note to Recommendation
MVTS	Money value transfer services
NPO	Non-profit organisations
R.	Recommendation
STR	Suspicious transaction report
SRB	Self-regulatory body
UNSCR	United Nations Security Council Resolution

Effective information sharing is one of the cornerstones of a well-functioning anti-money laundering/counter-terrorist financing (AML/CFT) framework. This is a consolidation of the existing FATF Standards on information sharing. The FATF is publishing them in this form in response to feedback from the private sector that this would add value and clarify the requirements which are currently spread across 25 of the FATF Recommendations, and which impact 7 Immediate Outcomes in the FATF Methodology for assessing effectiveness.

This consolidation is comprised of relevant excerpts from the FATF Recommendations which set out requirements on:

a) the types of information that should be shared, including the types of information that competent authorities are required to make publicly available

b) the circumstances in which such information should be shared, and

c) the protections and safeguards which should apply to information sharing and exchange.

These excerpts have been organised into five main thematic categories:

1) General provisions

2) Transparency of basic and beneficial ownership information

3) Information sharing within the private sector

4) Information sharing between the public and private sectors, and

5) Information sharing among public authorities.

6) Assessing effective implementation of the FATF standards on information sharing, which sets out the relevant excerpts from the *Methodology,* and demonstrates how the FATF assesses whether these requirements are being implemented effectively.

Going forward, the FATF will continue its work to develop best practices aimed at facilitating information sharing between the public and private sectors, and within the private sector, and its work on issues related to information sharing among public authorities—both domestically and internationally.

THE CONSOLIDATED FATF STANDARDS ON INFORMATION SHARING

RELEVANT EXCERPTS FROM THE FATF RECOMMENDATIONS AND INTERPRETIVE NOTES

1) GENERAL PROVISIONS

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations. R.9

2) TRANSPARENCY OF BASIC & BENEFICIAL OWNERSHIP INFORMATION

Transparency and beneficial ownership of legal persons

Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities [...] Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22. R.24

Competent authorities should be able to obtain, or have access in a timely fashion to, adequate, accurate and current information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information[1]) that are created[2] in the country. Countries may choose the mechanisms they rely on to achieve this objective, although they should also comply with the minimum requirements set out below. It is also very likely that countries will need to utilise a combination of mechanisms to achieve the objective. As part of the process of ensuring that there is adequate transparency regarding legal persons, countries should have mechanisms that: (a) identify and describe the different types, forms and basic features of legal persons in the country; (b) identify and describe the processes for: (i) the creation of those legal persons; and (ii) the obtaining and recording of basic and beneficial ownership information; (c) make the above information publicly available; INR.24, para.1, 2(a),

[1] Beneficial ownership information for legal persons is the information referred to in the interpretive note to Recommendation 10, paragraph 5(b)(i). Controlling shareholders as referred to in, paragraph 5(b)(i) of the interpretive note to Recommendation 10 may be based on a threshold, e.g. any persons owning more than a certain percentage of the company (e.g. 25%).

[2] References to creating a legal person, include incorporation of companies or any other mechanism that is used.

(b) and (c)

All companies created in a country should be registered in a company registry.[3] Whichever combination of mechanisms is used to obtain and record beneficial ownership information […], there is a set of basic information on a company that needs to be obtained and recorded by the company[4] as a necessary prerequisite. The minimum basic information to be obtained and recorded by a company should be: (a) company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g. memorandum & articles of association), a list of directors; and (b) a register of its shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder[5] and categories of shares (including the nature of the associated voting rights). The company registry should record all the basic information set out […] above. The company should maintain the basic information set out in […] (b) within the country, either at its registered office or at another location notified to the company registry. However, if the company or company registry holds beneficial ownership information within the country, then the register of shareholders need not be in the country, provided that the company can provide this information promptly on request. Countries should require their company registry to facilitate timely access by financial institutions, DNFBPs and other countries' competent authorities to the public information they hold, and, at a minimum to the information referred to in [..] (a) above. Countries should also consider facilitating timely access by financial institutions and DNFBPs to information referred to in […] (b) above. INR.24, para.4-6, and 13

Countries should ensure that either: (a) information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or (b) there are mechanisms in place so that the beneficial ownership of a company can be determined in a timely manner by a competent authority. INR.24, para.7

In order to meet the requirements [...] countries should use one or more of the following mechanisms: (a) Requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership; (b) Requiring companies to take reasonable measures[6] to obtain and hold up-to-date information on the companies' beneficial ownership; (c) Using existing information, including: (i) information obtained by financial institutions and/or DNFBPs, in accordance with

[3] "Company registry" refers to a register in the country of companies incorporated or licensed in that country and normally maintained by or for the incorporating authority. It does not refer to information held by or for the company itself.

[4] The information can be recorded by the company itself or by a third person under the company's responsibility.

[5] This is applicable to the nominal owner of all registered shares.

[6] Measures taken should be proportionate to the level of risk or complexity induced by the ownership structure of the company or the nature of the controlling shareholders.

Recommendations 10 and 22[7]; (ii) information held by other competent authorities on the legal and beneficial ownership of companies (e.g. company registries, tax authorities or financial or other regulators); (iii) information held by the company as required above in Section A; and (iv) available information on companies listed on a stock exchange, where disclosure requirements (either by stock exchange rules or through law or enforceable means) impose requirements to ensure adequate transparency of beneficial ownership. INR.24, para.8

Regardless of which of the above mechanisms are used, countries should ensure that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner. This should include: (a) Requiring that one or more natural persons resident in the country is authorised by the company[8], and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or (b) Requiring that a DNFBP in the country is authorised by the company, and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or (c) Other comparable measures, specifically identified by the country, which can effectively ensure cooperation [...] INR.24, para.9 (a), (b) and (c)

Countries should have mechanisms that ensure that basic information, including information provided to the company registry, is accurate and updated on a timely basis. Countries should require that any available information referred to in paragraph 7 is accurate and is kept as current and up-to-date as possible, and the information should be updated within a reasonable period following any change. INR.24, para.11

Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to the basic and beneficial ownership information held by the relevant parties. INR.24, para.12

Countries should take measures to prevent the misuse of bearer shares and bearer share warrants, for example by applying one or more of the following mechanisms [...] (d) requiring shareholders with a controlling interest to notify the company, and the company to record their identity. INR.24, para.14

Countries should take measures to prevent the misuse of nominee shares and nominee directors, for example by applying one or more of the following mechanisms: (a) requiring nominee shareholders and directors to disclose the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register; or (b) requiring nominee

[7] Countries should be able to determine in a timely manner whether a company has an account with a financial institution within the country.

[8] Members of the company's board or senior management may not require specific authorisation by the company.

shareholders and directors to be licensed, for their nominee status to be recorded in company registries, and for them to maintain information identifying their nominator, and make this information available to the competent authorities upon request. INR.24, para.15

In relation to foundations, Anstalt, and limited liability partnerships, countries should take similar measures and impose similar requirements, as those required for companies, taking into account their different forms and structures [...] At a minimum, countries should ensure that similar types of basic information should be recorded and kept accurate and current by such legal persons, and that such information is accessible in a timely way by competent authorities. Countries should review the money laundering and terrorist financing risks associated with such other legal persons, and, based on the level of risk, determine the measures that should be taken to ensure that competent authorities have timely access to adequate, accurate and current beneficial ownership information for such legal persons. INR.24, para.16 and 17

Countries should rapidly, constructively and effectively provide international cooperation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to basic information held by company registries; (b) exchanging information on shareholders; and (c) using their powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts. Countries should monitor the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad. INR.24, para.19

Transparency and beneficial ownership of legal arrangements

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22. R.25

Countries should require trustees of any express trust governed under their law to obtain and hold adequate, accurate, and current beneficial ownership information regarding the trust. This should include information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust.

Countries should also require trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors. INR.25, para.1

All countries should take measures to ensure that trustees disclose their status to financial institutions and DNFBPs when, as a trustee, forming a business relationship or carrying out an occasional transaction above the threshold. Trustees should not be prevented by law or enforceable means from providing competent authorities with any information relating to the trust[9]; or from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship. INR.25, para.2

Countries are encouraged to ensure that other relevant authorities, persons and entities hold information on all trusts with which they have a relationship. Potential sources of information on trusts, trustees, and trust assets are: (a) Registries (e.g. a central registry of trusts or trust assets), or asset registries for land, property, vehicles, shares or other assets. (b) Other competent authorities that hold information on trusts and trustees (e.g. tax authorities which collect information on assets and income relating to trusts). (c) Other agents and service providers to the trust, including investment advisors or managers, lawyers, or trust and company service providers. INR.25, para.3

Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to obtain timely access to the information held by trustees and other parties, in particular information held by financial institutions and DNFBPs on: (a) the beneficial ownership; (b) the residence of the trustee; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction. INR.25, para.4

As regards other types of legal arrangement with a similar structure or function, countries should take similar measures to those required for trusts, with a view to achieving similar levels of transparency. At a minimum, countries should ensure that information similar to that specified above in respect of trusts should be recorded and kept accurate and current, and that such information is accessible in a timely way by competent authorities. INR.25, para.9

Countries should rapidly, constructively and effectively provide international cooperation in relation to information, including beneficial ownership information, on trusts and other legal arrangements on the basis set out in Recommendations 37

[9] Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

and 40. This should include (a) facilitating access by foreign competent authorities to any information held by registries or other domestic authorities; (b) exchanging domestically available information on the trusts or other legal arrangement; and (c) using their competent authorities' powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts. INR.25, para.10

3) INFORMATION SHARING WITHIN THE PRIVATE SECTOR

In the context of correspondent banking

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to: […] (e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank. R.13, para.(e)

In the context of processing wire transfers:

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain. R.16

Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply: (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer. (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information. INR.16, para.5

Information accompanying all qualifying wire transfers should always contain: (a) the name of the originator; (b) the originator account number where such an account is used to process the transaction; (c) the originator's address, or national identity number, or customer identification number[10], or date and place of birth;

[10] The customer identification number refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number referred to in paragraph 7. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: the customer address, a national identity number, or a date and place of birth.

(d) the name of the beneficiary; and (e) the beneficiary account number where such an account is used to process the transaction. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements[...]in respect of originator information, provided that they include the originator's account number or unique transaction reference number (as described [...] above), and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country. INR.16, para.6, 7 and 8

Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. INR.16, para.9

The ordering financial institution should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information. The ordering financial institution should ensure that cross-border wire transfers below any applicable threshold contain the name of the originator and the name of the beneficiary and an account number for each, or a unique transaction reference number [...] The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above. INR.16, para.11, 12 and 14

For cross-border wire transfers, financial institutions processing an intermediary element of such chains of wire transfers should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution. INR.16, para.15 and 16

An intermediary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing. An intermediary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action. INR.16, para.17 and 18

A beneficiary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible [...] A beneficiary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action. INR.16, para. 19 and 21

Money or value transfer service (MVTS) providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. INR.16, para.22

In the context of relying on third parties[11]:

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party. R.17

The criteria that should be met are as follows: (a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10. (b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay. (c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11. (d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk. R.17

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide

[11] These same requirements apply to DNFBP pursuant to R.22.

that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies. R.17

In the context of implementing group-wide AML/CFT programmes[12]:

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes [...] R.18

Financial groups' programmes against money laundering and terrorist financing should be applicable to all branches and majority-owned subsidiaries of the financial group [...] These programmes should include policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management [...] Adequate safeguards on the confidentiality and use of information exchanged should be in place. INR.18, para.4

In the context of protecting NPOs from terrorist abuse:

Effective information gathering and investigation: [...] (i) Countries should ensure effective cooperation, coordination and information-sharing to the extent possible among all [...] organisations that hold relevant information on NPOs. INR.8, para.6(c)(i)

4) INFORMATION SHARING BETWEEN THE PUBLIC & PRIVATE SECTORS

In the context of risk information:

Countries[13] should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: [...] (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant [...] self-regulatory bodies (SRBs), financial institutions and DNFBPs. INR.1, para.3

Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks and [...] either prescribe that financial

[12] These same requirements apply to DNFBP pursuant to R.23.

[13] Where appropriate, AML/CFT risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk assessments carried out by financial institutions and DNFBPs, in order to manage and mitigate risks appropriately. INR.1, para.4

Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks [...] and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs [...] INR.1, para.8

In the context of implementing targeted financial sanctions:

The competent authority(ies) should have appropriate legal authorities and procedures or mechanisms to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions. INR.6, para.4(c)

Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms. INR.6, para.6(c), and INR.7, para.6(c)

Countries should require financial institutions and DNFBPs[14] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by the competent authorities. INR.6, para.6(d), and INR.7, para.6(d)

Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of persons and entities designated pursuant to resolution 1267(1999) and its successor resolutions [or resolutions 1718(2006) and 1737(2006) and their successor resolutions] that, in the view of the country, do not or no longer meet the criteria for designation [...] INR.7, para.7

For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity. INR.6, para.9, and

[14] Security Council resolutions apply to all natural and legal persons within the country.

INR.7, para.8

With respect to designations on the Al-Qaida Sanctions List, countries should inform designated persons and entities of the availability of the United Nations Office of the Ombudsperson, pursuant to resolution 1904 (2009), to accept de-listing petitions. INR.6, para.11

Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action. INR.6, para.12, and INR.7, para.12

In the context of protecting NPOs from terrorist abuse

Without prejudice to the requirements of Recommendation 1, since not all NPOs are inherently high risk (and some may represent little or no risk at all), countries should identify which subset of organisations fall within the FATF definition of NPO. In undertaking this exercise, countries should use all relevant sources of information in order to identify features and types of NPOs, which, by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse.[15] INR.8, para.5

Countries should encourage and undertake outreach and educational programmes to raise and deepen awareness among NPOs as well as the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse. INR.8, para.6(a)(ii)

Effective information gathering and investigation: (i) Countries should ensure effective cooperation, coordination and information-sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs. (iii) Countries should ensure that full access to information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation. (iv) Countries should establish appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, this information is promptly shared with relevant competent authorities, in order to take preventive or investigative action. INR.8, para.5(c)(i),(iii)

[15] For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

and (iv)

In the context of conducting customer due diligence[16]

If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should: [...] (b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU), in accordance with Recommendation 20. INR.10, para.1(b)

If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR [...] INR.10, para.3

In the context of records which financial institutions must make available to the competent authorities upon appropriate request[17]*:*

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity [...] The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority. R.11

In the context of providing money or value transfer services

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate [...] R.14

In the context of processing wire transfers:

Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the [...] appropriate authorities by other means [...] The information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial

[16] These same requirements apply to DNFBP pursuant to R.22.

[17] These same requirements apply to DNFBP pursuant to R.22.

institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information. INR.16, para.9 and 10

In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider: (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and (b) should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit. INR.16, para.22

In the context of implementing group-wide AML/CFT programmes[18]:

If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform their home supervisors. INR.18, para.5

In the context of dealing with higher risk countries[19]:

Examples of the countermeasures that could be undertaken by countries include the following, and any other measures that have a similar effect in mitigating risks: [...] (b) Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions [...] There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries. ` INR.19, para.2(b)

In the context of reporting suspicious transactions[20]:

If a 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 (FIU). R.20

All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction. The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise (so called "indirect reporting"), is not acceptable. INR.20, para.3 and 4

[18] These same requirements apply to DNFBP pursuant to R.23.

[19] These same requirements apply to DNFBP pursuant to R.23.

[20] These same requirements apply to DNFBP pursuant to R.23.

Financial institutions, their directors, officers and employees should be: (a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and (b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. R.21

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. INR.23, para.1

Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of cooperation between these organisations and the FIU. INR.23, para.3

Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off. INR.23, para.4

In the context of guidance and feedback:

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions. R.34

In the context of regulation, supervision & monitoring:

[…] supervisors and SRBs should, as and when required in accordance with the Interpretive Notes to Recommendations 26 and 28, review the money laundering and terrorist financing risk profiles and risk assessments prepared by financial institutions and DNFBPs, and take the result of this review into consideration. INR.1, para.7

[…] supervisors: [...] (b) should have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the supervised institutions, including the quality of the compliance function of the financial institution or group (or groups, when applicable for Core Principles institutions) [...]. INR.26, para.2

Supervisors should [...] be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, R.27

Supervisors or SRBs should [...] have in place processes to ensure that the staff of those authorities maintain high professional standards, including standards concerning confidentiality. INR.28, para.4

Countries should ensure that financial supervisors [...] have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality. INR.26, para.6

In the context of analysing suspicious transactions:

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial [...] information that it requires to undertake its functions properly. R.29

The FIU serves as the central agency for the receipt of disclosures filed by reporting entities. At a minimum, this information should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures). INR.29, para.2

In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly. The information that the FIU should be permitted to obtain could include information that reporting entities are required to maintain pursuant to the relevant FATF Recommendations (Recommendations 10, 11 and 22). INR.29, para.5

In order to conduct proper analysis, the FIU should have access to the widest possible range of financial information. This should include information from open or public sources, as well as [...] where appropriate, commercially held data. INR.29, para.6

Information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations. An FIU must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, dissemination, and protection of, as well as access to such information. The FIU should ensure that its staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. The FIU should ensure that

there is limited access to its facilities and information, including information technology systems. The FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely, including the autonomous decision to request specific information. […] The FIU should have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality. INR.29, para.7, 8 and 10

In the context of conducting investigations:

Law enforcement authorities and prosecutorial authorities [...] should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality. INR.30, para.8

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence. Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU. R.31

Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs and their intended use. INR.32, para.5(b)

In the context of providing mutual legal assistance:

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

(a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and

(b) a broad range of other powers and investigative techniques; are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts. R.37

5) INFORMATION SHARING AMONG PUBLIC AUTHORITIES

In the context of risk information:

Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities […] INR.1, para.3

In the context of national cooperation and coordination:

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy-making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. R.2

In the context of implementing targeted financial sanctions:

When requesting another country to give effect to the actions initiated under the freezing mechanisms that have been implemented pursuant to resolution 1373 (2001), the initiating country should provide as much detail as possible on: the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions). INR.6, para.4(g)

In the context of protecting NPOs from terrorist abuse

Effective information gathering and investigation: (i) Countries should ensure effective cooperation, coordination and information-sharing to the extent possible among all levels of appropriate authorities [...] that hold relevant information on NPOs. [...] Countries should ensure that full access to information on the

administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation. Countries should establish appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is involved in terrorist financing abuse and/or is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures, or other forms of terrorist support; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, that this information is promptly shared with relevant competent authorities, in order to take preventive or investigative action.

INR.8, para.6(c)(i), (iii) and (iv)

Effective capacity to respond to international requests for information about an NPO of concern: Consistent with Recommendations on international cooperation, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support. INR.8, para.6(d)

In the context of analysing suspicious transactions:

The FIU [...] should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly. R.29

The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities. Dedicated, secure and protected channels should be used for the dissemination:

- **Spontaneous dissemination**: The FIU should be able to disseminate information and the results of its analysis to competent authorities when there are grounds to suspect money laundering, predicate offences or terrorist financing. Based on the FIU's analysis, the dissemination of information should be selective and allow the recipient authorities to focus on relevant cases/information.
- **Dissemination upon request:** The FIU should be able to respond to information requests from competent authorities pursuant to Recommendation 31. When the FIU receives such a request from a competent authority, the decision on conducting analysis and/or dissemination of information to the requesting authority should remain with the FIU. INR.29, para.4

In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. This

should include [...] relevant information collected and/or maintained by, or on behalf of, other authorities [...] INR.29, para.6

Information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations. An FIU must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, dissemination, and protection of, as well as access to such information. The FIU should ensure that its staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. The FIU should ensure that there is limited access to its facilities and information, including information technology systems. INR.29, para.7

The FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely, including the autonomous decision to analyse [...] and/or disseminate specific information. In all cases, this means that the FIU has the independent right to forward or disseminate information to competent authorities. INR.29, para.8

Countries should have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality [...] INR.29, para.10

The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information. INR.29, para.11

Countries should ensure that the FIU has regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIUs) [...] INR.29, para.13

In the context of conducting investigations:

Law enforcement authorities and prosecutorial authorities [...] should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality. INR.30, para.8

Information obtained through the declaration/disclosure process should be available to the FIU, either through a system whereby the FIU is notified about suspicious cross-border transportation incidents, or by making the declaration/disclosure information directly available to the FIU in some other way. INR.32, para.5(c)

The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with Recommendations 36 to 40. To facilitate such cooperation, in instances when: (i) a declaration or disclosure which exceeds the maximum threshold of USD/EUR 15,000 is made; or (ii) where there is a false declaration or false disclosure; or (iii) where there is a suspicion of money laundering or terrorist financing, this information shall be retained for use by competent authorities. At a minimum, this information will cover: (i) the amount of currency or BNIs declared, disclosed or otherwise detected; and (ii) the identification data of the bearer(s). INR.32, para.5(f)

Countries should implement Recommendation 32 subject to strict safeguards to ensure proper use of information. INR.32, para.5(g)

Authorities responsible for implementation of Recommendation 32 [...] should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality. INR.32, para.7

If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward the taking of appropriate action. INR.32, para.8

In the context of mutual legal assistance:

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should: (a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance. (b) [...] Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests [...] (c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters. (d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality. (e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country [...] R.37

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means [...] R.37

The authorities responsible for mutual legal assistance (e.g. a Central Authority) [...] should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality. R.37

In the context of extradition:

Each country should either extradite its own nationals, or, where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case, without undue delay, to its competent authorities for the purpose of prosecution of the offences set forth in the request [...] The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions [...] The authorities responsible for extradition [...] should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality. R.39

In the context of other forms of international cooperation:

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation. Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts. Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received. R.40

Principles applicable to all forms of international cooperation

When making requests for cooperation, competent authorities should make their best efforts to provide complete factual and, as appropriate, legal information, including indicating any need for urgency, to enable a timely and efficient execution of the request, as well as the foreseen use of the information requested. Upon

request, requesting competent authorities should provide feedback to the requested competent authority on the use and usefulness of the information obtained. INR.40, para.1

Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that: (a) the request is also considered to involve fiscal matters; and/or (b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart. INR.40, para.2

Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes, beyond those originally approved, should be subject to prior authorisation by the requested competent authority. INR.40, para.3

Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry[21], consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in the manner authorised. Exchange of information should take place in a secure way, and through reliable channels or mechanisms. Requested competent authorities may, as appropriate, refuse to provide information if the requesting competent authority cannot protect the information effectively. INR.40, para.4

Competent authorities should be able to conduct inquiries on behalf of a foreign counterpart, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically. INR.40, para.5

The general principles above should apply to all forms of exchange of information between counterparts or non-counterparts, subject to the paragraphs set out below. INR.40, para.6

[21] Information may be disclosed if such disclosure is required to carry out the request for cooperation.

Exchange of information between FIUs

FIUs should exchange information with foreign FIUs, regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing. INR.40, para.7

When making a request for cooperation, FIUs should make their best efforts to provide complete factual, and, as appropriate, legal information, including the description of the case being analysed and the potential link to the requested country. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided. INR.40, para.8

FIUs should have the power to exchange: (a) all information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, in particular under Recommendation 29; and (b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity. INR.40, para.9

Exchange of information between financial supervisors[22]

Financial supervisors should cooperate with their foreign counterparts, regardless of their respective nature or status. Efficient cooperation between financial supervisors aims at facilitating effective AML/CFT supervision of financial institutions. To this end, financial supervisors should have an adequate legal basis for providing cooperation, consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes. INR.40, para.10

Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, and in a manner proportionate to their respective needs. Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other relevant supervisors that have a shared responsibility for financial institutions operating in the same group: (a) Regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors. (b) Prudential information, in particular for Core Principle Supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness. (c) AML/CFT information, such as internal AML/CFT procedures and

[22] This refers to financial supervisors which are competent authorities.

policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information. INR.40, para.11

Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision. INR.40, para.12

Any dissemination of information exchanged or use of that information for supervisory and non- supervisory purposes, should be subject to prior authorisation by the requested financial supervisor, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation. The prior authorisation includes any deemed prior authorisation under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding issued by a core principles standard-setter applied to information exchanged under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding. INR.40, para.13

Exchange of information between law enforcement authorities

Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime. INR.40, para.14

Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement cooperation, such as the agreements between Interpol, Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority. INR.40, para.15

Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, countries should establish bilateral or multilateral arrangements to enable such joint investigations. Countries are encouraged to join and support existing AML/CFT law enforcement networks, and develop bi-lateral contacts with foreign law enforcement agencies, including placing liaison officers abroad, in order to facilitate timely and effective cooperation. INR.40, para.16

Exchange of information between non-counterparts

Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. Indirect

exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made. INR.40, para.17

Countries are also encouraged to permit a prompt and constructive exchange of information directly with non-counterparts. INR.40, para.18

6) ASSESSING EFFECTIVE IMPLEMENTATION OF THE FATF STANDARDS ON INFORMATION SHARING (EXCERPTS FROM THE METHODOLOGY)

IMMEDIATE OUTCOME 1 – RISK, POLICY AND COORDINATION

1. To what extent do the competent authorities and SRBs co-operate and co-ordinate the development and implementation of policies and activities to combat ML/TF and, where appropriate, the financing of proliferation of weapons of mass destruction?

2. To what extent does the country ensure that respective financial institutions, DNFBPs and other sectors affected by the application of the FATF Standards are aware of the relevant results of the national ML/TF risk assessment(s)?

IMMEDIATE OUTCOME 2 – INTERNATIONAL COOPERATION

3. To what extent has the country provided constructive and timely mutual legal assistance and extradition across the range of international co-operation requests? What is the quality of such assistance provided?

4. To what extent has the country sought legal assistance for international co-operation in an appropriate and timely manner to pursue domestic ML, associated predicate offences and TF cases which have transnational elements?

5. To what extent do the different competent authorities seek other forms of international co-operation to exchange financial intelligence and supervisory, law enforcement or other information in an appropriate and timely manner with their foreign counterparts for AML/CFT purposes?

6. To what extent do the different competent authorities provide (including spontaneously) other forms of international co-operation to exchange financial intelligence and supervisory, law enforcement or other information in a constructive and timely manner with their foreign counterparts for AML/CFT purposes?

7. How well are the competent authorities providing and responding to foreign requests for co-operation in identifying and exchanging basic and beneficial ownership information of legal persons and arrangements?

IMMEDIATE OUTCOME 3 – SUPERVISION

8. How well do the supervisors promote a clear understanding by financial institutions and DNFBPs of their AML/CFT obligations and ML/TF risks?

IMMEDIATE OUTCOME 4 – PREVENTIVE MEASURES

9. To what extent do financial institutions and DNFBPs meet their reporting obligations on the suspected proceeds of crime and funds in support of terrorism? What are the practical measures to prevent tipping-off?

10. How well do financial institutions and DNFBPs apply internal controls and procedures (including at financial group level) to ensure compliance with AML/CFT requirements? To what extent are there legal or regulatory requirements (e.g., financial secrecy) impeding its implementation?

IMMEDIATE OUTCOME 5 – LEGAL PERSONS AND ARRANGEMENTS

11. To what extent is the information on the creation and types of legal persons and arrangements in the country available publicly?

12. To what extent can relevant competent authorities obtain adequate, accurate and current basic and beneficial ownership information on all types of legal persons created in the country, in a timely manner?

13. To what extent can relevant competent authorities obtain adequate, accurate and current beneficial ownership information on legal arrangements, in a timely manner?

IMMEDIATE OUTCOME 6 – FINANCIAL INTELLIGENCE

14. To what extent are financial intelligence and other relevant information accessed and used in investigations to develop evidence and trace criminal proceeds related to ML, associated predicate offences and TF?

15. To what extent are the competent authorities receiving or requesting reports (e.g., STRs, reports on currency and bearer negotiable instruments) that contain relevant and accurate information that assists them to perform their duties?

16. To what extent is FIU analysis and dissemination supporting the operational needs of competent authorities?

17. To what extent do the FIU and other competent authorities co-operate and exchange information and financial intelligence? How securely do the FIU and competent authorities protect the confidentiality of the information they exchange or use?

IMMEDIATE OUTCOME 10 – TERRORIST FINANCING PREVENTIVE MEASURES AND FINANCIAL SANCTIONS

18. How well is the country implementing targeted financial sanctions pursuant to [...] UNSCR1373 (at the supra-national or national level [...] after examination, to give effect to the request of another country)?

19. To what extent, without disrupting legitimate NPO activities, has the country [...] conducted outreach [...] in dealing with NPOs that are at risk from the threat of terrorist abuse?