Financial Action Task Force Groupe d'action financière

FATF Guidance Document

International Best Practices

Detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments

19 February 2010

THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG

DETECTING AND PREVENTING THE ILLICIT CROSS-BORDER TRANSPORTATION OF CASH AND BEARER NEGOTIABLE INSTRUMENTS

INTERNATIONAL BEST PRACTICES

I. INTRODUCTION

1. FATF Special Recommendation IX (SR IX) requires jurisdictions to implement measures to detect and prevent the physical cross-border transportation of currency and bearer negotiable instruments, which is one of the main methods used to move illicit funds, launder money and finance terrorism.

2. Experience has shown that implementing SR IX can be challenging for jurisdictions. This is partly because the detailed requirements of SR IX all have to fully cover both incoming and outgoing cross-border transportations of currency and bearer negotiable instruments (BNI) by any of the following three methods of transportation: *i)* by cash couriers; *ii)* through the post; or *iii)* by containerised cargo. Non-implementation of any of these elements has a negative effect on the entire system.

3. This is a non-binding Best Practice Paper[1] that should be read in conjunction with the FATF standard on this issue which is comprised of SR IX and its Interpretative Note. This Best Practice Paper is based on the experience of jurisdictions with the implementation of SR IX. It does not cover all aspects of SR IX, but focuses on areas that have proven to be challenging for jurisdictions to implement and provides possible tested solutions (best practices).

4. The purpose of Special Recommendation IX is to ensure 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 BNI. For this purpose, certain requirements of SR IX (disclosure/declaration obligations) will apply to all physical cross-border transportations of currency and BNI that meet the applicable threshold requirements.

II. DEFINITIONS

5. For the purpose of this Best Practice Paper, the definitions set out in the Interpretative Note to SR IX apply[2]. In addition, the following definitions apply to this Best Practice Paper.

6. The term *cash couriers*[3] refers to the natural persons who physically transport currency and BNI on their person or accompanying luggage from one jurisdiction to another.

7. The term *declaration system* refers to a system whereby persons are required to pro-actively submit a truthful declaration to the designated competent authorities.

---

[1] This paper replaces FATF's Paper *Detecting and Protecting and Preventing the Cross-Border Transportation of Cash by Terrorists and other Criminals: International Best Practices*, dated 12 February 2005.

[2] The following terms are defined in the Interpretative Note to Special Recommendation IX: *bearer negotiable instruments*, *currency*, *physical cross-border transportation*, *false declaration*, and *false disclosure*.

[3] While SR IX is usually referred to as the Special Recommendation covering cash couriers, it also applies to bulk cash smuggling. The term *bulk cash smuggling* refers to the act of making a physical cross-border transportation of currency and BNI in large volumes where the currency/BNI is concealed in order to evade the reporting requirement, often using vehicles or containerised cargo or mail.

8. The term *disclosure system* refers to a system whereby persons are required to make a truthful disclosure to the designated competent authorities upon request.

9. The term *jurisdiction* includes references to supra-national jurisdictions, where appropriate.

10. The term *supra-national jurisdiction* refers to an autonomous entity with its own sovereign rights and legal order independent of its member states, to which both its member states and their nationals and residents are subject, and which includes binding and enforceable legislation on all member states regarding the obligatory declaration or disclosure of physical cross-border transportation of currency or bearer negotiable instruments, without prejudice to national legislation.

11. The term *threshold* refers to the maximum amount that may be carried or sent across borders without having to declare or disclose. This threshold cannot be higher than EUR/USD 15 000.

III. BASIC FEATURES OF A DECLARATION OR DISCLOSURE SYSTEM

12. Jurisdictions have three options for implementing SR IX: *i)* a declaration system; *ii)* a disclosure system; or *iii)* a mixed system. Jurisdictions do not need to choose between a declaration or disclosure system; a combination of both is also possible. Whatever system is chosen, a basic principle is that the measures should be implemented with a view to ensuring that legitimate activities are not unreasonably hindered or obstructed.

A. Declaration system

13. 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 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.

B. Disclosure system

14. Jurisdictions may opt for a system whereby travellers 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.

C. Best practices for any type of system

15. The following are best practices for jurisdictions, regardless of whether they have opted for a declaration, disclosure or mixed system.

16. Ensure that travellers are aware of their obligation to declare/disclose. Although every citizen/resident is assumed to be responsible for knowing and complying with the law, it is best practice for jurisdictions to make the declaration/disclosure requirements explicitly and clearly known to all travellers, especially at ports of entry and border crossings. This will enhance the overall effectiveness of the system, including the ability to successfully prosecute false declarations/disclosures[4] at a later stage. The following are some examples of how the requirements may be communicated to travellers.

a) Sufficient signs, advising travellers of the obligation to declare/disclose, are posted in highly visible places at all ports of entry and border crossings. Such signs:

   i) explain that both currency and BNI must be declared/disclosed;

   ii) describe how and when the declaration/disclosure is to be made (*e.g.* in an oral declaration system, such signs explain that, by choosing a particular channel—red or green—the traveller is making a declaration); and

   iii) set out the possible consequences (*e.g.* sanctions) for making a false declaration/disclosure.

b) Signs and declaration forms are readily available in all necessary languages. In particular, it is useful to ensure that signs and forms are translated in the official languages of the jurisdiction, and in the languages of those jurisdictions from where the majority of travellers are arriving. This will ensure that the obligation to declare/disclose is clearly communicated to the maximum number of travellers.

17. Take measures to facilitate the process of making a declaration/disclosure. The objective is to ensure that the system operates smoothly and travellers are not practically impeded from making a declaration/disclosure.

a) In a written declaration system, such measures may include:

---

[4] The definition of false declaration/disclosure in the Interpretative Note to Special Recommendation IX includes a failure to declare/disclose. See paragraph 6 and 7 of the Interpretative Note to Special Recommendation IX: *"The term false declaration/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 in the declaration/disclosure or otherwise requested by the authorities. This includes failing to make a declaration/disclosure as required."* Jurisdictions do not need to use the exact same terminology (*e.g.,* a jurisdiction could define a false declaration/disclosure as a failure to disclose, provided that they also ensure that the system covers a failure to declare/disclose, as is required by Special Recommendation IX).

i) requiring commercial carriers (*e.g.* airlines, passenger ships, bus operators) to give all passengers a declaration card for completion before arrival;

ii) having declaration forms and writing implements visible and readily available at all ports of entry and border crossings; and

iii) ensuring that declaration forms clearly state that travellers must declare both currency and BNI.

b) In an oral declaration system, such measures may include clearly labelling the channels from which the traveller must choose with an indication as to what the consequences of each choice are (*e.g.* labelling the red channel with "goods to declare" and labelling the green channel with "nothing to declare").

c) In a disclosure system, such measures may include ensuring that travellers are able to easily recognise the officials to whom they are required to make a disclosure upon request (*e.g.* by requiring customs authority officials to wear uniforms and having sufficient signs posted at their location).

18. Implement similar systems for both incoming and outgoing travellers. A harmonised approach is easier to implement because the staff of the relevant authorities only need to be trained on one system. However, it should be noted that it is common for jurisdictions to have in place a declaration system for incoming travellers and a disclosure system for outgoing travellers.

19. Where compatible with existing legal frameworks, a declaration system may be supplemented by a disclosure requirement to deal with those travellers who make a false declaration, with a view to ascertaining whether the false declaration was intentional or not.

20. Integrate the declaration/disclosure system with existing processes and mechanisms. For instance, declaration or disclosure systems may be based on and coexist (either separately or in a combined system) with existing currency control mechanisms and/or customs declaration requirements for goods other than currency/BNI. In such circumstances, it is important to ensure that the staff of the authority(ies) responsible for enforcing them are made aware of each system's respective characteristics, differences, objectives and rationales. Such awareness raising and training helps to ensure that the implementation of the declaration/disclosure system is not impeded by the implementation of a concurrent system of currency controls or customs declarations. Another useful practice is to integrate the practical implementation of concurrent systems, as they relate to the traveller, with a view to streamlining processes, and reducing the burden on both travellers and the authorities. For instance, where compatible with existing legal framework and work streams, this could be accomplished by using a common declaration form that covers the requirement to declare currency/BNI and the requirement to declare goods.

21. Ensure that the statistics collected make a distinction, where applicable, between professional currency transportations (*i.e.* by and between regulated and supervised financial institutions) and other (common) transportations of currency and BNI.

IV. RECORD KEEPING AND INFORMATION SHARING

22. SR IX requires jurisdictions to collect, record and share information. Declaration and disclosure systems both require travellers to provide information that jurisdictions are required to record and share,

where appropriate. In all cases, jurisdictions need to ensure that there is a proper legal basis for collecting and sharing such information.

A. Record keeping

23. The choice of system (declaration or disclosure) has an effect on the amount and type of information collected. At the initial stage (*i.e.* at first contact with the competent authorities before any suspicion arises), written declaration systems usually collect basic information, but from all travellers. Oral declaration systems tend to collect basic written information from few travellers (those that declare to be in the possession of currency/BNI), but not from those travellers who do not declare. Disclosure systems initially only collect information from travellers that are requested to disclose; however, such disclosures are usually oral and not recorded. At the second stage (*i.e.* in case a false declaration/disclosure is suspected or detected), all systems tend to collect and record the same amount of data (including seizure records), which is usually more detailed, resembling a *procès-verbal*. In any case, data that is not collected cannot be recorded, maintained or shared.

24. Collecting information serves four purposes. On the level of the individual traveller, the data can be used as a starting point for a case file. At the administrative or law enforcement/prosecutorial level, the data can serve as input for other cases and/or the analysis work of financial intelligence units (FIUs). For jurisdictions, the data can be used to detect trends which may assist in knowing where to allocate scarce resources in the most effective manner and red flags which may be used to train competent authorities. Trends and red flags can also be used for expert witness and evidence programmes. On the international level, the data can be used to assist other jurisdictions.

25. It is best practice to implement a system that collects all of the necessary data, without overburdening or overwhelming travellers and the competent authorities. This can be accomplished by tailoring the amount of information collected to the severity of the situation, and focusing on key information that is known to be relevant to the circumstances.

26. For example, at a minimum, this includes, at the initial contact, collecting the following information from each traveller who is required to declare/disclose: *i)* name; *ii)* date and place of birth; *iii)* identification document (number); *iv)* declared/disclosed amount and type (name and country) of currency and BNI; and *v)* nationality. Further, where appropriate and in some cases, depending of the stage of the process, this could also include collecting *vi)* home address and visiting address; *vii)* occupation; *viii)* purpose of the travel; *ix)* port/place of departure; *x)* jurisdictions visited between departure and arrival; and *xi)* mode of transport and vessel or vehicle identification number.

27. For travellers who declare/disclose currency or BNI, it is also important to collect the following additional information: *i)* the (beneficial) owner of the currency/BNI; *ii)* the intended recipient of the currency/BNI; *iii)* the provenance (origin/source) and intended use of the currency/BNI; *iv)* the transport route; and *v)* the means of transport.

28. Finally, in cases where a traveller has made a false declaration/disclosure, or where a suspicion of money laundering (ML) or terrorist financing (FT) arises, any information necessary to investigate and prosecute should be collected.

29. It is best practice for jurisdictions to periodically review the information being collected with a view to ensuring that only relevant data is being gathered, consistent with the above principles. Implementation will be enhanced by using available information that has already been collected (*e.g.* through the use of advanced passenger information systems), rather than asking travellers and/or third parties to provide the same information twice.

30. The information that is collected also needs to be recorded. It is best practice to enter all data/records into secured electronic databases—preferably a single database.

B. Information sharing

31. SR IX requires sharing of information with the FIU, other domestic partners and international counterparts, subject to strict safeguards to ensure proper use of the data. It is best practice to set out such safeguards in law and co-operation agreements such as memorandums of understanding (MOUs). An additional recommended safeguard is ensuring that electronic databases automatically disable unauthorised access and sharing of data. It should be noted that information sharing and feedback among the FIU and other domestic partners and international counterparts can considerably improve the targeting of illicit cash couriers.

32. There are a number of different ways to share data domestically with the FIU, for example: *i)* the data is entered into a customs database and the FIU is given access to the information; *ii)* the data is entered into a customs database, copied to the FIU, and then entered into the FIU database; or *iii)* the data is handed over to the FIU and entered into the FIU database. It is most efficient to use only one database and give customs authorities and the FIU direct access to relevant data.

33. Regardless of how information is shared between the customs authorities and the FIU, it is best practice to ensure that: the information being shared is comprehensive, tailored to the needs of the FIU and law enforcement authorities, and includes all recorded data; and the sharing is made in a timely fashion (preferably in real time). SR IX requires jurisdictions to (immediately) inform the FIU of suspicious cross-border transportations incidents, or ensure that the FIU has access to information on all cross-border transportations of currency/BNI. When determining which approach to use, the following factors are relevant for the jurisdiction's consideration: *i)* the overall volume of cross-border transportations of currency/BNI; *ii)* the usefulness of providing the FIU with a comprehensive overview of all such transportations; *iii)* and the relative capacity and resources of the FIU to handle reports. The objective is to ensure that the FIU has all of the information needed to effectively perform its functions, without being swamped by information that it does not have adequate capacity and resources to manage.

34. Sharing information with other domestic partners is equally important. In particular, it is best practice to ensure that the customs authorities co-operate and co-ordinate closely with law enforcement authorities, including being able to share information. Such co-operation may include conducting joint investigations where the custom authority is a law enforcement entity.

35. SRIX requires there to be adequate domestic co-ordination among customs, immigration and other related authorities on issues related to the implementation of SRIX. Immigration authorities and border authorities are usually located in the vicinity of customs authorities. It is best practice for customs authorities and immigration to co-ordinate and co-operate on the basis of a protocol. Where the custom authorities lack law enforcement powers, co-operation with immigration, border guard or law enforcement authorities to transfer information on possible ML/FT cases is especially important to ensure swift follow-up. It is also international best practice to create working groups consisting of all relevant authorities located at the border.

36. International co-operation is pivotal to a successful fight against cash couriers. The FIU and customs authorities are already required, under FATF Recommendation 40, to provide the widest possible assistance to counterparts in other jurisdictions. Jurisdictions are required to implement clear and effective gateways, mechanisms or channels to facilitate such co-operation. In this area, structural co-operation agreements (such as MOUs or Customs Mutual Assistance Agreements (CMAAs)) are particularly useful since the authorities of some jurisdictions are not authorised to share information in the absence of such an

agreement. It is also important to ensure that the customs authorities and the FIU have access to and contact with their overseas counterparts on short notice when necessary, on a case-by-case basis. Such contact is facilitated by ensuring that the competent authorities distribute the contact information of overseas counterparts within their organisations. It is also a best practice to ensure that the staff of the customs authorities know what information can be shared directly with which of their foreign counterparts.

37. International co-operation is usually demand driven and, since incoming travellers always arrive from somewhere, it is important that destination jurisdictions and jurisdictions of origin share information, both spontaneously and upon request, in relation to cross-border transportations of currency/BNI. In particular, since one jurisdiction's outgoing traveller will be another jurisdiction's incoming traveller, it is best practice for the competent authorities to inform their overseas counterparts, in a proactive manner, of travellers who are known to be carrying significant amounts of currency/BNI and who are on their way to the other jurisdiction, especially where there is insufficient suspicion to restrain the currency/BNI or detain the traveller. Likewise, when a traveller arrives from an overseas jurisdiction with a significant amount of currency/BNI, it is also best practice to proactively inform overseas counterparts of the jurisdiction from where the traveller departed, given the practical challenges of monitoring outbound currency/BNI flows.

V. PRE-INTERDICTION EFFORTS: IDENTIFICATION AND TARGETING

38. Measures to detect false declarations, false disclosures and possible cases of ML/FT are an important element of an effective system to deter ML/FT through the use of cash couriers. Key features of any such pre-interdiction measures are co-ordination and feedback. To this end, the establishment of task forces, working groups and interagency agreements on protocols are recommended.

A. Measures to detect false declarations and disclosures

39. To enhance their ability to detect false declarations/disclosures and possible ML/FT, jurisdictions need to: *i)* use risk assessments; *ii)* know or predict who is travelling; *iii)* know what to look for; and *iv)* co-operate with their counterparts.

i) Use of risk assessments

40. Jurisdictions are encouraged to base targeting efforts upon intelligence and analysis together with risk and threat assessments. Authorities must first identify travel routes, flights, ships and concealment methods that are considered high-risk. Detection methods should be focused on key transit, destination and source jurisdictions, and the authorities in these jurisdictions should co-ordinate activities, intelligence and information on targeted carriers or individuals. Access to the information described in section IV.A of this paper, intelligence reports, seizure analysis and historical data, both domestically and internationally, is essential in identifying trends used by cash smugglers. Risk assessments should also take into account weaknesses and other vulnerabilities that have an impact, either directly or indirectly, on the financial infrastructure of the jurisdiction. The assessment should therefore take into account the size and scope of a jurisdiction's financial infrastructure, its laws, policies and financial reporting requirements.

ii) The traveller

41. To plan an efficient deployment of scarce resources, jurisdictions need to map traveller streams and know what kinds of travellers are most likely to arrive from what port of origin or depart to what destination. This knowledge needs to be constantly kept up-to-date.

42. On the level of a customs region (covering a certain area) or a customs post (covering a certain port of entry), authorities need to be kept up-to-date with information on expected aggregated traveller

trends. Targeting passengers for examination on the basis of race, religion or ethnicity should be strictly prohibited. In practice, streams of travellers may be anticipated on the basis of the timetables of commercial carriers or schedules of events with cross-border relevance (*e.g.* bilateral or multi-national sporting events).

43. Additionally, advanced passenger information systems hold data on passengers and are generally used by the immigration authorities. The relevant information from these systems can also usefully enhance the ability of the customs authorities to make quality risk assessments and take targeted actions. Examples of such systems include: *i)* full ("master") or limited ("slave") passenger name records (PNR); *ii)* the passenger manifest (PAX); and *iii)* industry systems such as the global distribution systems (GDSs) or computer reservation systems (GDSs), airline reservation systems (ARSs), departure control systems (DCSs) and airline frequent flyer systems (AFFSs). It is a best practice for the customs authorities to have appropriate access to relevant advanced passenger information systems. The extent to which such access may be appropriate will depend on the level of ML/FT risk and the application of data protection or privacy laws. Where the customs authorities cannot be given direct access to these systems, one possibility would be for other competent authorities who do have access to such data to furnish the customs authorities with relevant data or targeted warnings, as appropriate.

44. Access to advanced passenger systems enables customs authorities to target risk and focus on high risk travellers. That should lower the burden of targeted controls on bona fide travellers who will be checked less often. However, the use of advanced passenger systems is never a substitute or restriction for other targeted checks, such as those based on red flags or typologies.

iii) Currency/BNI

45. To establish a false declaration/disclosure, the competent authorities need to establish the amount of currency/BNI that the traveller is carrying.

46. At the border, the following best practices facilitate the capacity of jurisdictions to detect currency and BNI: *i)* use of animal units (such as canine units), x-rays and other detection equipment, all of which may be used in accordance with a risk-based targeted approach; *ii)* use of at-random selection mechanisms to select travellers for search; ; *iii)* use of field interviews on those individuals who merit further examination; *iv)* the preparation and official endorsement of an comprehensive guide that would provide an example of types of BNI (domestic and, to the extent possible, foreign) with its definition, use and characteristics (i.e. security features) as well as possible scenarios where a BNI would become subject to a declaration/disclosure; and *v)* availability of information (databases) on persons of interest other than those from advanced passenger information systems. Persons of interest could be those with relevant criminal records (such as ML/FT and other crimes that generate proceeds) and those subject to targeted sanctions (such as the regimes linked to United Nations Security Council Resolutions 1267 and 1373).

iv) Co-operation

47. Custom officials located at busy ports of entry and border crossings usually only have a short period of time in which they may interact with an individual traveller, and decide whether to take further action or allow the traveller to proceed. Pre-interdiction operations can assist custom officials by enabling them to target suspected travellers long before they actually approach or cross the border. Pre-interdiction operations can take a variety of forms, and may target both individual travellers and criminal networks. A common and indispensible feature of all pre-interdiction operations is close co-operation at the domestic, supranational and international levels.

48. *At the domestic level*, interagency co-operation protocols can be developed. These protocols are based on the normal flow of cases to make them easier to implement. Protocols to be used by customs authorities in the field need to be practical, easy to follow (*i.e.* not legal documents), and designed to ensure that, when followed, all applicable legal provisions are respected. Where more than one authority would be competent to handle cases, it is useful to ensure that protocols contain de-conflicting measures. Such measures are also useful at the supranational level.

49. *At the supranational level*, it is useful to implement measures, such as those described for the domestic context, that facilitate co-operation and co-ordination and apply to the relevant competent authorities of all jurisdictions that belong to the supranational entity. In this context, as best practices are considered the setting up of a working group, or holding meetings with all jurisdictional members of the supranational jurisdiction in order to network, harmonise and monitor procedures, exchange best practices and ensure the exchange of information and the setting up of common targeting actions. Common guidelines, analysis at the supra-national level of the cash declarations/disclosures gathered and of the control results achieved, mutual working visits and common databases to exchange targeting and other relevant cash related data are further best practices.

50. *At the international level*, day-to-day co-operation is enhanced by the formation of integrated border enforcement teams that combine the intelligence and law enforcement expertise of competent authorities from both sides of the border. Additionally, international co-operation to target currency smuggling builds on existing frameworks for international customs co-operation, such as the World Customs Organisation (WCO) and related (regional) entities. It is also a best practice for jurisdictions to engage in global or regional multi-lateral enforcement actions that target currency smuggling. These actions which take place during a fixed period allow jurisdictions to share real-time intelligence and information on cash declarations/disclosures. Jurisdictions can facilitate such efforts by engaging in co-operation through international law enforcement organisations such as INTERPOL. These international efforts also provide an opportunity to share expertise and training techniques on the detection, interdiction and investigation of cash smuggling.

51. Proactive contact with foreign counterparts is a powerful tool in detecting ML/FT, particularly in circumstances where there are suspicions which are not sufficient to justify restraining the currency/BNI involved or detaining the traveller. Customs authorities should appoint a national contact person to facilitate the exchange of information with international counterparts or utilise existing law enforcement attaches in the originating or destination country. By contacting the authorities of the jurisdiction from where the traveller originated, the information provided by the traveller may be cross-checked to determine whether there are any suspicious inconsistencies (*e.g.* different reasons are given for carrying a large amount of currency/BNI). Where suspicions remain even after inquiries are made, but restraint or detention still cannot be justified, it is useful to forewarn or simply inform (depending on the nature of the message) the authorities of the destination jurisdiction of the traveller about the grounds for suspicion and any details of the traveller's imminent arrival. This gives the authorities of the destination jurisdiction the opportunity to reassess the traveller, with a view to determining whether sufficient grounds for restraint or detention are now made out.

B. Measures to detect ML/FT

52. ML/FT cases can follow equally from truthful declarations/disclosures or false declarations/disclosures. In developing measures to detect and prevent the illicit cross-border transportation of cash and bearer negotiable instruments for terrorist financing or money laundering purposes, it is critical that countries conduct interdiction operations to disrupt this criminal activity. The identification and targeting techniques described in the previous sub-section of this paper are equally applicable for this purpose. The risk-assessments noted above should be based on methods and source and

destination jurisdictions with known or possible links to terrorist financing or other illicit finance movement.

53. The obvious first step for all jurisdictions is to ensure that customs staff and the staff of other competent authorities know what ML and FT are. To raise their awareness, it is a best practice to provide staff with sufficient training and equip them with simplified information cards that describe: *i)* the relevance and reason for having a declaration/disclosure system in place; *ii)* the relevant legal framework, including the criminalisation of ML/FT; *iii)* an overview of red flags and typologies; and *iv)* directions on next steps in cases were ML/FT is suspected. It is important that all staff be made aware that ML/FT may occur even in circumstances where a truthful declaration/disclosure of currency/BNI has been made. The creation and dissemination of recurring intelligence bulletins, circulars or newsletters that contain tactical and operational information on cash smuggling help raise awareness to operational staff and managers. These circulars are often helpful in identifying cash smuggling techniques which are often similar to drug smuggling techniques that authorities may be accustomed to seeing.

54. Further, it is best practice is to ensure that all relevant authorities, financial institutions and designated non-financial businesses and professions are aware that a declaration/disclosure does not constitute an AML/CFT clearance form or any other endorsement by the government that the underlying currency/BNI are legitimate. The existence of a declaration/disclosure is not a substitute for financial institutions and other obliged institutions to verify the source of funds or conduct regular or enhanced ongoing due diligence, nor is a declaration/disclosure a ground for financial institutions and other obliged institutions to apply simplified or reduced due diligence. Regulatory guidance issued by the relevant supervisory authorities is a useful way to reinforce awareness of these issues.

C. Restraint/Confiscation of currency

55. When a false declaration or false disclosure occurs, or when there are reasonable grounds for suspicion of money laundering or terrorist financing, countries are encouraged to consider imposing a reverse burden of proof on the person carrying currency or bearer negotiable instruments across borders on the question of the legitimacy of such currency and bearer negotiable instruments. Therefore if, under these circumstances, a person is unable to demonstrate the legitimate origin and destination of the currency or bearer negotiable instruments, those funds may be stopped or restrained. Countries may consider confiscation of currency or bearer negotiable instruments without criminal conviction in a manner consistent with FATF Recommendation 3.

VI. POST-INTERDICTION EFFORTS: INVESTIGATIONS AND PROSECUTIONS

56. SR IX requires jurisdictions to ensure that persons who make a false declaration/disclosure and persons who are carrying out a physical cross-border transportation of currency/BNI related to ML/FT are subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative. In practice, this means that jurisdictions need to be able to investigate and/or prosecute and sanction such conduct.

A. Measures to investigate and/or prosecute and sanction false declarations and disclosure

57. Investigating the reasons why a false declaration/disclosure was made may uncover information that may be useful for intelligence purposes, or to support an investigation, prosecution and/or sanction against the traveller.

58. It is important to apply appropriate sanctions in circumstances where a false declaration/disclosure has been made since this has a preventive effect and may deter possible cash couriers.

59. There is no agreed minimum or maximum level for sanctions. However, considering that criminals/criminal networks are found to exploit mules (straw men) to transport currency/BNI, it is a best practice to confiscate the amounts transported, as a sanction or as an additional measure. However, confiscation of the full amount being transported may not be appropriate if it is found that the false declaration/disclosure was based on a justified error.

60. Criminal sanctions prohibiting the act of or attempt to conceal/smuggle currency and BNI greatly assist law enforcement investigative efforts. Criminal organisations are well aware of the legal requirements imposed on law enforcement which necessitate a linkage between the currency that is intercepted and the criminal act that resulted in those proceeds. As a result currency discovered during failed smuggling attempts often has to be returned to the violators for lack of evidence linking the currency and/or violator to criminal activities. The act of concealing/smuggling currency and/or BNI in order to evade crosses reporting requirements is a widely recognised red flag indicator for illicit activity which is worthy of independent criminal sanctions.

B. Measures to investigate and prosecute ML/FT

61. It is best practice for the customs authorities to ensure that their handling of suspected ML/FT is consistent with their powers and competencies, and with the overall law enforcement framework of the jurisdiction. Depending on the powers and competences of customs authorities, a file/traveller may be handled fully or partially by the customs authorities, or immediately referred to another competent authority (*e.g.* the police or a specialised ML/FT unit). In jurisdictions where the customs authorities are competent to investigate an ML/FT case, but do not have legal authority (*e.g.* to restrain the currency/BNI or detain the traveller for a sufficiently long period), it is best practice to ensure that such cases are handled by other authorities who have both the required competence and sufficient investigative authorities. This may necessitate implementing mechanisms, protocols or other arrangements to facilitate the rapid involvement of such authorities and avoid the risk of the traveller leaving the jurisdiction if released.

62. The effectiveness of the system is also facilitated if the customs authorities are made aware of the specific needs of other competent authorities who may play a role in the investigation and prosecution of a ML/FT case (*e.g.* the FIU, and law enforcement and prosecutorial authorities). In particular, on-going criminal investigations can benefit greatly when it is known that targets or associates have previously filed cross-border declarations. Historical reports on truthful declarations/disclosures have been used by law enforcement to establish knowledge and intent in on-going money laundering or other criminal investigations. Such awareness raising and/or training, supplemented by forms and templates for collecting evidence and taking statements, will facilitate the customs authorities in their collection of information that may usefully support an investigation or prosecution, and will alert and remind customs staff about the needs of other authorities.

VII. ADDITIONAL MEASURES AND BEST PRACTICES

63. The following are examples of additional measures that jurisdictions may choose to implement and which go beyond the requirements of SR IX and its Interpretative Note.

64. Jurisdictions have the possibility to lower the threshold for declaration/disclosure below the minimum set by the Interpretative Note to SR IX. This might be prudent in any of the following circumstances: *i)* where it is found that a reasonable number of travellers carry suspicious amounts of

currency/BNI below the threshold prescribed by the Interpretative Note to SR IX; *ii)* to bring the requirements/threshold for targeting cash couriers in line with the threshold requirements for currency control systems; and *iii)* to ensure that the threshold is appropriate and relevant for the jurisdiction if, for example, the cost of living in the jurisdiction is particularly low.

65. In some instances, jurisdictions may choose to target travellers who are carrying amounts of currency/BNI below the prescribed threshold. This may be appropriate, based on experience, intelligence and/or typologies (*e.g.* if the authorities are aware that certain travellers, sharing a common profile or background, are likely to be transporting the proceeds of crime). It is important to ensure that a proper legislative authority exists and a clear process has been established for such cases. For example, in some jurisdictions with advanced electronic payment systems, the possession of even relatively small amounts of currency can be unusual or even suspicious. Developing and updating intelligence-based typologies helps keep relevant authorities informed of trends in the ML/TF environment. It is useful to incorporate such typologies into the training programmes for the staff of customs, law enforcement and prosecutorial authorities and/or judges. In any event, it is important to ensure that such staff are aware that ML/FT may occur and is criminalised, irrespective of the threshold that applies to the declaration/disclosure system.

66. Another measure that jurisdictions may take is to not issue high denomination bank notes. This limits the means of cash couriers and increases the ability of customs to detect large amounts of cash being transported (*i.e.* bulk cash smuggling), since large values of smaller denominations will significantly increase the size and weight of the load.

67. In jurisdictions that do issue high denomination bank notes, it is best practice for the monetary authorities to track the spread of those bank notes on a macro level, including through co-operation with commercial banks which engage in cross border transport of currency. In particular, if new streams and flows of high denomination bank notes are detected, it is useful to share this information with the relevant AML/CFT authorities.

68. Other measures that the monetary authorities may take to discourage cash couriers are: using machines to automatically detect and record individual bank notes on the basis of the serial number; developing more means to detect and trace high denomination bank notes, such as the use of radio-frequency identification tags (RFID-tags); and encouraging the use of electronic payment systems.

VIII. RED FLAGS/INDICATORS

69. The FATF has developed a collection of red flags/indicators that can be used to detect cash couriers. In many cases, only more than one red flag/indicator will be a ground for suspicion.

a) Traveller has a connection with a risk area or jurisdiction. High risk jurisdictions include: jurisdictions with specific crime issues; jurisdictions with non-functioning state institutions; jurisdictions lacking customs authorities (*i.e.* free ports); jurisdictions with reduced presence of customs authorities (*i.e.* free trade zones); jurisdictions with high levels of corruption; and jurisdictions that do not or insufficiently apply the FATF Recommendations. The connection(s) that the traveller has with a risk area or jurisdiction may include the following:

   i) (former) nationality of traveller;

   ii) destination jurisdiction;

   iii) jurisdiction of origin of travel;

iv) (other) transit jurisdiction; and

v) jurisdiction travelled before.

b) Goods:

i) possession of illegal goods (*i.e.* narcotics, endangered species, counterfeit goods);

ii) traveller has a connection with high risk goods;

iii) lack of explanation for possession of goods originating from a high risk jurisdiction;

iv) traveller is in unusual possession of small valuable items (*i.e.* precious metals and stones, art objects, electronic goods);

v) traveller is in the possession of a (new) (pre-paid) mobile phone with unknown and/or few number(s) saved in the phone book;

vi) possession of stored value cards that cannot be endorsed in destination country.

c) Traveller:

i) has knowledge of and/or shows interest in the declaration/disclosure system and/or procedure;

ii) is actively seeking to have the import/export of currency/BNI documented by competent authorities;

iii) has a relevant previous criminal record;

iv) has a history of lost or stolen travel documents;

v) purpose of travel unknown or inconsistent with the profile of the traveller;

vi) has refused to consume food and drinks offered on vessel, indicating that currency might be hidden in body;

vii) uneasy movement or unusual body shape due to bulk cash hidden on body;

viii) traveller leaves jurisdictions with more currency than when the traveller entered the jurisdiction;

ix) is a politically exposed person or otherwise a person of interest;

x) leaves baggage at border/(air)port;

xi) travels with no or little baggage;

xii) aborts attempt to cross border;

xiii) overreacts to the presence of detection animals and/or refuses to be in the vicinity of detection animals and/or other detection equipment (*i.e.* x-ray machines);

xiv) has a suspicious travel history;

xv) travels with tickets purchased at the last minute / paid in cash / purchased by a third party.

d) Documents:

i) travel document pages appear to be damaged to conceal past travel;

ii) (suspected) use of different travel documents to conceal past travel;

iii) nationality stated on the travel document does not match the traveller.

e) Green border (*i.e.* non official border crossings):

i) traveller attempts to cross the green border;

ii) indication of and earlier undocumented border crossing.

f) Currency:

i) high risk currency;

ii) volume of the currency in possession of the traveller exceeds currency/monetary control threshold of country of issuance;

iii) cash is carried in several currencies;

iv) currency withdrawn close to the border;

v) possession of large amounts of currency from jurisdictions unrelated to the traveller;

vi) amounts declared/disclosed do not match the actual amounts carried;

vii) source of funds cannot be explained;

viii) small denomination, damaged and/or dirty banknotes;

ix) banknotes carried in concealed form (more than necessary to prevent against theft);

x) possession of counterfeit currency or BNI;

xi) traveller does not object when presented with the possibility that the currency/BNI will be seized by the authorities.

g) Patterns:

i) multiple individual travellers appear to be involved in similar movements or show similar travel patterns;

ii) travel patterns that mirror smuggling patterns of illegal goods (*i.e.* drugs) and human being trafficking routes;

iii) travel patterns that lack geographic, political or economic logic.

70. Jurisdictions agree that these red flags/indicators should be disseminated to competent authorities, including through the following channels: the FATF and the FATF-style regional bodies (FSRBs); the World Customs Organisation network; Interpol; the Egmont Group; the United Nations Counter-Terrorism Executive Directorate and 1267 Committee; the International Monetary Fund; and the World Bank.

IX. CASE EXAMPLES

71. *International co-operation*: In May 2009, the customs authorities of country A agreed to fully support the prosecutorial intentions of the customs authorities in country B. This particular case involves the arrest of two individuals and a bulk currency seizure made by the customs authorities of country A. The subjects originated their non-stop travel on an island territory of country B. As a result of the bilateral co-operation, the customs authorities on the island territory of country B successfully indicted the individuals previously arrested by authorities of country A. These subjects were charged with bulk cash smuggling violations. Three more spinoff investigations were undertaken, involving bulk cash smuggling from the island territory of country B to country A. These investigations are associated with three additional seizures made by the authorities of country A, totalling approximately USD 1.9 million.

72. *Domestic co-operation:* The customs authorities of country A noticed an increase in the amount of bulk cash smuggling being transported by different organisations via “go-fast” vessels. Customs authority agents based on an island territory of country A developed information, through ongoing investigations, regarding the smuggling of a large amount of currency out of the island territory of country A. On one occasion, customs agents, in co-ordination with border protection authorities and air and marine authorities, interdicted two vessels travelling without navigation lights. A subsequent search of the vessel resulted in the discovery and seizure of approximately USD 1.7 million concealed within suitcases, and the arrest of two individuals. During a separate and unrelated incident, customs authority agents in co-ordination with border protection authorities and the police of the island territory of country A intercepted a go-fast vessel southeast of the island territory. A search of the vessel yielded the discovery of USD 2.1 million concealed within the vessel. According to the investigation, the currency was to be utilised to purchase approximately 500 kilograms of cocaine in a nearby tax and customs free territory of countries B and C, which would subsequently be smuggled to the island territory of country A.

73. *Domestic and international co-operation:* After seizing USD 150 000, the responsible local law enforcement entity in country A contacted its customs authorities and provided the intelligence gathered during the enforcement action. This information was forwarded to a specialised customs office, which initiated an investigation into various individuals involved in bulk cash smuggling activities. This investigation initially generated several arrests and seizures totalling approximately USD 1 000 000 and

200 kilograms of marijuana. As a result, the customs office co-ordinated with the authorities in country B and initiated a spinoff investigation targeting co-conspirators and three drug cartels based in country B. Based on the evidence developed by the customs authorities in country A and the international co-operation, the authorities in country B used special investigation techniques to support a money laundering investigation in country B. This multijurisdictional investigation resulted in approximately 12 additional arrests in country B. Most of the subjects arrested in the country B were subsequently extradited to country A.

74. *Statistical data and working groups*: Country A established a domestic working group (task force), with members from law enforcement entities, customs, intelligence services and the FIU. This group has focused on the use of declarations/disclosures as a mean to launder money. For this, the group collected statistics to identify ports of entry most often used to declare/disclose currency/BNI. As a second step, the group identified the natural and legal persons that were connected to the declaration/disclosure. These data were enriched by data from the FIU. On the basis of the statistical analytical work by the task force, the member authorities of the task force were able to identify and stop cash couriers.

75. *Comparing declarations/disclosures with STRs*: A traveller declares/discloses EUR 20 000 to customs in country A Customs immediately sends the file to the FIU, which compares the declaration/disclosure to STRs in its database. The FIU is able to link the traveller, through another person, to several cash-related STRs. A further check with law enforcement databases indicated a connection with several cases of sexual exploitation.

76. *Persons of interests*: Custom authorities in country A are aware that persons of interests are involved in a profit generating crime. They attempted to carry the funds out of country A, but are stopped because of their status as person of interest. As they were searched, the authorities found almost AUD 100 000 (USD 90 000) in cash which had not been declared. The funds were seized and the persons of interest charged with failure to declare currency, and later convicted for that reason. The currency was confiscated and a large portion was used to compensate the persons defrauded by the persons of interest.

77. *Assisting third countries*: Upon entering country A, suspect 1 fails to declare/disclose AUD 30 000 (USD 27 000). While being detained for non-declaration/disclosure, a law enforcement data check reveals that suspect 1 and a connected person receive large fund transfers from country B, which are immediately followed up by identical fund transfers to country C. Both suspects also appear to own a number of valuable properties despite the fact that one of them is an unemployed student. A further investigation reveals that the multiple transactions were used to receive false tax concessions in country C. The authorities of country C were not yet aware of these criminal facts, but could be informed on the basis of this failure to declare/disclose.

78. *Use of commercial airline:* Airport security officials at an x-ray security point discovered a large amount of currency hidden in a false-bottom briefcase. The security officials then notified customs authorities who responded by performing a search of passengers who were boarding the same international flight. An announcement was made prior to the passengers boarding the flight notifying them of the requirement (in the departure country) to declare cash. One suspect then declared cash in the amount under the reporting requirements. While boarding the aircraft, the suspect was stopped in the jet way and advised of the reporting requirement and was afforded the opportunity to amend his previous declaration. After he chose not to avail himself of that option, an inspection disclosed that the suspect was carrying significantly more currency than he had declared. This currency was immediately seized.

79. *Use of private vehicles:* As a result of a lookout at a land border port, Country B intercepted a total of USD 165 000 in suspected proceeds of crime. The subject of the lookout was returning from Country A. Upon inspecting the pick up truck, officers noticed that the airbag cover in the passenger side

was loose. Officers removed the plastic cover revealing a false compartment, which was found to be concealing the bundles of currency. In addition, the passenger of the vehicle was carrying a large quantity of currency on her person.

80. *Use of air parcels:* Law enforcement authorities in Country C initiated an investigation based on two bulk currency seizures of USD 200 000 discovered in express outbound courier shipments intended for a particular business in Country X. This currency was destined for a country of concern. The business and its owner located in Country X were ultimately identified as members of a known and designated Middle Eastern terrorist organisation.