



ICSA

INTERNATIONAL COUNCIL of SECURITIES ASSOCIATIONS

December 14, 2011

Giancarlo Del Bufalo
President
Financial Action Task Force
2, rue Andre Pascal
75016 Paris
France

Dear Mr. Del Bufalo:

On behalf of the members of the ICSA Working Group on AML, we would like to thank you for the invitation to participate in the meeting that was held last week in Milan and for the opportunity to comment further on the proposed revisions to the FATF Recommendations.¹ ICSA members appreciate and strongly support the open dialogue that FATF has established with private sector representatives in order to enhance AML/CFT regimes at both the international and domestic level and look forward to continuing to work closely with the FATF.

ICSA members generally support the recommendations set out in FATF's most recent consultation paper. However, ICSA members do not believe that financial institutions or DNFBPs should be charged with collecting information on beneficial ownership when that information is not publicly available, as is currently the case in most jurisdictions. Since corporate entities can be formed only with the approval of public sector bodies, only the public sector has the capacity to compel firms and other legal entities to supply the necessary information. Therefore, ICSA members urge FATF to alter its current proposal on data base registries. Rather than encouraging countries to include beneficial ownership information in public registries, we suggest that FATF require that such information is included in the registries as an obligation on firms arising from the privilege of limited legal liability. If FATF does not favour full transparency for the public registries, financial institutions and DNFBPs must have access to beneficial ownership details that are submitted by firms to the registries even when that information is not available to the general public.

ICSA members also urge FATF to clearly state that the risk-based approach applies to the FATF 40+ Recommendations in their entirety. We think that this is necessary since there is still some

¹ ICSA is composed of trade associations and self-regulatory organizations that collectively represent and/or regulate the vast majority of the world's financial services firms on both a national and international basis. ICSA's objectives are: (1) to encourage the sound growth of the international securities markets by promoting harmonization in the procedures and regulation of those markets; and (2) to promote mutual understanding and the exchange of information among ICSA members. ICSA's Working Group on AML participates in FATF's Consultative Forum as the representative of the global securities industry.

ambiguity in the proposed revised text as to whether or not the RBA applies to all of the 40+ Recommendations.

ICSA members have some suggested changes to the proposed language regarding these and other aspects of the revised Recommendations. The suggested changes are highlighted in green and are on pages 6, 8, 11, 13, 27-29, 31, 33-37, 44-49, 70 and 98 of the enclosed document.

Please do not hesitate to contact us if you would like to discuss these issues further.

Best regards,



Kung Ho Hwang, Chairman
International Council of Securities
Associations (ICSA)



Duncan Fairweather, Chairman,
ICSA Standing Committee on
Regulatory Affairs



ICSA

INTERNATIONAL COUNCIL of SECURITIES ASSOCIATIONS

December 14, 2011

Giancarlo Del Bufalo
President
Financial Action Task Force
2, rue Andre Pascal
75016 Paris
France

Dear Mr. Del Bufalo:

On behalf of the members of the ICSA Working Group on AML, we would like to thank you for the invitation to participate in the meeting that was held last week in Milan and for the opportunity to comment further on the proposed revisions to the FATF Recommendations.¹ ICSA members appreciate and strongly support the open dialogue that FATF has established with private sector representatives in order to enhance AML/CFT regimes at both the international and domestic level and look forward to continuing to work closely with the FATF.

ICSA members generally support the recommendations set out in FATF's most recent consultation paper. However, ICSA members do not believe that privately owned financial institutions or any private sector bodies should be charged with collecting information on beneficial ownership when that information is not publicly available, as is currently the case in most if not all jurisdictions. Since corporate entities can be formed only with the approval of public sector bodies, only the public sector has the capacity to compel firms and other legal entities to supply the necessary information. Therefore, ICSA members urge FATF to alter its current proposal on data base registries. Rather than encouraging countries to include beneficial ownership information in public registries, we suggest that FATF must require that such information is included in the registries as an obligation on firms arising from the privilege of limited legal liability. If FATF does not favour full transparency for the public registries, financial institutions and DNFbps must have access to beneficial ownership details that are submitted by firms to the registries even when that information is not available to the general public.

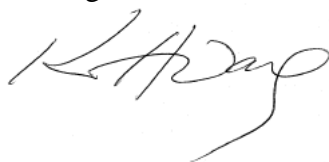
¹ ICSA is composed of trade associations and self-regulatory organizations that collectively represent and/or regulate the vast majority of the world's financial services firms on both a national and international basis. ICSA's objectives are: (1) to encourage the sound growth of the international securities markets by promoting harmonization in the procedures and regulation of those markets; and (2) to promote mutual understanding and the exchange of information among ICSA members. ICSA's Working Group on AML participates in FATF's Consultative Forum as the representative of the global securities industry.

ICSA members also urge FATF to clearly state that the risk-based approach applies to the FATF 40+ Recommendations in their entirety. We think that this is necessary since there is still some ambiguity in the proposed revised text as to whether or not the RBA applies to all of the 40+ Recommendations.

ICSA members have some suggested changes to the proposed language regarding these and other aspects of the revised Recommendations. The suggested changes are highlighted in green and are on pages 6, 8, 11, 13, 27-29, 31, 33-37, 44-49, 70 and 98 of the enclosed document.

Please do not hesitate to contact us if you would like to discuss these issues further.

Best regards,



Kung Ho Hwang, Chairman
International Council of Securities
Associations (ICSA)



Duncan Fairweather, Chairman,
ICSA Standing Committee on
Regulatory Affairs

**Financial Action Task Force
on Money Laundering**
Groupe d'action financière
sur le blanchiment de capitaux

***PROPOSED REVISION OF THE
FATF
RECOMMENDATIONS***

Document for FATF Private Sector Consultative Forum meeting,

Milan, 5–6 December 2011

Version of: 28/10/2011

Notes

This document indicates the proposed revisions (shown in redlines) to the FATF Forty Recommendations and Nine Special Recommendations.

Please note that the revisions are proposals under consideration by the FATF as at end-October 2011, and have not yet been agreed by FATF members or formally adopted at the FATF Plenary. The document is confidential, and is being made available only to members of the Consultative Forum to facilitate the discussion at the Forum's meeting in Milan on 5-6 December. It is not for public circulation.

As a part of the Review of the FATF Standards, it is also proposed that the Recommendations be reorganised, in order to make them clearer and better-integrated. This document presents the 40 Recommendations and Nine Special Recommendations in their current format, in order to clearly indicate any changes to the substance of the requirements. Therefore, in addition to the changes which are marked in this document, a number of organisational changes are expected to be made, including the integration of the Nine Special Recommendations into the body of the FATF Forty Recommendations.

The FATF will continue to work on these proposals, and expects to adopt the revised Recommendations in February 2012.

The Forty Recommendations

THE FORTY RECOMMENDATIONS

A. LEGAL SYSTEMS

Scope of the criminal offence of money laundering

1. Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.

Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offences under their national law or should include offences which are punishable by a maximum penalty of more than one year's imprisonment or for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences, which are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offences within each of the designated categories of offences¹.

Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

2. Countries should ensure that:
 - a) The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances.
 - b) Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.

¹ See the definition of "designated categories of offences" in the Glossary.

The Forty Recommendations

Provisional measures and confiscation

3. Countries should adopt measures similar to those set forth in the *United Nations Convention against Illicit Traffic in Narcotics and Psychotropic Substances (1988) (the Vienna Convention)*, the *United Nations Convention against Transnational Organised Crime (2000) (the ~~and~~ Palermo Convention)* and the *International Convention for the Suppression of the Financing of Terrorism (1999) (the Terrorist Financing Convention)*s, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of bona fide third parties: property laundered, proceeds from money laundering or predicate offences, property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations, instrumentalities used in or intended for use in the commission of any of these offences, or property of corresponding value, ~~without prejudicing the rights of bona fide third parties~~.

Such measures should include the authority to: (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or avoid actions that prejudice the State's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

B. MEASURES TO BE TAKEN BY FINANCIAL INSTITUTIONS AND NON-FINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

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

Customer due diligence ~~and record-keeping~~

5. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence (CDD) measures, ~~including identifying and verifying the identity of their customers~~, when²:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or

² RBA does not apply to the circumstances when CDD should be required, but may be used to determine the extent of such measures.

The Forty Recommendations

- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The ~~customer due diligence (CDD)~~ measures to be taken are as follows:

- a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information³.
- b) Identifying the beneficial owner, and taking reasonable measures⁴ to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions ~~taking reasonable measures to~~ understanding the ownership and control structure of the customer.
- c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
- d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should may determine the extent of such measures using a RBA in accordance with the Interpretative Note to Recommendation 5 and Interpretative Note on the Risk-Based Approach. on a risk sensitive basis depending on the type of customer, business relationship or transaction.

~~Reduced or simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.~~

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (c) above (subject to appropriate modification of the extent of the measures on a risk based approach), it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

³ Reliable, independent source documents, data or information will hereafter be referred to as "identification data".

~~* Recommendations marked with an asterisk should be read in conjunction with their Interpretative Note.~~

⁴ In determining the reasonableness of the identity verification measures, regard should be had to the identified money laundering and terrorist financing risks.

The Forty Recommendations

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

The principle that financial institutions should conduct customer due diligence should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or other enforceable means.

6. Financial institutions should, in relation to foreign politically exposed persons (whether as customer or beneficial owner), in addition to performing normal due diligence measures:
- a) Have appropriate risk management systems to determine whether the customer or the beneficial owner is a politically exposed person.
 - b) Obtain senior management approval for establishing or continuing (if it is an existing customer) such business relationships.
 - c) Take reasonable measures to establish the source of wealth and source of funds.
 - d) Conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer is a domestic politically exposed person or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs b, c and d.

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

The Interpretative Note on the Risk Based Approach shall apply to this Recommendation.

7. Financial institutions should, in relation to cross-border correspondent banking and other similar relationships⁵-in addition to performing normal due diligence measures:
- a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.
 - b) Assess the respondent institution's anti-money laundering and terrorist financing controls.
 - c) Obtain approval from senior management before establishing new correspondent relationships.
 - d) Document the respective responsibilities of each institution.
 - e) With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

⁵ ~~Similar relationships to which financial institutions should apply criteria (a) to (e) include for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.~~

The Forty Recommendations

8. Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

~~Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non face to face business relationships or transactions.~~

9. Countries may permit financial institutions to rely on ~~intermediaries or other~~ third parties to perform elements (a) – (c) of the CDD ~~measures process~~ or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

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 process~~.
- 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, ~~and~~ supervised or monitored for, and has measures in place to comply with CDD and record keeping requirements in line with Recommendations 5 and 10.
- 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.

~~It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations.~~

When a financial institution relies on a third party which is part of the same financial group, and that group applies CDD and record keeping requirements in line with Recommendations 5, 6 and 10 and programmes against money laundering and terrorist financing in accordance with Recommendation 15 and 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, relevant competent authorities⁶ may consider that the financial institution applies measures under (b) and (c) above through its group programme and may decide that (d) is not a necessary

⁶ The term *relevant competent authorities* means (i) the home authority, that should be involved for the understanding of group policies and controls at group-wide level, and (ii) the host authorities for the involved branches/subsidiaries.

The Forty Recommendations

precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

10. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic ~~and or~~ 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.

Financial institutions should keep all records ~~on the identification data~~ obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

Financial institutions should be required by law to maintain records on transactions and information obtained through the customer due diligence measures.

11. Financial institutions should ~~pay special attention to~~ obtain information on and examine, as far as possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose, ~~when considered against the information collected during the CDD process, when compared to the information collected about the customer during the CDD process.~~ The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

12. The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:
- a) Casinos (including internet casinos) – when customers engage in financial transactions equal to or above the applicable designated threshold.
 - b) Real estate agents - when they are involved in transactions for their client concerning the buying and selling of real estate.
 - c) Dealers in precious metals and dealers in precious stones - when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
 - d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:
 - buying and selling of real estate;
 - managing of client money, securities or other assets;
 - management of bank, savings or securities accounts;
 - organisation of contributions for the creation, operation or management of companies;
 - creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

The Forty Recommendations

- e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

Reporting of suspicious transactions and compliance

- 13. 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, ~~directly~~ by law ~~or regulation~~, to report promptly its suspicions to the financial intelligence unit (FIU).
- 14. Financial institutions, their directors, officers and employees should be:
 - a) Protected by ~~legal provisions-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.
 - b) Prohibited by law from disclosing ("~~tipping-off~~") the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.
- 15. Financial institutions should ~~be required to implement develop~~ 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.~~

~~These programmes should include:~~

- ~~a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.~~
 - ~~b) An ongoing employee training programme.~~
 - ~~c) An audit function to test the system.~~
- 16. The requirements set out in Recommendations 13, to 15 (~~where appropriate~~), and 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:
 - a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.
 - b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
 - c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in Recommendation 12(e).

The Forty Recommendations

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

Other measures to deter money laundering and terrorist financing

17. Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.
18. Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.
19. Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.
20. Countries should consider applying the FATF Recommendations to financial activities (other than those set out in the definition of financial institution), or to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk.

Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.

Measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations

21. ~~Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.~~

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with persons, including legal persons or arrangements companies and financial institutions, from countries for which this is called for by the FATF. The type of EDD measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

The Forty Recommendations

22. Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above are also applied to branches and majority owned subsidiaries located abroad, ~~especially in countries which do not or insufficiently apply the FATF Recommendations to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.~~

Regulation and supervision

23. Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

24. Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.
- a) Casinos (including internet casinos) should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:
- Casinos should be licensed;
 - competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino;
 - competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.
- b) Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The Forty Recommendations

25. The competent authorities and SROs 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.

C. INSTITUTIONAL AND OTHER MEASURES NECESSARY IN SYSTEMS FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Competent authorities, their powers and resources

26. Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of suspicious transaction reports (STRs) ~~receiving (and, as permitted, requesting), analysis and dissemination of STR~~ and other information ~~regarding relevant to~~ potential money laundering, predicate offences or terrorist financing, and the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities and should have access, ~~directly or indirectly,~~ on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, ~~including the analysis of STR.~~
27. Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of a national AML/CFT strategy. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering and terrorist financing offences and underlying predicate offences. This should include cases where the underlying predicate offence occurs outside of their jurisdictions. Countries should ensure that competent authorities have responsibility for, without delay, identifying, tracing and initiating freezing and seizing property that is, or may become subject to confiscation or is suspected of being proceeds of crime. Countries should also be able to make use of permanent or temporary multi-disciplinary groups specialized in financial or asset investigations and that co-operative investigations with appropriate competent authorities in other countries are taking place. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialised in asset investigation, and co-operative investigations with appropriate competent authorities in other countries
28. When conducting investigations of money laundering, terrorist financing and underlying predicate offences, 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 persons, for the search of persons and premises, and for the seizure and obtaining of evidence. Countries should ensure that competent authorities are able to use a wide range of investigative techniques suitable for the investigation of money laundering and terrorist financing. These investigative techniques include at a minimum 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 lawful process to identify assets without prior notification of the owner. When conducting investigations of money laundering, terrorist financing and underlying predicate offences, competent authorities should be able to ask for all relevant information held by the FIU.

The Forty Recommendations

29. Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions under R17 ~~adequate administrative sanctions~~ for failure to comply with such requirements.
30. Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.
31. Countries should ensure that policy makers, the FIU, law enforcement ~~and~~ supervisors and other relevant competent authorities, at the policy making and operational levels, have effective mechanisms in place which enable them to co-operate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering ~~and~~ terrorist financing and the financing of proliferation of weapons of mass destruction⁷.
32. Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation.

Transparency of legal persons and arrangements

33. Countries should take measures to prevent the unlawful use of legal persons for money laundering or terrorist financing. 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, financial institutions and DNFBPs. In particular, countries that have legal persons that are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take appropriate measures to ensure that they are not misused for money laundering or terrorist financing and be able to demonstrate the adequacy of those measures. Countries ~~could~~should consider measures to facilitate access to beneficial ownership and control information to financial institutions and DNFBPs undertaking the requirements set out in Recommendations 5 and 12.
34. Countries should take measures to prevent the unlawful use 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, financial institutions and DNFBPs. Countries ~~could~~should consider measures to facilitate access to beneficial ownership and control information ~~to~~by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 5 and 12.

⁷ In the context of the financing of proliferation of weapons of mass destruction, the FATF's *Best Practices Paper on Recommendation 31* provides a useful reference document and background information for identifying competent authorities that may be particularly relevant.

The Forty Recommendations

D. INTERNATIONAL CO-OPERATION

35. Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, the 2003 United Nations Convention against Corruption, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as ~~the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2001 Council of Europe Convention on Cybercrime~~, the 2002 Inter-American Convention against Terrorism, and the 2005 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism.

Mutual legal assistance and extradition

36. Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, underlying 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 co-operation. In particular, countries should:
- a) Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.
 - b) Ensure that they have clear and efficient processes for the timely prioritisation and execution of mutual legal assistance requests. Countries should use a central authority or another established official mechanism for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained. ~~Ensure that they have clear and efficient processes for the execution of mutual legal assistance 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.

Countries should ensure that of the powers and investigative techniques available to ~~of~~ their competent authorities as required under Recommendation 28:

- (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
- (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.

The Forty Recommendations

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

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. Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. the Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

37. ~~Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.~~ Countries should render mutual legal assistance notwithstanding the absence of dual criminality if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

38. ~~Countries ~~There~~ should~~ ensure that they have the ~~be~~ authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering, underlying predicate offences, and terrorist financing, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction based confiscation proceedings and related provisional measures, unless this is inconsistent with fundamental principles of their domestic law. The country ~~There~~ should also have ~~be~~ effective mechanisms for managing such property, instrumentalities, or property of corresponding value and arrangements for co-ordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

39. Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing without undue delay. In particular, countries should:

- a) Ensure money laundering and terrorist financing are extraditable offences.
- b) Ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained.
- c) Not place unreasonable or unduly restrictive conditions on the execution of requests.
- d) Ensure they have an adequate legal framework for extradition.

~~Countries should recognise money laundering as an extraditable offence.~~ 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

The Forty Recommendations

delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

~~Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.~~

Other forms of co-operation

40.* ~~Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing co-operation. 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.~~

~~Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to money laundering underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:~~

- ~~a) — Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.~~
- ~~b) — Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.~~
- ~~e) — Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.~~

~~Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.~~

Consultation on Draft Revision of the FATF Recommendations

The Forty Recommendations

~~—Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.~~

The IX Special Recommendations

FATF IX SPECIAL RECOMMENDATIONS

SR.I. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

SR.II. Criminalising the financing of terrorism and associated money laundering

Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. The basis for criminalising terrorist financing should be the United Nations International Convention for the Suppression of the Financing of Terrorism, 1999. Countries should ensure that such offences are designated as money laundering predicate offences.

SR.III. Freezing terrorist assets pursuant to relevant UNSCRs

Each ~~jurisdiction country~~ should implement targeted financial sanctions regimes ~~measures to comply with United Nations Security Council Resolutions, relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require jurisdictions to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of any person or entity either i) designated by, or under the authority of, terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with S/RES/1267(1999) and its successor resolutions⁸; or ii) designated by that jurisdiction pursuant to S/RES/1373(2001) resolutions relating to the prevention and suppression of the financing of terrorist acts.~~

~~Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.~~

SR.IV. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

⁸ This Recommendation is applicable to all current and future successor resolutions to S/RES/1267(1999). At the time of issuance of this Recommendation, [INSERT DATE], the successor resolutions to S/RES/1267(1999) are: S/RES/1333(2000), S/RES/1363(2001), S/RES/1390(2002), S/RES/1452(2002), S/RES/1455(2003), S/RES/1526(2004), S/RES/1617(2005), S/RES/1730(2006), S/RES/1735(2006), S/RES/1822(2008), S/RES/1904(2009), S/RES/1988(2011), and S/RES/1989(2011).

The IX Special Recommendations

SR.V. International Co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

SR.VI. Alternative Remittance

~~Countries~~ ~~Each country~~ should take measures to ensure that ~~persons natural~~ or legal ~~persons-entities, including agents,~~ that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered, ~~and~~ subject to all the FATF Recommendations that apply to ~~banks and non-bank~~ financial institutions and subject to effective systems for monitoring and ensuring compliance. Each country should ensure that ~~persons natural~~ or legal ~~persons-entities~~ that carry out this service illegally are subject to administrative, civil or criminal sanctions.

SR.VII. ~~Wire~~ Electronic funds transfers

~~Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.~~

~~Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).~~

Countries should ensure that financial institutions include full and accurate originator information, and full recipient⁹ information, on electronic funds transfers (EFT) and related messages, and that the information remains with the EFT or related message through the payment chain.

Countries should ensure that financial institutions monitor EFT for the purpose of detecting those which lack required originator and/or recipient information, and take appropriate measures.

Countries should ensure that, in the context of processing EFT, financial institutions take freezing action and should prohibit conducting transactions with designated parties, as per the obligations which are set out in the relevant United Nations Security Council Resolutions, such as S/RES/1267(1999) and its successor resolutions, and S/RES/1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

⁹ The paper “Due diligence and transparency regarding cover payment messages related to cross border wire transfers” by the Basel Committee on Banking Supervision (May 2009) uses the terms “beneficiary” for “recipient” and “beneficiary financial institution” for “receiving financial institution”.

The IX Special Recommendations

SR.VIII. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

- (i) by terrorist organisations posing as legitimate entities;
- (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and
- (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

SR.IX. Cash Couriers

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including implementing a declaration system or other disclosure obligation.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or instruments.

SR.X. Targeted financial sanctions related to proliferation

Each jurisdiction should implement targeted financial sanctions¹⁰ to comply with United Nations Security Council Resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.¹¹ These resolutions require jurisdictions to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any person or entity designated by, or under

¹⁰ This Recommendation and Interpretative Note are focused on targeted financial sanctions. However, it should be noted that the relevant United Nations Security Council Resolutions are much broader and prescribe other types of sanctions (such as travel bans) and other types of financial provisions (such as activity-based financial prohibitions and vigilance provisions). With respect to other types of financial provisions, the FATF has issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs. With respect to targeted financial sanctions related to the financing of proliferation of weapons of mass destruction, the FATF has also issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs.

¹¹ This Recommendation is applicable to all current UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, and any future successor resolutions. At the time of issuance of this Recommendation, [INSERT DATE], the UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: S/RES/1718(2006), S/RES/1737(2006), S/RES/1747(2007), S/RES/1803(2008), S/RES/1874(2009), and S/RES/1929(2010).

Consultation on Draft Revision of the FATF Recommendations

The IX Special Recommendations

the authority of, the United Nations Security Council under Chapter VII of the *Charter of the United Nations* .

Interpretative Notes

INTERPRETATIVE NOTES TO THE 40 RECOMMENDATIONS

General

- ~~1. Reference in this document to “countries” should be taken to apply equally to “territories” or “jurisdictions”.~~
- ~~2. Recommendations 5-16 and 21-22 state that financial institutions or designated non-financial businesses and professions should take certain actions. These references require countries to take measures that will oblige financial institutions or designated non-financial businesses and professions to comply with each Recommendation. The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation, while more detailed elements in those Recommendations, as well as obligations under other Recommendations, could be required either by law or regulation or by other enforceable means issued by a competent authority.~~
- ~~3. Where reference is made to a financial institution being satisfied as to a matter, that institution must be able to justify its assessment to competent authorities.~~
- ~~4. To comply with Recommendations 12 and 16, countries do not need to issue laws or regulations that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions so long as these businesses or professions are included in laws or regulations covering the underlying activities.~~
- ~~5. The Interpretative Notes that apply to financial institutions are also relevant to designated non-financial businesses and professions, where applicable.~~

Interpretative Notes - RBA

Interpretative Note on the Risk-based Approach

1. The Risk-Based Approach (RBA) is an effective way to combat ML and TF. In determining how the RBA should be implemented in a sector, countries should consider the capacity and AML/CFT experience of the relevant sector. Countries should understand that the discretion afforded and responsibility imposed on financial institutions and DNFBPs by the RBA is more appropriate in sectors with greater AML/CFT capacity and experience. This should not exempt financial institutions and DNFBPs from the requirement to apply enhanced measures when they identify higher risk scenarios. By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified, and be able to allocate resources in the most effective way.
 2. In implementing a RBA, financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate ML/TF risks. The general principle of a RBA is that where there are higher risks countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks, and that correspondingly where the risks are lower simplified measures may be permitted. Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing. The analysis of risk should also help competent authorities to make their decisions on how to most effectively allocate their own resources. Specific Recommendations set out more precisely how this general principle applies to particular requirements. Countries may also in strictly limited circumstances and where there is a proven low risk of money laundering and terrorist financing decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP (see below). Equally, if countries determine through their risk assessments that there are types of institutions, activities, businesses or professions that are at risk of abuse from ML/TF, and which do not fall under the definition of financial institution or DNFBP, they should consider applying AML/CFT requirements to such sectors. In implementing a RBA, countries, financial institutions and DNFBPs should consider the FATF RBA Guidance.
- A. *Obligations and decisions for countries*
3. **Assessing risk** – Countries¹² should take appropriate steps to identify and assess the ML/TF risks for the country, on an ongoing basis and as appropriate, in order to: (i) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures, (ii) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (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 competent authorities and SROs, financial institutions and DNFBPs. Countries should consider the FATF Guidance on... .
 4. **Higher risk** - Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks and, without prejudice to any other measures taken by countries to mitigate these higher risks, either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk

¹² Where appropriate, AML/CFT risk assessments at a supranational level may be considered as satisfying this obligation.

Interpretative Notes - RBA

assessments carried out by financial institutions and DNFBPs, in order to appropriately manage and mitigate risks.

5. **Lower risk** - Countries may decide to allow simplified measures for some of the FATF Recommendations¹³ requiring financial institutions or DNFBPs to take certain actions, provided that a lower risk has been identified and this is consistent with the country's assessment of its money laundering and terrorist financing risks, as referred to in paragraph 3.

Independent of any decision to specify certain lower risk categories in line with the previous paragraph, countries may also allow financial institutions and DNFBPs to apply simplified CDD measures, provided the requirements set out in section B below ("obligations and decisions for financial institutions and DNFBPs") and in paragraph 7 below are met.

Where Recommendations (e.g. R.6, R.7, and SR.VII) require enhanced or specific measures to be taken, the risk based approach does not permit such measures to be omitted on the basis of lower risk. However, the extent of such measures, when the nature of the measure allows it, may vary according to the level of risk.

While the information gathered may vary according to the level of risk, the requirements of R.10 to retain information should apply to whatever information is gathered.

6. **Exemptions** - Countries may decide not to apply some of the FATF Recommendations¹⁴ requiring financial institutions or DNFBPs to take certain actions, provided:
- a) this occurs in strictly limited and justified circumstances;
 - b) it is based on a proven low risk of money laundering and terrorist financing; and
 - c) it relates to a particular type of financial institution or activity, or DNFBP.

7. **Supervision and monitoring of risk** – Competent authorities (or SROs for DNFBPs other than casinos) should ensure that financial institutions and DNFBPs are effectively implementing the obligations set out below. When carrying out this function, competent authorities and SROs should as and when required in accordance with INR.23 and 24, review the ML/TF risk profiles and risk assessments prepared by financial institutions and DNFBPs and take the result of this review into consideration.

B. Obligations and decisions for financial institutions and DNFBPs

8. **Assessing risk** - Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their ML/TF risks (for customers, countries or geographic areas; and products/services/transactions/delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SROs. The nature and extent of any assessment of ML/TF risks should be appropriate to the nature and size of the business. Financial institutions and DNFBPs should always understand their ML/TF risks, but, competent authorities or SROs may determine that individual documented risk assessments are not required if the specific risks inherent to the sector are clearly identified and understood.

¹³ Countries should not allow simplified measures for R.13 and R.16 (applying R.13)

¹⁴ Countries should not allow exemptions for SR.VI or SR.VII

Interpretative Notes - RBA

9. **Risk management and mitigation** - Financial institutions and DNFBPs should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified (either by the country or by the financial institution or DNFBP). They should be required to monitor the implementation of those controls and to enhance them if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SROs.
10. **Higher risk** - Where higher risks are identified financial institutions and DNFBPs should be required to take enhanced measures to manage and mitigate the risks, as set out in R.5.
11. **Lower risk** - Where financial institutions and DNFBPs identify lower risks, countries may allow them to take simplified measures to manage and mitigate those lower risks, as set out in R.5.
12. **When assessing risk, financial institutions and DNFBPs should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. Financial institutions and DNFBPs may differentiate the extent of measures depending on the type and level of risk for the various risk factors, e.g. in a particular situation, it could apply standard CDD for customer acceptance measures but enhanced CDD for ongoing monitoring or vice versa.**

Interpretative Notes

INR.3 and 38

Countries should establish mechanisms that will enable their competent authorities to effectively manage, and when necessary dispose of, property that is frozen or seized, or has been confiscated. These mechanisms should be applicable both in the context of domestic proceedings, and pursuant to requests by foreign countries. In this regard, countries should consider the Best Practices paper on Confiscation.

INR 5, 12 and 16

The designated thresholds for transactions ~~(under Recommendations 5 and 12)~~ are as follows:

- ~~• Financial institutions (for occasional customers under Recommendation 5) - USD/EUR 15,000.~~
- Casinos, including internet casinos (under Recommendation 12) - USD/EUR 3000
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16) - USD/EUR 15,000.

Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

The Interpretative Notes that apply to financial institutions are also relevant to designated non-financial businesses and professions, where applicable. To comply with Recommendations 12 and 16, countries do not need to issue laws or regulations that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions so long as these businesses or professions are included in laws or regulations covering the underlying activities.

Interpretative Notes – R.5

INR.5

Customer due diligence and tipping off

1. 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:
 - a) Normally seek to identify and verify the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply.
 - b) Make a STR to the FIU in accordance with Recommendation 13.
2. Recommendation 14 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.
3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping off when performing the CDD customer due diligence process. 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. Institutions should ensure that their employees are aware of and sensitive to these issues when conducting CDD.

CDD – persons acting on behalf of a customer

4. When performing elements (a) and (b) of the CDD measures specified under Recommendation 5, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person. Financial institutions are not required to verify the identity of any person (or any employee of that person) acting on behalf of the customer where the person is not a third party nor a person who usually acts on behalf of customers in its ordinary course of business (e.g. lawyers, accountants, investment firms) and the person is regulated or supervised and is monitored for money laundering and terrorist financing purposes by a competent authority.

CDD for legal persons and arrangements

5. When performing the CDD process in relation to customers that are legal persons or legal arrangements¹⁵, financial institutions should be required to identify and verify the customer and understand the nature of its business, and its ownership and control structure. The purpose of the requirements set out in (a) and (b) below regarding the identification and verification of the customer and the beneficial owner is twofold, namely to prevent the unlawful use of legal persons

¹⁵ In these Recommendations references to legal arrangements such as trusts (or other similar arrangements) being the customer of a financial institution or DNFBP or carrying out a transaction, refers to situations where a natural or legal person that is the trustee establishes the business relationship or carries out the transaction on the behalf of the beneficiaries or according to the terms of the trust. The normal CDD requirements for customers that are natural or legal persons would continue to apply, including paragraph 4 of INR.5, but in addition, the additional requirements regarding the trust and the beneficial owners of the trust (as defined) would also apply.

Interpretative Notes – R.5

and arrangements, by gaining a sufficient understanding of the customer to be able to properly assess the potential money laundering and terrorist financing risks associated with the business relationship and then to take appropriate steps to mitigate the risks. As two aspects of one process, these requirements are likely to interact and complement each other naturally.– In this context, financial institutions should be required to:

a) Identify the customer and verify its identity. The type of information that would normally be needed to perform this function would be:

i. Name, legal form and proof of ~~current~~ existence – verification could be obtained for example through a certificate of incorporation, a certificate of good standing, ~~a document from the public register~~ a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

ii. ~~The powers that regulate and bind the legal person or arrangement e.g. the memorandum and articles of association of a company, as well as~~ ~~The names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).~~

iii. The address of the registered office ~~and or, in its absence,~~ the main physical place of business, ~~if different~~

b) Identify the beneficial owners of the customer and take reasonable measures¹⁶ to verify the identity of such persons. The types of measures that would normally be needed to perform this function satisfactorily would require obtaining and taking reasonable measures to verify the following information:

i. For legal persons: (i.i) the identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest in a legal person – ~~a natural person or group of natural persons acting together who own 25% or more of the legal person are deemed to have a controlling interest of the legal person,~~ or (i.ii) where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means ; or (i.iii) where no natural person is identified under i.i. or i.ii. above, the identity of the relevant natural person who holds the position of senior managing official.

ii. For legal arrangements: (ii.i) trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries / class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership); (ii.ii) other types of legal arrangements – the identity of persons in equivalent or similar positions.

Where the customer or the owner of the controlling interest is a company listed on a recognised stock exchange, and subject to disclosure requirements, it is not necessary to identify and verify the identity of any shareholder of that company. ~~In addition, where the customer or the owner of the~~

¹⁶ In determining the reasonableness of the identity verification measures, regard should be had to the money laundering and terrorist financing risks posed by the customer and the business relationship.

Interpretative Notes – R.5

controlling interest is a financial institution or DNFBP regulated or supervised and monitored for money laundering and terrorist financing purposes by a competent authority in an equivalent jurisdiction, it is not necessary to identify and verify the identity of any shareholder of that company.

The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

CDD for beneficiaries of life insurance policies

6. For life or other investment related insurance business, financial institutions should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies as soon as the beneficiary(ies) is identified/designated:

- a) for beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;
- b) for beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

The information collected under (a) and/or (b) should be recorded and maintained in accordance with the provisions of Recommendation 10.

7. For both the cases referred to above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout or at the time when the beneficiary(ies) intends to exercise vested rights.

8. Where there is higher risk identified, and in particular through the financial institution's relationship with the policyholder, the identification and verification on the basis of reasonable measures of the identity of the beneficial owner of a beneficiary, which is a legal person or legal arrangement, would be required at the time of the payout or at the time when the beneficiary(ies) intends to exercise vested rights.

9. Where a financial institutions is unable to comply with paragraphs (6) to (8) above, it should consider making a suspicious transaction report.

Reliance on identification and verification already performed

10. The CDD measures set out in Recommendation 5 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated which is not consistent with the customer's business profile.

Interpretative Notes – R.5

Timing of verification

11. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of life insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business include:
 - Non face-to-face business.
 - Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
 - ~~Life insurance business. In relation to life insurance business, countries may permit the identification and verification of the beneficiary under the policy to take place after having established the business relationship with the policyholder. However, in all such cases, identification and verification should occur at or before the time of payout or the time where the beneficiary intends to exercise vested rights under the policy.~~
12. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of expected norms for that type of relationship. ~~Financial institutions should refer to the Basel CDD paper¹⁷ (section 2.2.6.) for specific guidance on examples of risk management measures for non face to face business.~~

Requirement to identify New customers and existing customers

13. ~~The principles set out in the Basel CDD paper concerning the identification of existing customers should serve as guidance when applying customer due diligence processes to institutions engaged in banking activity, and could apply to other financial institutions where relevant. Financial institutions should be required to apply CDD measures to existing customers¹⁸ on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.~~

Risk Based Approach

Higher risks

14. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher risk situations (in addition to those set out in Recommendations 6, 7 and 8) include the following:

¹⁷ ~~“Basel CDD paper” refers to the guidance paper on Customer Due Diligence for Banks issued by the Basel Committee on Banking Supervision in October 2001.~~

¹⁸ ~~Existing customers as at the date that the national requirements are brought into force.~~

Interpretative Notes – R.5

(a) Customer risk factors:

- The business relationship is conducted in unusual circumstances e.g. significant unexplained geographic distance between the financial institution and the customer.
- Non-resident customers.
- Legal persons or arrangements that are personal asset holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash intensive.

(b) Country or geographic risk factors¹⁹:

- Countries identified by credible sources such as mutual evaluation or detailed assessment reports or published follow-up reports, as having inadequate AML/CFT laws, regulations and other measures.
- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:

- Private banking.
- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or transactions.
- Payment received from unknown or un-associated third parties

Other examples of higher risk situations are set out in the FATF Guidance on the Risk-Based Approach, which countries and financial institutions should consider when applying a Risk-Based Approach.

Lower risks

15. There are circumstances where the risk of ML or TF may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures.

¹⁹ Under Recommendation 21 it is mandatory for countries to require financial institutions to apply enhanced due diligence when the FATF calls for such measures to be introduced.

Interpretative Notes – R.5

16. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

(a) customer risk factors:

- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
- Public companies listed on a regulated stock exchange and which are subject to regulatory disclosure requirements.
- Public administrations or enterprises.

(b) product, service, transaction or delivery channel risk factor:

- Life insurance policies where the annual premium is no more than USD/EUR 1 000 or a single premium is no more than USD/EUR 2 500.
- Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.
- Financial products or services that provide appropriately defined and limited services to certain types of customers so as to increase access for financial inclusion purposes.

(c) country risk factors:

- Country identified by credible sources such as mutual evaluation or detailed assessment reports, as adequately complying with and having effectively implemented the FATF Recommendations.
- Country identified by credible sources as having a low level of corruption, or other criminal activity.

In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in ML/TF risk between different regions or areas within a country.

Financial institutions, in their assessments of risk, could also consider the higher risk or lower risk situations identified in the FATF Global Threat Assessment.

17. Having a lower ML/TF risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for on-going monitoring of transactions. For example, transactions conducted by a listed company with public enterprises in countries/sectors where the risk of corruption is significant through a bank specialising in trade finance for this sector/region could require enhanced ongoing due diligence on certain transactions but not require enhanced measures regarding the identification and verification of the listed company.

Interpretative Notes – R.5

Risk Variables

18. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a financial institution should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship.
- The level of assets to be deposited by a customer or the size of transactions undertaken.
- The regularity or duration of the business relationship.

Enhanced CDD measures

19. Financial institutions should examine, as far as possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose when considered against the information collected about the customer during the CDD process. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher risk business relationships include:

- Obtaining additional information on the customer (occupation, volume of assets, information available through public databases, internet, etc) and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Simplified CDD measures

20. Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors e.g. the simplified measures could relate only to customer acceptance measures or to aspects of on-going monitoring. Examples of possible measures are:

Interpretative Notes – R.5

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship, e.g. if account transactions rise above a defined monetary threshold.
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinising transactions based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific higher risk scenarios apply.

Thresholds

21. The designated threshold for transactions by occasional customers under Recommendation 5 is: USD/EUR 15,000. Financial transactions above the designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Interpretative Notes

INR.6

~~Countries are encouraged to extend the requirements of Recommendation 6 to individuals who hold prominent public functions in their own country.~~

- ~~1. Financial institutions should be required to have appropriate risk management systems to determine whether the beneficiaries of a life insurance policy and/or the beneficial owner of the beneficiary are foreign politically exposed persons. This should occur at the latest at the time of the payout or when the beneficiary intends to exercise vested rights. In addition to performing normal CDD measures, financial institutions should be required to:
 - ~~a) Inform senior management before the payout of the policy proceeds.~~
 - ~~b) Conduct enhanced scrutiny on the whole business relationship with the policyholder and consider making a suspicious transaction report.~~~~
- ~~2. Financial institutions should be required to take reasonable measures to determine whether the beneficiaries of a life insurance policy and/or the beneficial owner of the beneficiary is a politically exposed person. In cases of higher risk, financial institutions should be required to apply the measures (b) and (c) above.~~

INR.7

~~The similar relationships to which financial institutions should apply criteria (a) to (e) include for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.~~

INR9

~~This Recommendation does not apply to outsourcing or agency relationships. In a third party reliance scenario, the third party should be subject to CDD and record keeping requirements in line with Recommendations 5 and 10 and be regulated, supervised or monitored. The third party will usually have an existing business relationship with the customer which is independent from the relationship to be formed with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution or DNFBP, in accordance with its procedures and is subject to the delegating financial institution's or DNFBP's control of the effective implementation of those procedures by the outsourced entity.~~

~~This Recommendation also does not apply to relationships, accounts or transactions between financial institutions for their clients. Those relationships are addressed by Recommendations 5 and 7.~~

INR10 and 11

~~In relation to insurance business, the word "transactions" should be understood to refer to the insurance product itself, the premium payment and the benefits.~~

INR13

1. The reference to criminal activity in Recommendation 13 refers to:

Interpretative Notes

- a) all criminal acts that would constitute a predicate offence for money laundering or terrorist financing, including funds that are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism in the jurisdiction; or
- b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1.

Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

2. ~~In implementing Recommendation 15, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state *inter alia* that their transactions relate to tax matters.~~

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 ML or FT offence or otherwise (so called “indirect reporting”), is not acceptable.

(
Reinstate deleted Paragraph 2 above

INR14 (tipping off)

~~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.~~

INR15

1. Financial institutions programmes against money laundering and terrorist financing should include:
 - a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.
 - b) An ongoing employee training programme.
 - c) An independent audit function to test the system.
2. The type and extent of measures to be taken ~~for each of the requirements set out in the Recommendation~~ should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.
3. Compliance management arrangements should include the appointment of a compliance officer at the management level.
4. 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 measures under (a) to (c) above, and should be appropriate to the business of the branches and majority owned subsidiaries. Such programmes should be effectively implemented at the level of branches and majority-owned subsidiaries. These programmes should include policies and procedures for sharing information required for the purposes of CDD and

Interpretative Notes

ML/FT risk management. Group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. Adequate safeguards on the confidentiality and use of information exchanged should be in place. ~~If the host country does not permit the proper implementation of the measures above, financial groups should apply additional safeguards to manage the potential ML/TF risks. Host countries of branches and subsidiaries of financial groups based in other countries should not prevent the adoption, by any means, of all of the elements of a group's AML and TF programmes by local branches and subsidiaries of the financial group, where the Group's programme is at least compliant with the minimum local requirements of the host country to combat money laundering and terrorist financing.~~

INR16

1. It is for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.
2. 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 co-operation between these organisations and the FIU.
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.21

The enhanced due diligence measures that could be undertaken by financial institutions include those measures set out in paragraph 19 of INR.5, and any other measures that have a similar effect in mitigating risks.

Examples of the counter-measures that could be undertaken by countries include the following, and any other measures that have a similar effect in mitigating risks:

- Requiring financial institutions to apply specific elements of Enhanced Due Diligence.
- Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions.
- Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.
- Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems.

Interpretative Notes

- Limiting business relationships or financial transactions with the identified country or persons in that country.
- Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process.
- Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned.
- Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned.
- Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

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

Interpretative Note to R.22

Where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit.

INR23

~~Recommendation 23 should not be read as to require the introduction of a system of regular review of licensing of controlling interests in financial institutions merely for anti money laundering purposes, but as to stress the desirability of suitability review for controlling shareholders in financial institutions (banks and non banks in particular) from a FATF point of view. Hence, where shareholder suitability (or “fit and proper”) tests exist, the attention of supervisors should be drawn to their relevance for anti money laundering purposes.~~

Risk-based approach to Supervision

1. Risk-based approach to supervision refers to (a) the general process by which a supervisor according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising institutions that apply an AML/CFT risk-based approach.
2. Adopting a risk-based approach to supervising financial institutions’ AML/CFT systems and controls allows supervisory authorities to shift resources to those areas that are perceived to present higher risk. As a result supervisory authorities can use their resources more effectively. This means that supervisors: (a) should have a clear understanding of the ML/FT risks present in a country, and (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). The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions/groups should be based on the ML/FT risks and the

Interpretative Notes

policies, internal controls and procedures associated with the institution/group as identified by the supervisor's assessment of the institution/group's risk profile and on the ML/FT risks present in the country.

3. The assessment of the ML/FT risk profile of a financial institution/group, including the risks of non-compliance, should be reviewed both periodically and when there are major events or developments in the management and operations of the financial institution/group, in accordance with the country's established practices for ongoing supervision. This assessment should not be static; it will change depending on how circumstances develop and how threats evolve.
4. AML/CFT supervision of financial institutions/groups that apply a risk-based approach should take into account the degree of discretion allowed under RBA to the financial institution/group, and encompass in an appropriate manner a review of the risk assessments underlying this discretion, and of the adequacy and implementation of its policies, internal controls and procedures.
5. These principles should apply to all financial institutions/groups. To ensure effective AML/CFT supervision, supervisors should take into consideration the characteristics of the financial institutions/groups, in particular the diversity and number of financial institutions and the degree of discretion allowed to them under RBA.

Resources of supervisors

6. Countries should provide their competent authorities responsible for supervision with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

INR 24

1. Risk-based approach to supervision refers to (a) the general process by which a supervisor or SRO, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising or monitoring institutions that apply an AML/CFT risk-based approach.
2. Competent authorities and SROs should determine the frequency and intensity of their supervisory or monitoring actions on DNFBPs on the basis of their understanding of the ML/TF risks, and taking into consideration their characteristics, in particular the diversity and number of DNFBPs, in order to ensure effective AML/CFT supervision or monitoring. This means having a clear understanding of the ML/TF risks: (a) present in the country, and (b) associated with the type of DNFBP and their customers, products and services.
3. Competent authorities or SROs assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs should properly take into account the ML/TF risk profile of those DNFBPs, and the degree of discretion allowed to them under RBA.
4. Competent authorities and SROs should have adequate powers to perform their functions (including powers to monitor and sanction), and adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

Interpretative Notes

INR25

When considering the feedback that should be provided, countries should have regard to the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.

INR26

~~Where a country has created an FIU, it should consider applying for membership in the Egmont Group. Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU.~~

General

This note explains the core mandate and functions of a financial intelligence unit (FIU) and provides further clarity on the obligations contained in the standard. The FIU is part of and plays a central role in a country's AML/CFT operational network, and provides support to the work of other competent authorities. Considering that there are different FIU models, Recommendation 26 does not prejudge a country's choice for a particular model and applies equally to all of them.

Functions

(a) Receipt

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 (STRs), as required by Recommendation 13, Special Recommendation IV and Recommendation 16, and it should include other information as required by national legislation (such as cash transaction reports, electronic funds transfers reports and other threshold – based declaration/disclosures).

(b) Analysis

FIU analysis should add value to the information received and held by the FIU. While all the information should be considered, the analysis may focus either on each single disclosure received or on appropriate selected information, depending on the type and volume of the disclosures received, and on the expected use after dissemination. FIUs should be encouraged to use analytical software to process information more efficiently and assist in establishing relevant links; however such tools cannot fully replace the human judgement element of analysis. FIUs should conduct the following types of analysis:

- Operational analysis uses available and obtainable information to identify specific targets (e.g. persons, assets, criminal networks and associations), to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences or terrorist financing.
- Strategic analysis uses available and obtainable information, including data that may be provided by other competent authorities, to identify ML/TF related trends and patterns. This information is then also used by the FIU or other state entities in order to determine ML/TF related threats and vulnerabilities. Strategic analysis may also help establish policies and goals for the FIU or more broadly for other entities of within the AML/CFT regime.

Interpretative Notes

(c) Dissemination

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 analysis, dissemination 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 28. 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.

Access to Information

(a) Obtaining Additional Information from Reporting Entities

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 properly perform its analysis. 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 (R.10, R.12 and R.21).

(b) Access to Information from other sources

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 information from open or public sources as well as relevant information collected and/or maintained by or on behalf of other state authorities and, where appropriate, commercially held data.

Information Security and Confidentiality

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.

Operational Independence

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, request 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.

An FIU may be established as part of an existing governmental authority. When a FIU is located within the existing structure of another authority, the FIU's core functions should be distinct from those of the other authority.

The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively. Countries should

Interpretative Notes

have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

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.

Undue Influence or Interference

The FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

Egmont Group

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 Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU). The FIU should apply for membership in the Egmont Group.

Large Cash Transaction Reporting

Countries should consider the feasibility and utility of a system where financial institutions and DNFBPs would report all domestic and international currency transactions above a fixed amount.

Interpretative Notes

INR27

~~Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.~~

There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, predicate offences and terrorist financing are properly investigated through the conduct of a financial investigation. Countries should also designate one or more competent authorities to identify, trace, and initiate freezing and seizing of property that is or may become subject to confiscation.

A ‘financial investigation’ means an enquiry into the financial affairs related to a suspect, with a view to:

- Identifying the extent of criminal networks and/or the scale of criminality.
- Identifying and tracing the proceeds of crime, terrorist funds or any other assets that are or may become subject to confiscation.
- Developing evidence which can be used in criminal proceedings.

A ‘parallel financial investigation’ refers to conducting a financial investigation alongside or in the context of a (traditional) criminal investigation into ML, TF and/or predicate offence(s). Law enforcement investigators of offences in the designated categories of offences should either be authorised to pursue the investigation of any related ML/TF offences during a parallel investigation, or be able to refer the case to another designated agency to follow up with such investigations.

Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering and terrorist financing cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

Recommendation 27 also applies to those competent authorities which are not law enforcement authorities per se, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under R.27.

Anti-corruption enforcement authorities with enforcement powers may be designated to investigate ML and FT offences arising from or related to corruption offences under R.27 and these authorities should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets.

The range of law enforcement agencies and other competent authorities mentioned above should be taken into account when jurisdictions make use of multi-disciplined groups in financial investigations. Law Enforcement Authorities and Prosecutorial Authorities should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

Interpretative Notes

INR33

1. Competent authorities, financial institutions and DNFBPs 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 information²⁰) that are created²¹ 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.
2. 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 and forms and basic features of legal persons in the country.
 - b) Identify and describe the processes: (i) for the creation of those legal persons, and (ii) for the obtaining and recording of basic and beneficial ownership information.
 - c) Make the above information publicly available.
 - d) Assess the ML/TF risks associated with different types of legal persons created in the country.

A. Basic Information

3. In order to determine who the beneficial owners of a company are, competent authorities, financial institutions and DNFBPs will require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. This would include information about the status and powers of the company, its shareholders and its directors.
4. All companies created in a country should be registered in a company registry²². Whichever combination of mechanisms are used to obtain and record beneficial ownership information (see section B), there is a set of basic information on a company that needs to be obtained and recorded by the company²³ 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 shareholder²⁴ and categories of shares (including the nature of the associated voting rights).
5. The company registry should record all the basic information set out in paragraph 4(a) above.

²⁰ Beneficial ownership information for legal persons is the information referred to in INR.5, paragraph 5(b)(i). Controlling shareholders as referred to in INR5, paragraph 5(b)(i) must be based on a threshold, e.g. any persons owning more than 25% a certain percentage of the company (e.g. 24%)

²¹ References to creating a legal person, include incorporation of companies or any other mechanism that is used.

²² "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.

²³ The information can be recorded by the company itself or by a third person under the company's responsibility.

²⁴ This is applicable to the nominal owner of all registered shares.

Interpretative Notes

6. The company should maintain the basic information set out in paragraph 4(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 the company can provide this information promptly on request.

B. Beneficial Ownership Information

7. 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.

8. In order to meet the requirements in paragraph 6, countries should use one or more of the following mechanisms:

a) (i) Requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership;

b) (ii) Requiring companies to take reasonable measures²⁵ to obtain and hold up-to-date information on the companies' beneficial ownership;

c) (iii) ~~Using existing information, including (i) information obtained by financial institutions and/or DNFBS, in accordance with Recommendations 5 and 12²⁶, (ii) information held by other competent authorities on the legal and beneficial ownership of companies, for example company registries, tax authorities or financial or other regulators, and (iii) information held by the company as required above in Section A.~~

9. 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:

- Requiring that one or more natural persons resident in the country is authorised by the company²⁷ and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or
- Requiring that a DNFBS 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
- Other comparable measures specifically identified by the country which can effectively ensure cooperation.

10. All the persons, authorities and entities mentioned above, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should maintain the information and records referred to for at least five years after the date on which the company is dissolved or otherwise ceases to exist, or five years after the date on which the company

²⁵ 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.

²⁶ Countries should be able to determine in a timely manner whether a company has an account with a financial institution within the country.

²⁷ Members of the company's board or senior management may not require specific authorisation by the company.

Interpretative Notes

ceases to be a customer of the professional intermediary or the financial institution (for such intermediaries/institutions).

C. Timely access to current and accurate information

11. Countries should have mechanisms that ensure that basic and beneficial ownership 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.
12. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary in order to be able to obtain timely access to the basic and beneficial ownership information held by the relevant parties.
13. 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 paragraph 4(a) and beneficial ownership information above. Countries should consider also facilitating timely access by FIs and DNFBPs to information referred to in paragraph 4(b) above.
14. Countries should require companies to inform their company registry of any changes in previously filed basic or beneficial ownership information within a reasonable time of the change. Countries should require companies to confirm to the registry, on an annual basis, there has been no changes in the basic or beneficial information that have not been notified to the registry.

D. Obstacles to Transparency

14. 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: (a) prohibiting them; (b) converting them to registered shares or share warrants (for example through dematerialisation); (c) immobilising them by requiring them to be held with a regulated financial institution or professional intermediary, or (d) requiring shareholders with a controlling interest to notify the company, and the company to record their identity.
15. 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) require 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) require nominee 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, financial institutions and DNFBP upon request.

E. Other Legal Persons

17. 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.
18. As regards other types of legal persons, countries should take into account the different forms and structures of those other legal persons, and the levels of ML/TF risks associated with each type of legal person with a view to achieving appropriate levels of transparency. 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

Interpretative Notes

authorities, financial institutions and DNFBPs. Countries should review the ML/TF 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.

F. Liability and sanctions

19. There should be a clearly stated responsibility to comply with the requirements in this Interpretative Note, as well as liability and effective, proportionate and dissuasive sanctions as appropriate for any legal or natural person that fails to properly comply with the requirements.

G. International Cooperation

20. Countries should rapidly, constructively and effectively provide international cooperation in relation to basic and beneficial ownership information, on the basis set out in R.36 and R.40. This should include (a) facilitating access by foreign competent authorities to basic and beneficial ownership information held by company registries; (b) exchanging information on shareholders and beneficial owners 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.

Interpretative Notes

INR34

1. 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.
2. All countries should take measures to ensure that trustees disclose their status as a trustee to financial institutions and DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold as a trustee. Trustees should not be prevented by law or enforceable means from providing competent authorities with any information relating to the trust²⁸; 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.
3. Countries ~~should be 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:
 - Registries (for example, a central registry of trusts or trust assets), or asset registries for land, property, vehicles, shares or other assets.
 - Other competent authorities that hold information on trusts and trustees, for example tax authorities which collect information on assets and income relating to trusts.
 - Other agents and service providers to the trust, including investment advisors or managers.
4. 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.
5. Professional trustees should be required to maintain the information referred to in paragraph 1 for at least five years after their involvement with the trust ceases. Countries are encouraged to require non-professional trustees and the other authorities, persons and entities mentioned in paragraph 3 above to maintain the information for at least five years.
6. Countries should require that any information held pursuant to paragraph 1 above should be kept accurate and be as current and up to date as possible, and the information should be updated within a reasonable period following any change.
7. Countries should ~~consider measures to~~ facilitate access to any information on trusts that is held by the other authorities, persons and entities referred to in paragraph 3, by Financial Institutions and DNFBPs undertaking the requirements set out in Recommendations 5 and 12.

²⁸ Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

Interpretative Notes

8. In the context of this Recommendation, countries are not required to give legal recognition to trusts. Countries need not include the requirements of paragraphs 1, 2 and 6 in legislation, provided that appropriate obligations to such effect exist for trustees, e.g. through common law or case law.

Other Legal Arrangements

9. 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, financial institutions and DNFBPs.

International Cooperation

10. 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 R.36 and R.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.

Liability and Sanctions

11. Countries should ensure that there are clear responsibilities to comply with the requirements in this Interpretative Note; and that trustees are either legally liable for any failure to perform the duties relevant to meeting the obligations in paragraphs 1, 2, 6 and (where applicable) 5; or that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply²⁹. Countries should ensure that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to grant to competent authorities timely access to information regarding the trust referred to in paragraph 1 and 5.

²⁹ This does not affect the requirements for effective, proportionate, and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

Interpretative Notes

INR38

For the purposes of R38, the term *non-conviction based confiscation* means confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required. Jurisdictions need not have the authority to act on the basis of all such requests, but should be able to do so, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown.

Countries should consider ~~(a)~~ establishing an asset forfeiture fund in its respective country into which all or a portion of confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes. ~~(b)~~ Countries should take such measures as may be necessary to enable it to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.

INR40

Principles applicable to all forms of international cooperation:

Obligations on requesting authorities

1. When making requests for co-operation, 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.

Unduly restrictive measures

2. 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.

Safeguards on information exchanged

3. 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.

Interpretative Notes

4. 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 inquiry³⁰, 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.

Power to search for information

5. 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.

Principles applicable to specific forms of international cooperation

6. 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.

Exchange of information between FIUs

7. 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, predicate offences and terrorist financing.

8. When making a request for co-operation, 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.

9. 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 R.26, 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.

Exchange of information between financial supervisors

10. Financial supervisors should co-operate 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

³⁰

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

Interpretative Notes

standards for supervision, in particular the exchange of supervisory information related to or relevant for AML/CFT purposes.

11. 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 ~~of~~ financial institutions operating in the same a group:

- Regulatory information, such as information on the domestic regulatory system, general information on financial sectors.
- 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.
- AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

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

13. 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 an MOU or the Multi-lateral Memorandum of Understanding (MMOU) issued by a core principles standard-setter applied to information exchanged under the MOU or the MMOU.

Exchange of information between law enforcement authorities

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

15. 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.

16. 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

Interpretative Notes

agencies, including placing liaison officers abroad, in order to facilitate timely and effective cooperation.

Exchange of information between non counterparts

17. 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.

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

~~1. For the purposes of this Recommendation:~~

- ~~• “Counterparts” refers to authorities that exercise similar responsibilities and functions.~~
- ~~• “Competent authority” refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.~~

~~2. Depending on the type of competent authority involved and the nature and purpose of the co-operation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include: bilateral or multilateral agreements or arrangements, memoranda of understanding, exchanges on the basis of reciprocity, or through appropriate international or regional organisations. However, this Recommendation is not intended to cover co-operation in relation to mutual legal assistance or extradition.~~

~~3. The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.~~

~~4. FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:~~

- ~~• Searching its own databases, which would include information related to suspicious transaction reports.~~
- ~~• Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.~~

~~Where permitted to do so, FIUs should also contact other competent authorities and financial institutions in order to obtain relevant information~~

INTERPRETATIVE NOTES ON THE SPECIAL RECOMMENDATIONS

Interpretative Note to SR II

Objectives

1. Special Recommendation II (SR II) was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and inter alia money laundering, another objective of SR II is to emphasise this link by obligating countries to include terrorist financing offences as predicate offences for money laundering. ~~The basis for criminalising terrorist financing should be the United Nations International Convention for the Suppression of the Financing of Terrorism, 1999.~~³¹

Definitions

~~2. For the purposes of SR II and this Interpretative Note, the following definitions apply:~~

- ~~a) The term funds refers to assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit.~~
- ~~b) The term terrorist refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.~~
- ~~e) The term terrorist act includes:
 - ~~i) An act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms~~~~

³¹ ~~Although the UN Convention had not yet come into force at the time that SR II was originally issued in October 2001 and thus is not cited in the SR itself the intent of the FATF has been from the issuance of SR II to reiterate and reinforce the criminalisation standard as set forth in the Convention (in particular, Article 2). The Convention came into force in April 2003.~~

Interpretative Notes - SRII

~~located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and~~

~~ii) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.~~

~~d) The term terrorist financing includes the financing of terrorist acts, and of terrorists and terrorist organisations.~~

~~e) The term terrorist organisation refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.~~

Characteristics of the Terrorist Financing Offence

3. Terrorist financing offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.

4. Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy does not comply with this Recommendation.

5. Terrorist financing offences should extend to any funds whether from a legitimate or illegitimate source.

6. Terrorist financing offences should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

7. It should also be an offence to attempt to commit the offence of terrorist financing.

8. It should also be an offence to engage in any of the following types of conduct:

- a) Participating as an accomplice in an offence as set forth in paragraphs 3 or 7 of this Interpretative Note;
- b) Organising or directing others to commit an offence as set forth in paragraphs 3 or 7 of this Interpretative Note;
- c) Contributing to the commission of one or more offence(s) as set forth in paragraphs 3 or 7 of this Interpretative Note by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.

Interpretative Notes - SRII

~~9. Terrorist financing offences should be predicate offences for money laundering.~~

10. Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

11. The law should permit the intentional element of the terrorist financing offence to be inferred from objective factual circumstances.

12. Criminal liability for terrorist financing should extend to legal persons. Where that is not possible (i.e. due to fundamental principles of domestic law), civil or administrative liability should apply.

13. Making legal persons subject to criminal liability for terrorist financing should not preclude the possibility of parallel criminal, civil or administrative proceedings in countries in which more than one form of liability is available.

14. Natural and legal persons should be subject to effective, proportionate and dissuasive criminal, civil or administrative sanctions for terrorist financing.

Interpretative Notes - SR III

Interpretative Note to SR.III: Freezing and Confiscating Terrorist Assets

(Replaces the current text of INSR.III)

I. OBJECTIVE

FATF Special Recommendation III requires each jurisdiction to implement targeted financial sanctions to comply with the United Nations Security Council Resolutions (UNSCRs) that require jurisdictions to freeze without delay the funds or other assets and to ensure that no funds and other assets are made available to or for the benefit of: (i) any person or entity designated by the United Nations Security Council (the Security Council) under Chapter VII of the *Charter of the United Nations*, as required by S/RES/1267(1999) and its successor resolutions³²; or (ii) any person or entity designated by that jurisdiction pursuant to S/RES/1373(2001).

It should be stressed that none of the obligations in Special Recommendation III is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by Recommendation 3 (provisional measures and confiscation)³³. Measures under Special Recommendation III may *complement* criminal proceedings against a designated person or entity, and be adopted by a competent authority or a court, but are not *conditional* upon the existence of such proceedings. Instead, the focus of Special Recommendation III is on the preventative measures that are necessary and unique in the context of stopping the flow or use of funds or other assets to terrorist groups. In determining the limits of or fostering widespread support for an effective counter-terrorist financing regime, jurisdictions must also respect human rights, respect the rule of law, and recognise the rights of innocent third parties.

II. DEFINITIONS

For the purposes of Special Recommendation III and this Interpretative Note, the following definitions apply:

- a) The term *designation* refers to the identification of a person or entity that is subject to targeted financial sanctions pursuant to S/RES/1267(1999) and its successor resolutions, and S/RES/1373(2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination.

³² This Interpretative Note is applicable to all current and future successor resolutions to S/RES/1267(1999) and any future UNSCRs which impose targeted financial sanctions in the terrorist financing context. At the time of issuance of this Interpretative Note, [INSERT DATE], the successor resolutions to S/RES/1267(1999) are: S/RES/1333(2000), S/RES/1363(2001), S/RES/1390(2002), S/RES/1452(2002), S/RES/1455(2003), S/RES/1526(2004), S/RES/1617(2005), S/RES/1730(2006), S/RES/1735(2006), S/RES/1822(2008), S/RES/1904(2009), S/RES/1988(2011), and S/RES/1989(2011).

³³ Based on requirements set, for instance, in the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)* and the *United Nations Convention against Transnational Organised Crime (2000)*, which contain obligations regarding freezing, seizure and confiscation in the context of combating transnational crime. Additionally, the *International Convention for the Suppression of the Financing of Terrorism (1999)* contains obligations regarding freezing, seizure and confiscation in the context of combating terrorist financing. Those obligations exist separately and apart from the obligations set forth in Special Recommendation III and the United Nations Security Council Resolutions related to terrorist financing.

Interpretative Notes - SRIII

- b) The term *designated person* refers to:
- (i) Individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267(1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida;
 - (ii) Individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988(2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; or
 - (iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to S/RES/1373(2001).
- c) The term *ex parte* means proceeding without prior notification and participation of the affected party.
- d) The term *freeze* means to prohibit the transfer, conversion, disposition or movement of any funds or other assets on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism. The frozen funds or other assets remain the property of the person(s) or entity(ies) that held an interest in them at the time of the freezing and may continue to be administered by third parties, or through other arrangements established by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the implementation of targeted financial sanctions, jurisdictions may decide to take control of the funds or other assets as a means to protect against flight.
- e) The term *funds or other assets* means any assets, including, but not limited to, financial assets, economic resources, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.
- f) For the purposes of SRIII, the term *supra-national jurisdiction* refers to the European Union.
- g) The term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
- h) The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts³⁴ by any means, directly or indirectly, unlawfully and wilfully; (ii) participates

³⁴ A *terrorist act* includes an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) *Convention for the Suppression of Unlawful Seizure of Aircraft* (1970); (ii) *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (1971); (iii) *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents* (1973); (iv) *International Convention against the Taking of Hostages* (1979); (v) *Convention on the Physical Protection of Nuclear Material* (1980); (vi) *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (1988); (vii) *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation* (1988);

Interpretative Notes - SRIII

as an accomplice in terrorist acts or terrorist financing; (iii) organises or directs others to commit terrorist acts or terrorist financing; or (iv) contributes to the commission of terrorist acts or terrorist financing by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or terrorist financing or with the knowledge of the intention of the group to commit a terrorist act or terrorist financing.

- i) The term *third parties* includes, but is not limited to, financial institutions and designated non-financial businesses and professions.
- j) The term *terrorist organisation* refers to any legal person, group, undertaking or other entity owned or controlled directly or indirectly by a terrorist(s), and persons and entities acting on behalf of or at the direction of such terrorist(s).
- k) The term *those who finance terrorism* refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts.
- l) The phrase *without delay*, for the purposes of S/RES/1267(1999) and its successor resolutions, means, ideally, within a matter of hours of a designation by the 1267 Committee or the 1988 Committee. For the purposes of S/RES/1373(2001), the phrase *without delay* means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase *without delay* should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, and those who finance terrorism, and the need for global, concerted action to interdict and disrupt their flow swiftly.

III. IDENTIFYING AND DESIGNATING PERSONS AND ENTITIES FINANCING OR SUPPORTING TERRORIST ACTIVITIES

For S/RES/1267(1999) and its successor resolutions, designations relating to Al-Qaida are made by the 1267 Committee, and designations pertaining to the Taliban and related threats to Afghanistan are made by the 1988 Committee, with both Committees acting under the authority of Chapter VII of the United Nations Charter. For S/RES/1373(2001), designations are made, at the national or supranational level, by a jurisdiction or jurisdictions acting on its own motion, or at the request of another jurisdiction, if the jurisdiction receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in S/RES/1373(2001) as set forth in Appendix 1.

Jurisdictions need to have the authority, and effective procedures or mechanisms to identify and initiate proposals for designations of persons and entities targeted by S/RES/1267(1999) and its successor

(viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999).

Interpretative Notes - SRIII

resolutions, consistent with the obligations set out in those UNSCRs³⁵. Such authority and procedures or mechanisms are essential to propose persons and entities to the Security Council for designation in accordance with Security Council list-based programs, pursuant to those UNSCRs. Jurisdictions also need to have the authority and effective procedures or mechanisms to identify and initiate designations of persons and entities pursuant to S/RES/1373(2001) consistent with the obligations set out in that UNSCR. Such authority and procedures or mechanisms are essential to identify persons and entities who meet the criteria identified in S/RES/1373(2001) described in Appendix 1³⁶. A jurisdiction's regime to implement S/RES/1267(1999) and its successor resolutions, and S/RES/1373(2001), should include the following necessary elements:

- (a) Jurisdictions should identify a competent authority or a court as having responsibility for:
 - (i) proposing to the 1267 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in S/RES/1989(2011) (on Al Qaida) and related resolutions if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria;
 - (ii) proposing to the 1988 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in S/RES/1988(2011) (on the Taliban and those associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan) and related resolutions if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria; and
 - (iii) designating persons or entities that meet the specific criteria for designation as set forth in S/RES/1373(2001), as put forward either on the jurisdiction's own motion or, after examining and giving effect to, if appropriate, the request of another jurisdiction, if the jurisdiction receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in S/RES/1373(2001) as set forth in Appendix 1.
- (b) Jurisdictions should have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in S/RES/1988(2011) and S/RES/1989(2011) and related resolutions, and S/RES/1373(2001) (see Appendix 1 for the specific designation criteria of relevant UNSCRs). This includes having authority and effective procedures or mechanisms to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions, pursuant to S/RES/1373(2001). To ensure that effective co-operation is developed among jurisdictions, jurisdictions should ensure that when receiving a request, they make a prompt determination whether they are satisfied according to applicable (supra-)national principles that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in S/RES/1373(2011) as set forth in Appendix 1.
- (c) 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 UNSCRs.

³⁵ The relevant UNSCRs do not require states to identify persons or entities and submit these to the relevant UN Committees, but to have the authority and effective procedures and mechanisms in place to be able to do so.

³⁶

Interpretative Notes - SRIII

- (d) When deciding whether or not to make a (proposal for) designation, jurisdictions should apply an evidentiary standard of proof of “reasonable grounds” or “reasonable basis”. For designations under S/RES/1373(2001), the competent authority of each jurisdiction will apply the legal standard of its own legal system regarding the kind and quantum of evidence for the determination that “reasonable grounds” or “reasonable basis” exist for a decision to designate an individual or entity and thus initiate an action under a freezing mechanism. This is the case irrespective of whether the proposed designation is being put forward on the relevant jurisdiction’s own motion or at the request of another jurisdiction. Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding.
- (e) When proposing names to the 1267 Committee for inclusion on the Al-Qaida Sanctions List, pursuant to S/RES/1267(1999) and its successor resolutions, jurisdictions should:
- (i) follow the procedures and standard forms for listing, as adopted by the 1267 Committee;
 - (ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice;
 - (iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Appendix 1 for the specific designation criteria of relevant UNSCRs); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently listed person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1267 Committee; and
 - (iv) specify whether their status as a designating state may be made known.
- (f) When proposing names to the 1988 Committee for inclusion on the Taliban Sanctions List, pursuant to S/RES/1988(2011) and its successor resolutions, jurisdictions should:
- (i) follow the procedures for listing, as adopted by the 1988 Committee;
 - (ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice; and
 - (iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant designation (see Appendix 1 for the specific designation criteria of relevant UNSCRs); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently listed person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1988 Committee.

Interpretative Notes - SRIII

- (g) When requesting another jurisdiction to give effect to the actions initiated under the freezing mechanisms which have been implemented pursuant to S/RES/1373(2001), the initiating jurisdiction 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 Appendix 1 for the specific designation criteria of relevant UNSCRs).
- (h) Jurisdictions should have procedures to be able to operate *ex parte* against a person or entity who has been identified and whose (proposal for) designation is being considered.

IV. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

There is an obligation for jurisdictions to implement targeted financial sanctions without delay against persons and entities designated by the 1267 Committee and 1988 Committee (in the case of S/RES/1267(1999) and its successor resolutions), when these Committees are acting under the authority of Chapter VII of the *United Nations Charter*. For S/RES/1373(2001), the obligation for jurisdictions to take freezing action and prohibit the dealing in funds or other assets of designated persons, without delay, is triggered by a designation at the (supra-)national level, as put forward either on the jurisdiction's own motion or at the request of another jurisdiction if the jurisdiction receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in S/RES/1373(2001) as set forth in Appendix 1.

Jurisdictions should establish the necessary legal authority and identify competent domestic authorities responsible for implementing and enforcing targeted financial sanctions in accordance with the following standards and procedures:

- (a) Jurisdictions³⁷ should require all natural and legal persons within the jurisdiction to freeze, without delay and without prior notice, the funds or other assets of persons and entities designated pursuant to S/RES/1267(1999) and its successor resolutions, or S/RES/1373(2001). This obligation should extend to: all funds or other assets that are owned or controlled by the designated person/entity, and not just those that can be tied to a particular terrorist act, plot or threat; those funds or other assets which are wholly or jointly owned or controlled, directly or indirectly, by designated persons/entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons/entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of such persons or entities.
- (b) Jurisdictions should prohibit their nationals, or any persons and entities within their jurisdiction, from making any funds or other assets, economic resources, or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons; entities owned or controlled, directly or indirectly, by designated persons; and persons and entities acting on behalf of or at the direction of designated persons.

³⁷ In the case of the European Union (EU), which is a supra-national jurisdiction, the EU law applies as follows. The assets of designated persons are frozen by the EU regulations and their amendments. EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

Interpretative Notes - SRIII

unless licensed, authorised or otherwise notified in accordance with the relevant UNSCRs (see Section V below).

- (c) Jurisdictions should have mechanisms for communicating designations to the financial sector and the designated non-financial businesses and professions (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.
- (d) Jurisdictions should require financial institutions and DNFBPs³⁸ to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions, and ensure that such information is effectively utilized by appropriate authorities.
- (e) Jurisdictions should adopt effective measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Special Recommendation III.

V. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

Jurisdictions 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 S/RES/1267 (1999) and its successor resolutions that, in the view of the jurisdiction, do not or no longer meet the criteria for designation. In the event that the 1267 Committee or 1988 Committee has delisted a person or entity, the obligation to freeze no longer exists. In the case of de-listing requests related to Al-Qaida, such procedures and criteria should be in accordance with procedures adopted by the 1267 Committee under S/RES/1730(2006), S/RES/1735(2006), S/RES/1822(2008), S/RES/1904(2009), S/RES/1989(2011), and any successor resolutions. In the case de-listing requests related to the Taliban and related threats to the peace, security and stability of Afghanistan, such procedures and criteria should be in accordance with procedures adopted by the 1988 Committee under S/RES/1730(2006), S/RES/1735(2006), S/RES/1822(2008), S/RES/1904(2009), S/RES/1988(2011), and any successor resolutions.

For persons and entities designated pursuant to S/RES/1373(2001), jurisdictions should have appropriate authorities and procedures or mechanisms to delist and unfreeze the funds or other assets of persons/entities that no longer meet the criteria for designation. Jurisdictions should also have procedures in place to allow, upon request, review of the designation decision before a court or other independent competent authority.

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

Where jurisdictions have determined that funds or other assets of persons designated by the Security Council or one of its relevant sanctions committees are necessary for basic expenses; for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, jurisdictions should authorise access to such funds or other assets in accordance with the procedures set out in S/RES/1452(2002) and any successor resolutions. On the same grounds, jurisdictions should authorise

³⁸ UNSCRs apply to all natural and legal persons within the jurisdictions.

Interpretative Notes - SRIII

access to funds or other assets, if freezing measures are applied to persons designated by a (supra-)national jurisdiction pursuant to S/RES/1373(2001) and as set out in S/RES/1963(2010).

Jurisdictions should provide for a mechanism through which a designated person can challenge their designation with a view to having it reviewed by a competent authority or a court. With respect to designations on the Al-Qaida Sanctions List, jurisdictions should inform listed persons of the availability of the Office of the Ombudsperson to accept de-listing petitions.

APPENDIX 1

The criteria for designation as specified in the relevant United Nations Security Council Resolutions are:

- (a) **S/RES/1267(1999), S/RES/1989(2011) and their successor resolutions³⁹:**
- (i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of Al-Qaida, or any cell, affiliate, splinter group or derivative thereof⁴⁰; or
 - (ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection (i), (ii), or (iii) of this subparagraph, or by persons acting on their behalf or at their direction.
- (b) **S/RES/1267(1999), S/RES/1988(2011) and their successor resolutions:**
- (i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of those designated and other individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan,; or
 - (ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection (i) or (ii) of this subparagraph, or by persons acting on their behalf or at their direction.
- (c) **S/RES/1373(2001):**
- (i) any person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts;
 - (ii) any entity owned or controlled, directly or indirectly, by any person or entity designated under subsection (i) of this subparagraph; or
 - (iii) any person or entity acting on behalf of, or at the direction of, any person or entity designated under subsection (i) of this subparagraph.

³⁹ This Interpretative Note is applicable to all current and future successor resolutions to S/RES/1267(1999). At the time of issuance of this Interpretative Note, [INSERT DATE], the successor resolutions to S/RES/1267(1999) are: S/RES/1333(2000), S/RES/1367(2001), S/RES/1390(2002), S/RES/1455(2003), S/RES/1526(2004), S/RES/1617(2005), S/RES/1735(2006), S/RES/1822(2008), S/RES/1904(2009), S/RES/1988(2011), and S/RES/1989(2011).

⁴⁰ OP2 of S/RES/1617 (2005) further defines the criteria for being “associated with” Al-Qaida or Usama bin Laden.

Interpretative Notes – SR.VI

Interpretative Note to SR.VI: Alternative Remittance

INSR.VI

General

1. Money or value transfer systems have shown themselves vulnerable to misuse for money laundering and terrorist financing purposes. The objective of Special Recommendation VI is to increase the transparency of payment flows by ensuring that jurisdictions impose consistent anti-money laundering and counter-terrorist financing measures on all forms of money/value transfer systems, particularly those traditionally operating outside the conventional financial sector and not currently subject to the FATF Recommendations. This Recommendation and Interpretative Note underscore the need to bring all money or value transfer services, whether formal or informal, within the ambit of certain minimum legal and regulatory requirements in accordance with the relevant FATF Recommendations.

2. Special Recommendation VI consists of three core elements:

- a) Jurisdictions should require licensing or registration of persons (natural or legal) that provide money/value transfer services, including through informal systems;
- b) Jurisdictions should ensure that money/value ~~transfer transmission~~ services, including informal systems (as described in paragraph 5 below), are subject to applicable FATF Forty Recommendations (2003) (in particular, Recommendations 4-16 and 21-25)⁴¹ and the ~~Eight-Nine~~ Special Recommendations (in particular SR VII); and
- c) Jurisdictions should be able to impose sanctions on money/value transfer services, including informal systems, that operate without a licence or registration and that fail to comply with relevant FATF Recommendations.

Scope and Application

~~3. For the purposes of this Recommendation, the following definitions are used.~~

~~4. Money or value transfer service refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment.~~

~~5. A money or value transfer service may be provided by persons (natural or legal) formally through the regulated financial system or informally through non-bank financial institutions or other business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system. In some jurisdictions, informal systems are frequently referred to as *alternative remittance services* or *underground (or parallel) banking systems*. Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include *hawala*, *hundi*, *fei chien*, and the *black market peso exchange*.⁴²~~

⁴¹ When this Interpretative Note was originally issued, these references were to the 1996 FATF Forty Recommendations. Subsequent to the publication of the revised FATF Forty Recommendations in June 2003, this text was updated accordingly. All references are now to the 2003 FATF Forty Recommendations.

⁴² The inclusion of these examples does not suggest that such systems are legal in any particular jurisdiction.

Interpretative Notes – SR.VI

~~6. Licensing means a requirement to obtain permission from a designated competent authority in order to operate a money/value transfer service legally.~~

~~7. Registration in this Recommendation means a requirement to register with or declare to a designated competent authority the existence of a money/value transfer service in order for the business to operate legally.~~

~~8. The obligation of licensing or registration applies to agents. At a minimum, the principal business must maintain a current list of agents which must be made available to the designated competent authority. An agent is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).~~

~~**Applicability of Special Recommendation VI**~~

~~9. Special Recommendation VI should apply to all natural or legal persons (natural or legal), which conduct for or on behalf of another natural or legal person (natural or legal) the types of activity described in paragraphs 4 and 5 above as a primary or substantial part of their business or when such activity is undertaken on a regular or recurring basis, including as an ancillary part of a separate business enterprise.~~

Licensing or Registration and Compliance

11. Jurisdictions should designate ~~an~~ a competent authority to grant licences and/or carry out registration and ensure that the requirement is observed. There should be ~~an~~ a competent authority responsible for ensuring compliance by money/value transfer services with the FATF Recommendations ~~(including the Eight Special Recommendations)~~. There should also be effective systems in place for monitoring and ensuring such compliance. ~~This interpretation of Special Recommendation VI (i.e., the need for designation of competent authorities) is consistent with FATF Recommendation 23.~~

8. An agent is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires). In relation to agents of money or value transfer service businesses, either:

(i) agents should be licensed or registered by the competent authority; or

(ii) the money or value transfer service business should maintain a current list of agents which should be accessible by the designated competent authorities of the home and host country.

10. Jurisdictions need not impose a separate licensing ~~or~~ registration system or designate another competent authority in respect to natural or legal persons ~~(natural or legal)~~ already licensed or registered as financial institutions (as defined by the FATF Forty Recommendations (2003)) within a particular jurisdiction, which under such license or registration are permitted to perform activities indicated in paragraphs 4 and 5 above and which are already subject to the full range of applicable obligations under the FATF ~~Forty~~ Recommendations. (2003) (in particular, Recommendations 4-16 and 21-25) and the Eight Special Recommendations (in particular SR VII).

Interpretative Notes – SR.VI

Sanctions

12. Persons providing money/value transfer services without a license or registration should be subject to ~~appropriate~~ effective, proportionate and dissuasive administrative, civil or criminal sanctions.⁴³ Licensed or registered money/value transfer services which fail to comply fully with the relevant measures called for in the FATF Forty Recommendations (2003) ~~or the Eight Special Recommendations~~ should also be subject to appropriate sanctions.

⁴³ Jurisdictions may authorise temporary or provisional operation of money / value transfer services that are already in existence at the time of implementing this Special Recommendation to permit such services to obtain a licence or to register.

Interpretative Notes – SR.VII

Interpretative Note to SR.VII: ~~Wire~~ Electronic Funds Transfers

(Replaces current text of the Interpretative Note to SRVII)

Objective

Special Recommendation VII (SRVII) was developed with the objective of preventing terrorists and other criminals from having unfettered access to electronic funds transfers (EFT) for moving their funds and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and recipient of EFT is immediately available:

- (a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;
- (b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and
- (c) to ordering, intermediary and receiving financial institutions (FI) to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated parties, as per the obligations which are set out in the relevant United Nations Security Council Resolutions (UNSCRs), such as S/RES/1267(1999) and its successor resolutions, and S/RES/1373(2001) relating to the prevention and suppression of terrorism and terrorist financing.

To accomplish these objectives, countries should have the ability to trace all EFT. Due to the potential terrorist financing threat posed by small EFT, countries should minimise thresholds taking into account the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system.

Definitions

For the purposes of this interpretative note, the following definitions apply.

- (a) The term *accurate* is used to describe information that has been verified for accuracy.
- (b) The term *cover payment* refers to an EFT that combines a payment message sent directly by the ordering FI to the receiving FI with the routing of the funding instruction (the cover) from the ordering FI to the receiving FI through one or more intermediary FIs.
- (c) The term *cross-border EFT* refers to any EFT where the ordering FI and receiving FI are located in different countries. This term also refers to any chain of EFT where at least one of the FI involved is located in a different country.
- (d) The term *domestic EFT* refers to any EFT where the ordering FI and receiving FI are located in the same country. This term therefore refers to any chain of EFT that takes place entirely within the borders of a single country, even though the system used to effect

Interpretative Notes – SR.VII

the EFT may be located in another country. The term also refers to any chain of EFT that takes place entirely within the borders of the European Economic Area (EEA)⁴⁴.

- (d) The term *electronic funds transfer* (EFT) refers to any transaction carried out on behalf of an originator through an FI by electronic means with a view to making an amount of funds available to a recipient person at a receiving FI, irrespective of whether the originator and the recipient are the same person.⁴⁵
- (e) The term *full* is used to describe a situation in which all elements of required information are present.
- (f) The term *intermediary FI* refers to an FI in a serial or cover payment chain that receives and transmits an EFT on behalf of the ordering FI and the receiving FI, or another intermediary FI.
- (g) The term *ordering FI* refers to the FI which initiates the EFT and transfers the funds upon receiving the request for an EFT on behalf of the originator.
- (h) The term *originator* refers to the account holder who allows the EFT from that account, or where there is no account, the person (natural or legal) or legal arrangement that places the payment order with the ordering FI to perform the EFT.
- (i) The term *qualifying EFT* means a cross-border EFT above any applicable threshold as described in paragraph 6.
- (j) The term *receiving*⁴⁶ FI refers to the FI which receives the EFT from the ordering FI directly or through an intermediary FI and makes the funds available to the recipient.
- (k) The term *recipient*⁹ refers to the person (natural or legal) or legal arrangement who is identified by the originator as the receiver of the requested EFT.
- (l) The term *serial payment* refers to a direct sequential chain of payment where the EFT and accompanying payment message travel together from the ordering FI to the receiving FI directly or through one or more intermediary FIs (e.g., correspondent banks).
- (m) The term *straight through processing* refers to payment transactions that are conducted electronically without the need for manual intervention.
- (n) The term *unique transaction reference number* refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used to effect the EFT.

⁴⁴ An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of SRVII compliance.

⁴⁵ It is understood that the settlement of EFT may happen under a net settlement arrangement. This interpretative note refers to information which must be included in instructions sent from an originating FI to a receiving FI, including through any intermediary FI, to enable disbursement of the funds to the recipient. Any net settlement between the FIs may be exempt under paragraph 6(b).

⁴⁶ The paper “*Due diligence and transparency regarding cover payment messages related to cross border wire transfers*” by the *Basel Committee on Banking Supervision* (May 2009) uses the terms “beneficiary” for “recipient” and “beneficiary financial institution” for “receiving financial institution”.

Interpretative Notes – SR.VII

Scope

Special Recommendation VII applies to cross-border EFT and domestic EFT, including serial payments, and cover payments.

SRVII is not intended to cover the following types of payments:

- (a) Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction. However, when credit or debit or prepaid cards are used as a payment system to effect an EFT, they are covered by SRVII, and the necessary information should be included in the message.
- (b) FI-to-FI transfers and settlements where both the originator person and the recipient person are FIs acting on their own behalf.
- (c) Settlement of securities or commodity transactions between a financial institution and a regulated stock, commodity or associated derivatives exchange regardless of whether the financial institution is acting as agent for the customer or not.

Countries may adopt a *de minimus* threshold for cross-border transfers (no higher than EUR 1,000 or USD 1,000) below which the following requirements should apply:

- (a) Countries should ensure that FIs include with such transfers: (i) the name of the originator; (ii) the name of the recipient; 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 FI should verify the information pertaining to its customer.
- (b) Countries may nevertheless require that incoming cross-border EFT below the threshold contain full and accurate originator information.

Cross-border qualifying EFT

Information accompanying all qualifying EFTs 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, national identity number, customer identification number, or date and place of birth;
- (d) the name of the recipient; and
- (e) the recipient 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.

Qualifying cross-border EFT should be accompanied by full and accurate originator information, and full recipient information. However, countries may permit FIs to substitute the address with a national identity number, customer identification number⁴⁷, or date and place of birth.

⁴⁷ The customer identification number refers to a number which uniquely identifies the originator to the originating FI and is a different number to the unique transaction reference number referred to in

Interpretative Notes – SR.VII

Where several individual cross-border EFT from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements of paragraphs 7, 8 and 9 in respect of originator information, provided they include the originator's account number or unique transaction reference number (as described in paragraph 8 above), and the batch file contains full and accurate originator information, and full recipient information, that is fully traceable within the recipient country.

Domestic EFT

Information accompanying domestic EFT should also include originator information as indicated for cross-border EFT, unless full information can be made available to the receiving FI and appropriate authorities by other means. In this latter case, the ordering FI 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 recipient.

The information should be made available by the ordering FI within three business days of receiving the request either from the receiving FI or from appropriate authorities. Law enforcement authorities should be able to compel immediate production of such information.

Responsibilities of ordering, intermediary and receiving FIs

Ordering FI

The ordering FI should ensure that qualifying EFT contain full and accurate originator information, and full recipient information.

The ordering FI should ensure that cross-border EFT below any applicable threshold contains the name of the originator and the name of the recipient and an account number for each, or a unique transaction reference number.

The ordering FI should maintain all originator and recipient information collected, in accordance with Recommendation 10.

The ordering FI should not be allowed to execute the EFT if it does not comply with the requirements specified under paragraph 7.

Intermediary FI

For cross-border EFT, FIs processing an intermediary element of such chains of EFT should ensure that all originator and recipient information that accompanies an EFT is retained with it.

Where technical limitations prevent the full originator or recipient information accompanying a cross-border EFT from remaining with a related domestic EFT, a record should be kept for at least five years by the receiving intermediary FI of all the information received from the ordering FI or another intermediary FI.

paragraph 8. The customer identification number must refer to a record held by the originating FI which contains at least one of the following: the customer address, a national identity number, or a date and place of birth.

Interpretative Notes – SR.VII

An intermediary FI should take reasonable measures to identify cross-border EFT which lack full originator information or full recipient information. Such measures should be consistent with straight-through processing.

An intermediary FI should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend EFT lacking full originator or full recipient information; and (ii) the appropriate follow-up action.

Receiving FI

A receiving FI should take reasonable measures to identify cross-border EFT which lack full originator or full recipient information. Such measures may include post event monitoring or real time monitoring where feasible.

For qualifying EFTs, a receiving FI should verify the identity of the recipient, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 10.

A receiving FI should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend EFT lacking full originator or full recipient information; and (ii) the appropriate follow-up action.

Money or value transfer service operators

Money or value transfer service (MVTs) providers should be required to comply with all of the relevant requirements of Special Recommendation VII in the jurisdictions in which they operate, directly or through their agents. In the case of a MVTs provider that controls both the ordering and the receiving side of an EFT, the MVTs provider:

- (a) should take into account all the information from both the ordering and receiving sides in order to determine whether an STR has to be filed; and
- (b) should file an STR in any jurisdiction affected by the suspicious EFT, and make relevant transaction information available to the FIU.

Interpretative Notes – SR.VIII

Interpretative Note to SR.VIII: Non-profit organisations

Introduction

1. Non-profit organisations (NPOs) play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The ongoing international campaign against terrorist financing has unfortunately demonstrated however that terrorists and terrorist organisations exploit the NPO sector to raise and move funds, provide logistical support, encourage terrorist recruitment or otherwise support terrorist organisations and operations. This misuse not only facilitates terrorist activity but also undermines donor confidence and jeopardises the very integrity of NPOs. Therefore, protecting the NPO sector from terrorist abuse is both a critical component of the global fight against terrorism and a necessary step to preserve the integrity of NPOs.

2. NPOs may be vulnerable to abuse by terrorists for a variety of reasons. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. Depending on the legal form of the NPO and the country, NPOs may often be subject to little or no governmental oversight (for example, registration, record keeping, reporting and monitoring), or few formalities may be required for their creation (for example, there may be no skills or starting capital required, no background checks necessary for employees). Terrorist organisations have taken advantage of these characteristics of NPOs to infiltrate the sector and misuse NPO funds and operations to cover for or support terrorist activity.

Objectives and General Principles

3. The objective of Special Recommendation VIII (SR VIII) is to ensure that NPOs are not misused by terrorist organisations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes but diverted for terrorist purposes. In this Interpretative Note, the approach taken to achieve this objective is based on the following general principles:

- a) Past and ongoing abuse of the NPO sector by terrorists and terrorist organisations requires countries to adopt measures both: (i) to protect the sector against such abuse, and (ii) to identify and take effective action against those NPOs that either are exploited by or actively support terrorists or terrorist organizations.
- b) Measures adopted by countries to protect the NPO sector from terrorist abuse should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote transparency and engender greater confidence in the sector, across the donor community and with the general public that charitable funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of transparency, integrity and public confidence in the management and functioning of all NPOs are integral to ensuring the sector cannot be misused for terrorist financing.
- c) Measures adopted by countries to identify and take effective action against NPOs that either are exploited by or actively support terrorists or terrorist organisations should aim to prevent and

Interpretative Notes – SR.VIII

prosecute as appropriate terrorist financing and other forms of terrorist support. Where NPOs suspected of or implicated in terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose should to the extent reasonably possible avoid any negative impact on innocent and legitimate beneficiaries of charitable activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by NPOs.

- d) Developing co-operative relationships among the public, private and NPO sector is critical to raising awareness and fostering capabilities to combat terrorist abuse within the sector. Countries should encourage the development of academic research on and information sharing in the NPO sector to address terrorist financing related issues.
- e) A targeted approach in dealing with the terrorist threat to the NPO sector is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be vulnerable to misuse by terrorists, the need to ensure that legitimate charitable activity continues to flourish and the limited resources and authorities available to combat terrorist financing in each jurisdiction.
- f) Flexibility in developing a national response to terrorist financing in the NPO sector is also essential in order to allow it to evolve over time as it faces the changing nature of the terrorist financing threat.

Definitions

4. For the purposes of SR VIII and this interpretative note, the following definitions apply:

- a) The term *non-profit organisation* or *NPO* refers to a legal entity or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works”.
- b) The terms *FIU*, *legal arrangement* and *legal person* are as defined by the FATF Forty Recommendations (2003) (*the FATF Recommendations*).
- c) The term *funds* is as defined by the Interpretative Note to FATF Special Recommendation II.
- d) The terms *freezing*, *terrorist* and *terrorist organisation* are as defined by the Interpretative Note to FATF Special Recommendation III.
- e) The term *appropriate authorities* refers to competent authorities, self-regulatory bodies, accrediting institutions and other administrative authorities.
- f) The term *beneficiaries* refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.

Measures

5. Countries should undertake domestic reviews of their NPO sector or have the capacity to obtain timely information on its activities, size and other relevant features. In undertaking these assessments, countries should use all available sources of information in order to identify features and types of NPOs,

Interpretative Notes – SR.VIII

which by virtue of their activities or characteristics, are at risk of being misused for terrorist financing.⁴⁸ Countries should also periodically reassess the sector by reviewing new information on the sector’s potential vulnerabilities to terrorist activities.

6. There is a diverse range of approaches in identifying, preventing and combating terrorist misuse of NPOs. An effective approach, however, is one that involves all four of the following elements: (a) Outreach to the sector, (b) Supervision or monitoring, (c) Effective investigation and information gathering and (d) Effective mechanisms for international co-operation. The following measures represent specific actions that countries should take with respect to each of these elements in order to protect their NPO sector from terrorist financing abuse.

a. Outreach to the NPO sector concerning terrorist financing issues

- (i) Countries should have clear policies to promote transparency, integrity and public confidence in the administration and management of all NPOs.
- (ii) Countries should encourage or undertake outreach programmes to raise awareness in the NPO sector about the vulnerabilities of NPOs to terrorist abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.
- (iii) Countries should work with the NPO sector to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect the sector from terrorist abuse.⁴⁹
- (iv) Countries should encourage NPOs to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns.

b. Supervision or monitoring of the NPO sector

Countries should take steps to promote effective supervision or monitoring of their NPO sector. In practice, countries should be able to demonstrate that the following standards apply to NPOs which account for (1) a significant portion of the financial resources under control of the sector; and (2) a substantial share of the sector’s international activities.

- (i) NPOs should maintain information on: (1) the purpose and objectives of their stated activities; and (2) the identity of the person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information should be publicly available either directly from the NPO or through ~~relevant appropriate~~ authorities.
- (ii) NPOs should issue annual financial statements that provide detailed breakdowns of incomes and expenditures.
- (iii) NPOs should be licensed or registered. This information should be available to competent authorities.⁵⁰
- (iv) NPOs should have appropriate controls in place to ensure that all funds are fully accounted for and are spent in a manner that is consistent with the purpose and objectives of the NPO’s stated activities.
- (v) NPOs should follow a “know your beneficiaries and associate NPOs⁵¹” rule, which means that the NPO should make best efforts to confirm the identity, credentials and good standing

⁴⁸ For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

⁴⁹ The FATF’s *Combating the Abuse of Non-Profit Organisations: International Best Practices* provides a useful reference document for such exercises.

⁵⁰ Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, NPOs are already registered with tax authorities and monitored in the context of qualifying for favourable tax treatment (such as tax credits or tax exemptions).

Interpretative Notes – SR.VIII

of their beneficiaries and associate NPOs. NPOs should also undertake best efforts to document the identity of their significant donors and to respect donor confidentiality.

- (vi) NPOs should maintain, for a period of at least five years, and make available to relevant appropriate authorities, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organisation. This also applies to information mentioned in paragraphs (i) and (ii) above.
- (vii) ~~Appropriate~~ Relevant authorities should monitor the compliance of NPOs with applicable rules and regulations.⁵² ~~Appropriate~~ Relevant authorities should be able to properly sanction relevant violations by NPOs or persons acting on behalf of these NPOs.⁵³

c. *Effective information gathering and investigation*

- (i) Countries should ensure effective co-operation, co-ordination and information sharing to the extent possible among all levels of relevant appropriate authorities or organisations that hold relevant information on NPOs.
- (ii) Countries should have investigative expertise and capability to examine those NPOs suspected of either being exploited by or actively supporting terrorist activity or terrorist organisations.
- (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 all relevant competent authorities in order to take preventative or investigative action.

d. *Effective capacity to respond to international requests for information about an NPO of concern*

Consistent with ~~Special Recommendation V~~ 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 other forms of terrorist support.

⁵¹ ~~The term *associate NPOs* includes foreign branches of international NPOs.~~

⁵² In this context, rules and regulations may include rules and standards applied by self regulatory bodies and accrediting institutions.

⁵³ The range of such sanctions might include freezing of accounts, removal of trustees, fines, de-certification, de-licensing and de-registration. This should not preclude parallel civil, administrative or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

Interpretative Notes – SR.IX

Interpretative Note to SR.IX: Cash Couriers

Objectives

1. FATF Special Recommendation IX was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures 1) to detect the physical cross-border transportation of currency and bearer negotiable instruments, 2) to stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, 3) to stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed, 4) to apply appropriate sanctions for making a false declaration or disclosure, and 5) to enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering. ~~Countries should implement Special Recommendation IX subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements in any way.~~

Definitions

2. For the purposes of Special Recommendation IX and this Interpretative Note, the following definitions apply.

3. The term *bearer negotiable instruments* includes monetary instruments in bearer form such as: travellers cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.⁵⁴

4. The term *currency* refers to banknotes and coins that are in circulation as a medium of exchange.

5. The term *physical cross-border transportation* refers to any in-bound or out-bound physical transportation of currency or bearer negotiable instruments from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency through containerised cargo or (3) the mailing of currency or bearer negotiable instruments by a natural or legal person.

6. The term *false declaration* refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.

7. The term *false disclosure* refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for

⁵⁴ For the purposes of this Interpretative Note, gold, precious metals and precious stones are not included despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. 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 co-operate with a view toward establishing the source, destination, and purpose of the movement of such items and toward the taking of appropriate action.

Interpretative Notes – SR.IX

in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.

8. When the term *related to terrorist financing or money laundering* is used to describe currency or bearer negotiable instruments, it refers to currency or bearer negotiable instruments that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

The types of systems that may be implemented to address the issue of cash couriers

9. Countries may meet their obligations under Special Recommendation IX and this Interpretative Note by implementing one of the following types of systems; however, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

Declaration system

10. All persons making a physical cross-border transportation of currency or bearer negotiable instruments, which are of a value exceeding a pre-set, maximum threshold of EUR/USD 15,000 are required to submit a truthful declaration to the designated competent authorities. Jurisdictions may opt among the following three different types of declaration system: i) a written declaration system for all travellers; ii) a written declaration system for those travellers carrying an amount of currency or BNI above a threshold; and iii) an oral declaration system. These three systems are described below in their pure form; however, it is not uncommon for jurisdictions to opt for a mixed system.

i) *Written declaration system for all travellers:* In this system, all travellers are required to complete a written declaration before entering the jurisdiction. This would include questions contained on common or customs declaration forms. In practice, travellers have to make a declaration whether or not they are carrying currency or BNI (e.g., ticking a “yes” or “no” box).

ii) *Written declaration system for travellers carrying amounts above a threshold:* In this system, all travellers carrying an amount of currency or BNI above a pre-set designated threshold are required to complete a written declaration form. In practice, the traveller is not required to fill out any forms if they are not carrying currency or BNI over the designated threshold.

iii) *Oral declaration system for all travellers:* In this system, all travellers are required to orally declare if they carry an amount of currency or BNI above a threshold. Usually, this is done at customs entry points by requiring travellers to choose between the “red channel” (goods to declare) and the “green channel” (nothing to declare). The choice of channel that the traveller makes is considered to be the oral declaration. In practice, travellers do not declare in writing, but are required to actively report to a customs official.

Disclosure system:

11. Jurisdictions may opt for a system whereby travelers are required to provide the authorities with appropriate information upon request. In such systems, there is no requirement for travellers to make an upfront written or oral declaration. In practice, travellers need to be required to give a truthful answer to competent authorities upon request.

~~a) Declaration system: All persons making a physical cross border transportation of currency or bearer negotiable instruments, which are of a value exceeding a pre set, maximum threshold of EUR/USD 15,000, are required to submit a truthful declaration to the designated competent~~

Interpretative Notes – SR.IX

~~authorities. Countries that implement a declaration system should ensure that the pre-set threshold is sufficiently low to meet the objectives of Special Recommendation IX.~~

- b) ~~Disclosure system: The key characteristics of a disclosure system are as follows. All persons making a physical cross border transportation of currency or bearer negotiable instruments are required to make a truthful disclosure to the designated competent authorities upon request. Countries that implement a disclosure system should ensure that the designated competent authorities should have the authority to can make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.~~

Additional elements applicable to both systems

10. Whichever system is implemented, countries should ensure that their system incorporates the following elements:

- a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and bearer negotiable instruments.
- b) 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 bearer negotiable instruments and their intended use.
- c) Information obtained through the declaration/disclosure process should be available to the financial intelligence unit (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.
- d) At the domestic level, countries should ensure that there is adequate co-ordination among customs, immigration and other related authorities on issues related to the implementation of Special Recommendation IX.
- e) In the following two cases, competent authorities should be able to stop or restrain cash or bearer negotiable instruments for a reasonable time in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.
- f) The declaration/disclosure system should allow for the greatest possible measure of international co-operation and assistance in accordance with Special Recommendation V and Recommendations 35 to 40. To facilitate such co-operation, in instances when: (i) a declaration or disclosure which exceeds the maximum threshold of EUR/USD 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 the appropriate authorities. At a minimum, this information will cover: (i) the amount of currency or bearer negotiable instruments declared / disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

Interpretative Notes – SR.IX

- g) Countries should implement Special Recommendation IX subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements in any way.

Sanctions

11. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or bearer negotiable instruments.

Authorities responsible for implementation of SR.IX should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

Interpretative Notes – SR.X

Interpretative Note to Special Recommendation X

I OBJECTIVE

FATF Special Recommendation X requires jurisdictions to implement targeted financial sanctions to comply with United Nations Security Council Resolutions (UNSCRs) that require jurisdictions to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available to and for the benefit of any person or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations pursuant to UNSCRs that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction.⁵⁵

It should be stressed that none of the requirements in Special Recommendation X is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by international treaties or UNSCRs relating to weapons of mass destruction non-proliferation⁵⁶. The focus of Special Recommendation X is on preventative measures that are necessary and unique in the context of stopping the flow or use of funds or other assets to proliferators or proliferation as required by the United Nations Security Council (the Security Council).

II DEFINITIONS

For the purposes of Special Recommendation X and this Interpretive Note, the following definitions apply:

- a) The term *designation* refers to the identification of an individual, group, undertaking or entity that is subject to targeted financial sanctions pursuant to S/RES/1718(2006) and its successor resolutions⁵⁷, and S/RES/1737(2006) and its successor resolutions⁵⁸, and any future UNSCRs which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction.
- b) The term *designated person* refers to:

⁵⁵ This Interpretative Note is applicable to all current UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future UNSCRs which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Interpretative Note, **[INSERT DATE]**, the UNSCRs applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: S/RES/1718(2006), S/RES/1737(2006), S/RES/1747(2007), S/RES/1803(2008), S/RES/1874(2009), and S/RES/1929(2010).

⁵⁶ Based on requirements set, for instance, in the *Nuclear Non-Proliferation Treaty*, the *Biological and Toxin Weapons Convention*, the *Chemical Weapons Convention*, and S/RES/1540(2004). Those obligations exist separately and apart from the obligations set forth in Special Recommendation X and its interpretative note.

⁵⁷ This Interpretative Note is applicable to all current and future successor resolutions to S/RES/1718(2006). At the time of issuance of this Interpretative Note, **[INSERT DATE]**, the successor resolutions to S/RES/1718(2006) are: S/RES/1874(2009).

⁵⁸ This Interpretative Note is applicable to all current and future successor resolutions to S/RES/1737(2006). At the time of issuance of this Interpretative Note, **[INSERT DATE]**, the successor resolutions to S/RES/1737(2006) are: S/RES/1747(2007), S/RES/1803(2008), and S/RES/1929(2010).

Interpretative Notes – SR.X

- (i) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to S/RES/1718(2008) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the Security Council Committee established pursuant to resolution 1718(2006) (the 1718 Sanctions Committee) pursuant to S/RES/1718(2006); and
- (ii) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to S/RES/1737(2006) and its successor resolutions by the Security Council in annexes to the relevant resolutions, or by the Security Council Committee established pursuant to paragraph 18 of resolution 1737(2006) (the 1737 Sanctions Committee) pursuant to S/RES/1737(2006) and its successor resolutions.
- c) The term *ex parte* means proceeding without prior notification and participation of the affected party.
- d) The term *freeze* means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons. The frozen funds or other assets remain the property of the person(s) or entity(ies) that held an interest in them at the time of the freezing and may continue to be administered by third parties⁵⁹ or through other arrangements established by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the implementation of targeted financial sanctions, jurisdictions may decide to take control of the funds or other assets as a means to protect against flight.
- e) For the purposes of SRX, the term *supra-national jurisdiction* refers to the European Union.
- f) The term *funds or other assets* means any assets, including, but not limited to, financial assets, economic resources, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.
- g) The term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
- h) The phrase *without delay* means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g., the 1718 Sanctions Committee or the 1737 Sanctions Committee). The phrase *without delay* should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

III DESIGNATIONS

Designations are made by the Security Council in annexes to the relevant resolutions, or by the Security Council Committees established pursuant to these resolutions. There is no specific obligation upon UN Member States to submit proposals for designations to the relevant Security Council Committees.

⁵⁹ The term third parties includes, but is not limited to, financial institutions and designated non-financial businesses and professions.

Interpretative Notes – SR.X

However, in practice, the Committees primarily depend upon requests for designation by Member States. S/RES/1718(2006) and S/RES/1737(2006) provide that the relevant Committees shall promulgate guidelines as may be necessary to facilitate the implementation of the measures imposed by these resolutions.

Jurisdictions could consider establishing the authority and effective procedures or mechanisms to propose persons and entities to the Security Council for designation in accordance with relevant UNSCRs which impose TFS in the context of the financing of proliferation of weapons of mass destruction. In this regard, jurisdictions could consider the following elements:

- (a) identifying a competent authority(ies), either executive or judicial, as having responsibility for:
 - (i) proposing to the 1718 Sanctions Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in S/RES/1718(2006) and its successor resolutions if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria; and
 - (ii) proposing to the 1737 Sanctions Committee, for designation as appropriate, persons or entities that meet the criteria for designation as set forth in S/RES/1737(2006) and its successor resolutions if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Appendix 1 for the specific designation criteria associated with relevant UNSCRs).
- (b) having a mechanism(s) for identifying targets for designation, based on the designation criteria set out in S/RES/1718(2006), S/RES/1737(2006), and their successor resolutions (see Appendix 1 for the specific designation criteria of relevant UNSCRs). Such procedures should ensure the determination, according to applicable (supra-)national principles, whether reasonable grounds or a reasonable basis exists to propose a designation.
- (c) having appropriate legal authority, 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 UNSCRs.
- (d) when deciding whether or not to propose a designation, taking into account the criteria in Appendix 1 of this interpretative note. For proposals of designations, the competent authority of each jurisdiction will apply the legal standard of its own legal system, taking into consideration human rights, respect for the rule of law, and in recognition of the rights of innocent third parties.
- (e) when proposing names to the 1718 Sanctions Committee, pursuant to S/RES/1718(2006) and its successor resolutions, or to the 1737 Sanctions Committee, pursuant to S/RES/1737(2006) and its successor resolutions, providing as much detail as possible on:
 - (i) the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and
 - (ii) specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Appendix 1 for the specific designation criteria of relevant UNSCRs).

Interpretative Notes – SR.X

- (f) having procedures to be able, where necessary, to operate *ex parte* against a person or entity who has been identified and whose proposal for designation is being considered.

IV FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

There is an obligation for jurisdictions to implement targeted financial sanctions without delay against persons and entities designated:

- (a) in the case of S/RES/1718(2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1718 Sanctions Committee of the Security Council; and
- (b) in the case of S/RES/1737(2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1737 Sanctions Committee of the Security Council,

when these Committees are acting under the authority of Chapter VII of the *United Nations Charter*.

Jurisdictions should establish the necessary legal authority and identify competent domestic authorities responsible for implementing and enforcing targeted financial sanctions in accordance with the following standards and procedures:

- (a) Jurisdictions⁶⁰ should require all natural and legal persons within the jurisdiction to freeze, without delay and without prior notice, the funds or other assets of persons and entities designated pursuant to S/RES/1718(2006) or S/RES/1737(2006) and their successor resolutions. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person/entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets which are wholly or jointly owned or controlled, directly or indirectly, by designated persons/entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons/entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of such persons or entities.
- (b) Jurisdictions should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of such persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant UNSCRs (see Section V below).
- (c) Jurisdictions should have mechanisms for communicating designations to financial institutions and designated non-financial businesses and professions (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.

⁶⁰ In the case of the European Union (EU), which is considered a supra-national jurisdiction under SRX by the FATF, the assets of designated persons are frozen under EU regulations (as amended). EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

Interpretative Notes – SR.X

- (d) Jurisdictions should require financial institutions and DNFBBs⁶¹ to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions, and ensure that such information is effectively utilized by appropriate authorities.
- (e) Jurisdictions should adopt effective measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Special Recommendation X.
- (f) Jurisdictions should adopt appropriate measures for monitoring and ensuring compliance by financial institutions and DNFBBs, with the relevant legislation, rules or regulations governing the obligations under Special Recommendation X. Failure to comply with such legislation, rules or regulations should be subject to civil, administrative or criminal sanctions.

V DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

Jurisdictions 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 S/RES/1718(2006), S/RES/1737(2006), and their successor resolutions, that, in the view of the jurisdiction, do not or no longer meet the criteria for designation. Once the relevant Sanctions Committee has delisted the person or entity, the obligation to freeze no longer exists. Such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the Security Council pursuant to S/RES/1730(2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution.

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

Where jurisdictions have determined that the exemption conditions set out in S/RES/1718(2006) and S/RES/1737(2006) are met, jurisdictions should authorise access to funds or other assets in accordance with the procedures set out therein.

Jurisdictions should permit the addition to the accounts frozen pursuant to S/RES/1718(2006) or S/RES/1737(2006) of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to be subject to these provisions and are frozen.

Freezing action taken pursuant to S/RES/1737(2006) shall not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that:

- (a) The relevant jurisdictions have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in the relevant UNSCR, and

⁶¹ UNSCRs apply to all natural and legal persons within the jurisdiction.

Interpretative Notes – SR.X

- (b) The relevant jurisdictions have determined that the payment is not directly or indirectly received by a person or entity designated pursuant to S/RES/1737(2006);
- (c) The relevant jurisdictions have submitted prior notification to the 1737 Sanctions Committee of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation.⁶²

APPENDIX 1

The criteria for designation as specified in the relevant United Nations Security Council Resolution are:

- (a) **S/RES/1718(2006):**
 - (i) Any person or entity engaged in DPRK’s nuclear-related, other WMD-related and ballistic missile-related programs;
 - (ii) Any person or entity providing support for DPRK’s nuclear-related, other WMD-related and ballistic missile-related programs, including through illicit means;
 - (iii) Any person or entity acting on behalf of or at the direction of any person or entity designated under subsection (i) or subsection (ii) of this subparagraph⁶³; or
 - (iv) Any legal person or entity owned or controlled, directly or indirectly, by any person or entity designated under subsection (i) or subsection (ii) of this subparagraph⁶⁴.
- (b) **S/RES/1737(2006), S/RES/1747(2007), S/RES/1803(2008) and S/RES/1929(2010)::**
 - (i) Any person or entity engaged in Iran’s proliferation sensitive nuclear activities or the development of nuclear weapon delivery systems;
 - (ii) Any person or entity directly associated with or providing support for Iran’s proliferation sensitive nuclear activities or the development of nuclear weapon delivery systems;
 - (iii) Any person or entity acting on behalf or at a direction of any person or entity in (i) and/or (ii), or by entities owned or controlled by them;
 - (iv) Any person or entity any person or entity acting on behalf or at the direction of the individuals and entities of the Islamic Revolutionary Guard Corps designated pursuant to S/RES/1929(2010);
 - (v) any person or entity acting on behalf or at the direction of the individuals and entities of the Islamic Republic of Iran Shipping Lines (IRISL) designated pursuant to S/RES/1929(2010);

⁶² In cases where the designated party is a financial institution, jurisdictions should consider the FATF guidance issued as an annex to *The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction*, adopted in September 2007.

⁶³ The funds or assets of these persons or entities are frozen regardless of whether they are specifically identified by the Committee.

⁶⁴ Ibid.

Interpretative Notes – SR.X

- (vi) any legal person or entity owned or controlled, including through illicit means, by the individuals and entities of the Islamic Revolutionary Guard Corps designated pursuant to S/RES/1929(2010)⁶⁵; or
- (vii) any person or entity determined by the United Nations Security Council or the Committee to have assisted designated persons or entities in evading sanction of, or in violating the provisions of, S/RES/1737(2006), S/RES/1747(2007), S/RES/1803(2008), or S/RES/1929(2010).

⁶⁵ Ibid.

Glossary

GLOSSARY

Terms	Definitions
<i>Accounts</i>	References to “accounts” should be read as including other similar business relationships between financial institutions and their customers.
<u><i>Agent (Rec.9)</i></u>	<u>For the purpose of R.9, an agent is any person who carries out AML/CFT requirements on behalf of and under the control of a financial institution. An agreement creating the relation between the agent and the financial institution may be express or implied, and both the agent and the financial institution may be either a natural or legal person (such as a corporation or partnership). The ultimate responsibility for carrying out the AML/CFT requirements remains with the financial institution having recourse to the agent.</u>
<i>Agent (SRVI)</i>	For the purposes of SRVI, an <i>agent</i> is any natural or legal person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).
<i>Appropriate authorities (SRVIII)</i>	<u>For the purpose of SRVIII, the term <i>appropriate authorities</i> refers to competent authorities, including accrediting institutions, and self-regulatory organisations. competent authorities, self-regulatory bodies, accrediting institutions and other administrative authorities.</u>
<i>Associate NPOs (SRVIII)</i>	The term <i>associate NPOs</i> includes foreign branches of international NPOs.
<i>Batch transfer (SRVII)</i>	<u>In the context of SRVII, a <i>batch transfer</i> is a transfer comprised of a number of individual <u>EFTs</u> wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.</u>
<i>Bearer negotiable instruments</i>	<i>Bearer negotiable instruments</i> includes monetary instruments in bearer form such as: travellers cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee’s name omitted.
<i>Bearer shares</i>	<i>Bearer shares</i> refers to negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate.
<i>Beneficial</i>	<i>Beneficial owner</i> refers to the natural person(s) who ultimately ⁶⁶ owns or controls a customer ⁶⁷ and/or the person on whose behalf a transaction is being conducted. It also

⁶⁶ Reference to “ultimately owns or controls” and “ultimate effective control” refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

⁶⁷ This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

Glossary

Terms	Definitions
<i>owner</i>	incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
<i>Beneficiary</i>	<p>For the purposes of Special Recommendation VIII, the term <i>beneficiaries</i> refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.</p> <p>For the purposes of the other FATF Recommendations, the term <i>beneficiary</i> is as follows. <u>In trust law, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. All trusts (other than charitable or statutory permitted non-charitable trusts) must have beneficiaries, who may include the settlor, and a maximum time, known as the perpetuity period, normally of 100 years. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period.</u></p> <p><u>A beneficiary under a life or other investment linked insurance policy is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy.</u></p>
<i>Beneficiary (SRVIII)</i>	For the purposes of SR VIII, the term <i>beneficiaries</i> refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.
<i>Competent authorities</i>	<p><i>Competent authorities</i> refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.</p> <p><u><i>Competent authorities</i> refers to all authorities concerned with combating money laundering and/or terrorist financing. In particular, this entails the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency; and authorities that have AML/CFT supervisory or oversight responsibilities for monitoring AML/CFT compliance by financial institutions and DNFBPs. SROs are not to be regarded as a competent authority.</u></p>
<i>Confiscation</i>	The term <i>confiscation</i> , which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. <u>Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.</u>

Glossary

Terms	Definitions
<i>Consider</i>	References in the Recommendations that require a country to <i>consider</i> taking particular measures means that the country should have made a proper consideration or assessment of whether to implement such measures.
<i>Core Principles</i>	<i>Core Principles</i> refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
<i>Correspondent banking</i>	<i>Correspondent banking</i> is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers of funds <u>EFTs</u> , cheque clearing, payable-through accounts and foreign exchange services.
<u><i>Counterparts</i></u>	<u>See definition of “foreign counterpart”.</u>
<i>Country</i>	All references in the FATF Recommendations and in this Methodology to <i>country</i> or <i>countries</i> apply equally to territories or jurisdictions ⁶⁸ .
<i>Cover Payment (SRVII)</i>	<u>In the context of SRVII , the term cover payment refers to a form of EFT combining a payment message directly sent, separately from the funds, by the ordering FI to the beneficiary FI and allowing the latter, if so decided, to credit the beneficiary’s account before reception of the funds, on the one hand, and the separate and indirect routing of the funds (the cover) from the former FI to the latter FI through one or more intermediary FIs, on the other hand.</u>
<u><i>Criminal activity</i></u>	<u><i>Criminal activity</i> refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in the country; or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1.</u>
<i>Cross-border EFT transfer (SR VII)</i>	<u>In the context of SRVII, Cross-border EFT transfer <u>wire transfer</u> means any <u>electronic funds transfer</u> wire transfer where the originator and beneficiary institutions are located in different <u>countries jurisdictions</u>. This term also refers to any chain of <u>EFTs</u> wire transfers that has at least one cross-border element.</u>
<i>Currency</i>	Currency refers to banknotes and coins that are in circulation as a medium of exchange.
<i>Designated categories of offences</i>	<i>Designated categories of offences</i> means: <ul style="list-style-type: none"> • participation in an organised criminal group and racketeering; • terrorism, including terrorist financing; • trafficking in human beings and migrant smuggling; • sexual exploitation, including sexual exploitation of children;

⁶⁸ See also the “Note to assessors” under C.VII.3 of the Methodology.

Glossary

Terms	Definitions
	<ul style="list-style-type: none"> • illicit trafficking in narcotic drugs and psychotropic substances; • illicit arms trafficking; • illicit trafficking in stolen and other goods; • corruption and bribery; • fraud; • counterfeiting currency; • counterfeiting and piracy of products; • environmental crime; • murder, grievous bodily injury; • kidnapping, illegal restraint and hostage-taking; • robbery or theft; • smuggling; <u>(including in relation to customs and excise duties and taxes);</u> • <u>tax crimes (related to direct taxes and indirect taxes);</u> • extortion; • forgery; • piracy; and • insider trading and market manipulation. <p>When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.</p>
<p><i>Designated non-financial businesses and professions</i></p>	<p><i>Designated non-financial businesses and professions</i> means:</p> <ol style="list-style-type: none"> a) Casinos (which also includes internet casinos). b) Real estate agents. c) Dealers in precious metals. d) Dealers in precious stones. e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to ‘internal’ professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering. f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties: <ul style="list-style-type: none"> • acting as a formation agent of legal persons; • acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; • providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; • acting as (or arranging for another person to act as) a trustee of an express trust <u>or performing the equivalent function for another form of legal arrangement;</u>

Glossary

Terms	Definitions
	<ul style="list-style-type: none"> acting as (or arranging for another person to act as) a nominee shareholder for another person.
<i>Designated person</i>	<p>The term <i>designated person</i> refers to those persons or entities designated by the Al-Qaida and Taliban Sanctions Committee pursuant to S/RES/1267(1999) or those persons or entities designated and accepted, as appropriate, by <u>countries jurisdictions</u> pursuant to S/RES/1373(2001).</p> <p><u>In the context of SRIII, the term <i>designated person</i> refers to:</u></p> <p><u>(i) any natural or legal person or entity designated by the Committee of the Security Council established pursuant to resolution 1267(1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida;</u></p> <p><u>(ii) any natural or legal person or entity designated by the Committee of the Security Council established pursuant to resolution 1988(2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; or</u></p> <p><u>(iii) any natural or legal person or entity designated by jurisdictions pursuant to S/RES/1373(2001).</u></p>
<i>Designated threshold</i>	<i>Designated threshold</i> refers to the amount set out in the Interpretative Notes <u>to the Forty Recommendations</u> .
<i>Domestic EFT (SR VII)</i>	<u>In the context of SRVII, the term domestic EFT refers to any EFT where the ordering FI and beneficiary FI are located in the same country. This term therefore refers to any chain of EFT that takes place entirely within the borders of a single country, even though the system used to effect the EFT may be located in another country. The term also refers to any chain of EFT that takes place entirely within the borders of the European Union (EU)</u>
<u><i>Electronic funds transfer</i></u>	<u>The term electronic funds transfer (EFT) refers to any transaction carried out on behalf of an originator through an FI by electronic means with a view to making an amount of money available to a beneficiary person at an FI. The originator and the beneficiary may be the same person.</u> ⁶⁹
<u><i>Enforceable means</i></u>	<u><i>Enforceable means</i> refers to regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued by a competent authority (e.g. a financial supervisory authority or any other competent authority) or an SRO using powers delegated by such an authority or provided directly by law. The sanctions for non-compliance should be effective, proportionate and dissuasive (see R.17).</u>

⁶⁹ It is understood that the settlement of EFT may happen under a net settlement arrangement. This interpretative note refers to information which must be included in instructions sent from an originating FI to a beneficiary FI, including through any intermediary FI, to enable disbursement of the funds to the beneficiary. Any net settlement between the FIs may be exempt under paragraph 13(b).

Glossary

Terms	Definitions
<i>Express trust</i>	<i>Express trust</i> refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).
<i>False declaration</i> (SR IX)	<i>False declaration</i> refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is required for submission asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
<i>False disclosure</i> (SR IX)	<i>False disclosure</i> refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for upon request in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.
<i>FATF Recommendations</i>	<i>The FATF Recommendations refers to the Forty Recommendations and to the Nine Special Recommendations on Terrorist Financing.</i>
<u><i>Financial group</i></u>	<u><i>Financial group means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.</i></u>
<i>Financial institutions</i>	<i>Financial institutions</i> ⁷⁰ means any natural or legal person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer: <ol style="list-style-type: none"> 1. Acceptance of deposits and other repayable funds from the public.⁷¹ 2. Lending.⁷² 3. Financial leasing.⁷³ 4. The transfer of money or value.⁷⁴ 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments.

⁷⁰ For the purposes of Special Recommendation VII, it is important to note that the term *financial institution* does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds.

⁷¹ This also captures private banking.

⁷² This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

⁷³ This does not extend to financial leasing arrangements in relation to consumer products.

⁷⁴ This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.

Glossary

Terms	Definitions
	<p>7. Trading in: (a) money market instruments (cheques, bills, CDs, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading.</p> <p>8. Participation in securities issues and the provision of financial services related to such issues.</p> <p>9. Individual and collective portfolio management.</p> <p>10. Safekeeping and administration of cash or liquid securities on behalf of other persons.</p> <p>11. Otherwise investing, administering or managing funds or money on behalf of other persons.</p> <p>12. Underwriting and placement of life insurance and other investment related insurance⁷⁵.</p> <p>13. Money and currency changing.</p> <p>When a financial activity (other than the transferring of money or value) is carried out by a natural or legal person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is low little risk of money laundering or terrorist financing activity occurring, a country may decide that the application of AML/CFT anti-money laundering measures is not necessary, either fully or partially.</p> <p>In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.</p>
<i>FIU</i>	FIU means financial intelligence unit.
<i>Foreign counterparts</i>	Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the cooperation which is sought, even where such foreign competent authorities have a different nature or status (e.g. depending on the country, AML/CFT supervision of certain financial sectors may be performed by a supervisor that also has prudential supervisory responsibilities or by a supervisory unit of the FIU).
<i>Freeze</i>	The term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism. The frozen funds or other assets remain the property of the natural or legal person(s) or entity(ies) that held an interest in them at the time of the freezing and may continue to be administered by third parties, or through other arrangements established by such natural or legal person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the

⁷⁵ This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

Glossary

Terms	Definitions
	<u>implementation of targeted financial sanctions, jurisdictions may decide to take control of the funds or other assets as a means to protect against flight or dissipation.</u>
<i>Fundamental principles of domestic law</i>	<p>This refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or expressed within a national Constitution or similar document, or through decisions of the highest level of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person’s right to effective protection by the courts.</p> <p><u>If an assessed country relies on fundamental principles of domestic law, whether for non-prosecution of self-laundering in the context of Recommendation 1, or failure to have corporate criminal liability under Recommendation 2, the assessors should ensure that (1) each case is reviewed on the basis of the legal system of the assessed country, even where that may appear contrary to other legal systems and principles; (2) the country clearly states the nature of the fundamental principle of domestic law upon which it relies, e.g. it suggests the <i>ne bis in idem</i> principle applies to prevent self laundering prosecutions; (3) the country sets out material to support its arguments e.g. provisions of the Constitution or case law from the highest court to show the existence of the fundamental principle; (4) the principle preventing prosecution of self-laundering is a fundamental principle (as defined), as opposed to legal tradition, judicial practice or a particular criminal law policy, wherever the principle is set out.</u></p>
<i>Funds</i>	Except in the case of Special Recommendation II, <i>funds</i> refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, <u>however acquired</u> , and legal documents or instruments <u>in any form, including electronic or digital</u> , evidencing title to, or interest in, such assets.
<i>Funds or other assets</i>	The term <i>funds or other assets</i> means <u>any</u> financial assets, <u>economic resources</u> , property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.
<i>Funds transfer</i>	The terms <i>funds transfer</i> refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.
<i>Identification data</i>	Reliable, independent source documents, data or information will be referred to as “identification data”.
<i>Intermediaries</i>	<i>Intermediaries</i> can be financial institutions, DNFBP or other reliable persons or businesses that meet Criteria 9.1 to 9.4.
<u><i>International</i></u>	<u>International organisations are entities established by formal political agreements</u>

Glossary

Terms	Definitions
<u>organisations</u>	<u>between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organizations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.</u>
<i>Investigations, prosecutions and related proceedings</i>	<i>Investigations, prosecutions and related proceedings</i> may be of a criminal, civil enforcement or administrative nature, and includes proceedings in relation to confiscation or provisional measures.
<i>Law or regulation</i>	<i>Law or regulation</i> refers to primary and secondary legislation, such as laws, decrees, implementing regulations or other similar requirements, issued or authorised by a legislative body, and which impose mandatory requirements with sanctions for non-compliance. The sanctions for non-compliance should be effective, proportionate and dissuasive. <u><i>Law</i> refers to any legislation issued or approved through a Parliamentary process or by such other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for non compliance. The sanctions for non compliance should be effective, proportionate and dissuasive (see R.17). The notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country.</u>
<i>Legal arrangements</i>	<i>Legal arrangements</i> refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.
<i>Legal persons</i>	<i>Legal persons</i> refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.
<i>Licensing (SRVI)</i>	For the purposes of SRVI only , <i>Licensing</i> means a requirement to obtain permission from a designated competent authority in order to operate a money/value transfer service legally.
<i>Money laundering (ML) offence</i>	References in this Methodology (except in R.1) to a <i>money laundering (ML) offence</i> refer not only to the primary offence or offences, but also to ancillary offences.
<i>Money or value transfer service (SRVI)</i>	<i>For the purpose of SR VI, Money or value transfer service</i> refers to a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such

Glossary

Terms	Definitions
	<p>services can involve one or more intermediaries and a third party final payment.</p> <p>A money or value transfer service may be provided by <u>natural or legal persons</u> formally through the regulated financial system or informally through non-bank financial institutions or other business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system. In some jurisdictions, informal systems are frequently referred to as <i>alternative remittance services</i> or <i>underground (or parallel) banking systems</i>. Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include <i>hawala</i>, <i>hundi</i>, <i>fei-chien</i>, and the <i>black market peso exchange</i>. (This definition is drawn from the Interpretative Note to SR.VI. It is used in the criteria under SR.VI.)</p>
<p><u><i>Non-conviction based confiscation</i></u> <u>(Rec.38)</u></p>	<p><u>For the purpose of Rec. 38, Non-conviction based confiscation means confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required. Countries need not have the authority to act on the basis of all such requests, but should be able to do so, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown.</u></p>
<p><i>Non-profit organisations</i></p>	<p>The term <i>non-profit organisation</i> or <i>NPO</i> refers to a legal <u>person entity</u> or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works”.</p>
<p><i>Originator</i> <i>(SR VII)</i></p>	<p>The <i>originator</i> is the account holder, or where there is no account, the <u>natural or legal person (natural or legal)</u> that places the order with the <u>ordering FI financial institution</u> to perform the <u>EFT-wire transfer</u>.</p>
<p><i>Other Enforceable means</i></p>	<p>Other enforceable means refers to guidelines, instructions or other documents or mechanisms that set out enforceable requirements with sanctions for non-compliance, and which are issued by a competent authority (e.g. a financial supervisory authority) or an SRO. The sanctions for non-compliance should be effective, proportionate and dissuasive.</p>
<p><i>Palermo Convention</i></p>	<p>The 2000 UN Convention against Transnational Organized Crime.</p>
<p><i>Payable-through accounts</i></p>	<p><i>Payable-through accounts</i> refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.</p>
<p><i>Physical cross-border transportation</i></p>	<p><i>Physical cross-border transportation</i> refers to any in-bound or out-bound physical transportation of currency or bearer negotiable instruments from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person’s accompanying luggage or vehicle; (2) shipment of currency through containerised cargo or (3) the mailing of currency or bearer negotiable instruments by a natural or legal person.</p>
<p><i>Politically Exposed</i></p>	<p><i>PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians,</i></p>

Glossary

Terms	Definitions
<i>Persons</i> ” (PEPs)	<p>senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.</p> <p>PEPs are individuals who are or have been entrusted with prominent public functions <u>either domestically or</u> by a foreign country or in an international organisation, for example Heads of State or of government, senior politician, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. <u>PEPs are also individuals who are or have been entrusted with prominent functions by an international organisation and are members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.</u> Foreign PEPs are those individuals who are or have been entrusted with prominent public functions by a foreign country, while domestic PEPs are those who are or have been entrusted domestically with such a function. Business relationships with family members or close associate of PEPs involve reputational risks similar to those with PEPs themselves. The definition <u>of PEPs</u> is not intended to cover middle ranking or more junior individuals in the foregoing categories.</p>
<i>Proceeds</i>	<i>Proceeds</i> refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
<i>Property</i>	<i>Property</i> means assets of every kind, whether corporeal or incorporeal, moveable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
<i>Registration</i> (SRVI)	For the purposes of SR VI, <i>Registration</i> means a requirement to register with or declare to a designated competent authority the existence of a money/value transfer service in order for the business to operate legally.
<i>Related to terrorist financing or money laundering</i>	When used to describe currency or bearer negotiable instruments, the term <i>Related to terrorist financing or money laundering</i> refers to currency or bearer negotiable instruments that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.
<i>Risk</i>	All references to <i>risk</i> in refer to the risk of money laundering and/or terrorist financing. <u>This term should be read in conjunction of the IN on the Risk-Based Approach in the IN to the 40 Recommendations.</u>
<i>Satisfied</i>	Where reference is made to a financial institution being <i>satisfied</i> as to a matter, that institution must be able to justify its assessment to competent authorities.
<i>Seize</i>	The term <i>seize</i> means to prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified funds or other assets. The seized funds or other assets remain the property of

Glossary

Terms	Definitions
	the <u>natural or legal</u> person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized funds or other assets.
<i>Self-regulatory organisation (SRO)</i>	A <i>SRO</i> is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members <u>from the professionals</u> , has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. For example, it would be normal for this body to enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.
<u><i>Serial Payment (SRVII)</i></u>	<u>For the purpose In the context of SRVII, the term serial payment refers to a direct sequential chain of payment where the EFT and accompanying payment message travel together from the ordering FI to the beneficiary FI directly or through one or more intermediary FIs (e.g., correspondent banks).</u>
<i>Settlor</i>	<i>Settlers</i> are <u>natural or legal</u> persons or companies who transfer ownership of their assets to trustees by means of a trust deed <u>or similar arrangement</u> . Where the trustees have some discretion as to the investment and distribution of the trusts assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.
<i>Shell bank</i>	<i>Shell bank</i> means a bank that has no physical presence in the country in which it is incorporated <u>and licensed</u> , and which is unaffiliated with a regulated financial <u>services group that is subject to effective consolidated supervision</u> . <u>Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.</u>
<i>Should</i>	For the purposes of assessing compliance with the FATF Recommendations, the word <i>should</i> has the same meaning as <i>must</i> .
<i>S/RES/1267(1999)</i>	The term <i>S/RES/1267(1999)</i> refers to <i>S/RES/1267(1999)</i> and its successor resolutions. When issued, <i>S/RES/1267(1999)</i> had a time limit of one year. A series of resolutions have been issued by the United Nations Security Council (UNSC) to extend and further refine provisions of <i>S/RES/1267(1999)</i> . By successor resolutions are meant those resolutions that extend and are directly related to the original resolution <i>S/RES/1267(1999)</i> . As of [...], these resolutions included <i>S/RES/1333(2000)</i> , <i>S/RES/1363(2001)</i> , <i>S/RES/1390(2002)</i> , <i>S/RES/1455(2003)</i> ; <i>S/RES/1526(2004)</i> ; <u><i>S/RES/1617(2005)</i>; <i>S/RES/1699(2006)</i>; <i>S/RES/1730(2006)</i> and <i>S/RES/1735(2006)</i>.</u>
<i>STR</i>	<i>STR</i> refers to suspicious transaction reports.
<u><i>Subsidiaries</i></u>	<u><i>Subsidiaries</i> refers to majority owned subsidiaries.</u>
<i>Supervisors</i>	<i>Supervisors</i> refers to the designated competent authorities responsible for ensuring compliance by financial institutions <u>and casinos</u> with requirements to combat money laundering and terrorist financing.

Glossary

Terms	Definitions
<i>Targeted financial sanctions</i>	<u>The term <i>targeted financial sanctions</i> means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.</u>
<i>Terrorist</i>	For purposes of SRIII, the term <i>terrorist</i> is as defined in the Interpretative Note of SRIII. Otherwise, it refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts <u>or terrorist financing</u> ; or (iv) contributes to the commission of terrorist acts <u>or terrorist financing</u> by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act <u>or terrorist financing</u> or with the knowledge of the intention of the group to commit a terrorist act <u>or terrorist financing</u> .
<i>Terrorist act</i>	A <i>terrorist act</i> includes: (i) An act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and (ii) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
<i>Terrorist financing (FT)</i>	<i>Terrorist financing (FT)</i> includes the financing of terrorist acts, and of terrorists and terrorist organisations.
<i>Terrorist Financing Convention</i>	The 1999 United Nations International Convention for the Suppression of the Financing of Terrorism
<i>Terrorist financing offence</i>	References in the Methodology (except in SR II) to a <i>terrorist financing (FT) offence</i> refer not only to the primary offence or offences, but also to ancillary offences.
<i>Terrorist organisation</i>	For purposes of SRIII, the term <i>terrorist organisation</i> <u>is as defined in the Interpretative Note of SRIII refers to any legal person, group, undertaking or other entity owned or controlled directly or indirectly by a terrorist(s).</u>

Glossary

Terms	Definitions
	Otherwise, it refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
<i>Third parties</i> (R.9)	<i>For the purposes of R.9</i> only , <i>third parties</i> means financial institutions or DNFBP that are supervised <u>or monitored</u> and that meet <u>the requirements under Rec.9. Criteria 9.1 to 9.4</u>
<i>Those who finance terrorism</i> (SR III)	For the purposes of SR III only , the phrase <i>those who finance terrorism</i> refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts.
<i>Transactions</i>	In the insurance sector, the word <i>transactions</i> should be understood to refer to the insurance product itself, the premium payment and the benefits. <u>For specific requirements with regard to record keeping of transactions in the insurance sector, see the IAIS Guidance Notes of January 2002.</u>
<i>Trustee</i>	<i>Trustees</i> , who may be paid professionals or companies or unpaid persons, hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor's trust deed, taking account of any letter of wishes. There may also be a protector, who may have power to veto the trustees' proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.
<i>Unique identifier</i> (SR VII)	For the purposes of Special Recommendation VII, a <i>unique identifier</i> refers to any unique combination of letters, numbers or symbols that refers to a specific originator.
<i>Vienna Convention</i>	The 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
<i>Wire transfer</i>	the term <i>wire transfer</i> refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.
<i>Without delay</i> (SR III)	<u>For the purposes of Special Recommendation III</u> , the phrase <i>without delay</i> has the following specific meaning. For the purposes of S/RES/1267(1999), it means, ideally, within a matter of hours of a designation by the Al-Qaida and Taliban Sanctions Committee. For the purposes of S/RES/1373(2001), the phrase <i>without delay</i> means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a

Glossary

Terms	Definitions
	<p>person or entity is a terrorist, one who finances terrorism or a terrorist organisation. The phrase <i>without delay</i> should be interpreted in the context of the need to prevent the flight or dissipation of terrorist-linked funds or other assets, and the need for global, concerted action to interdict and disrupt their flow swiftly.</p>