A DRAFT FRAMEWORK FOR MONEY LAUNDERING/TERRORIST FINANCING RISK ASSESSMENT OF A REMITTANCE CORRIDOR

September 2021

Table of Contents

Disclaimer

This work is a joint product of the staff of the International Monetary Fund (IMF) and the World Bank Group (WBG). The findings, interpretations, and conclusions expressed in this work belong to the authors of the report and do not necessarily reflect the views of the IMF or the WBG, their Boards of Executive Directors, and the governments they represent.

Acronyms and Abbreviations

AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
BBs	Building Blocks
BSA	Banking Secrecy Act
CBR	Correspondent Banking Relationship
CDD	Customer Due Diligence
CPMI	Committee on Payments and Market Infrastructures
CRA	Corridor Risk Assessment
E-KYC	Electronic Know Your Customer
EMDE	Emerging Market and Developing Economy
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSB	Financial Stability Board
FSRB	FATF-Style Regional Body
ID	Identification
KYC	Know Your Customer
ML/TF	Money Laundering/Terrorist Financing
MSB	Money Service Business
MTO	Money Transfer Operator
MVTS	Money or Value Transfer Service
NGO	Non-Governmental Organization
NPO	Non-Profit Organization
NRA	National Risk Assessment
PEP	Politically Exposed Person
POC	Proceeds of Crime
RBA	Risk-Based Approach to AML/CFT
RSP	Remittance Service Provider

SRC	Safe Remittance Corridor
STR	Suspicious Transaction Report
TTR	Transaction Threshold Report

Introduction

Remittances are the financial lifeblood not only for the families of migrant workers but also for the economies of many emerging markets and developing economies (EMDEs). Remittances, however, may pose money laundering and terrorist financing (ML/TF) risks, depending on the context of the sender and/or recipient countries as well as the scale and the characteristics of criminal activities and terrorism in these transactions. If these risks are not well understood and mitigated effectively, a remittance corridor could be abused by criminals, organized crime groups, terrorists, and terrorist organizations, potentially undermining national security, social order, and economic stability on both sides of the corridor.

Though remittances may pose ML/TF risks, all remittance corridors and all the transaction categories in a remittance corridor should not be treated as inherently higher risk and lower[1] risk situations can be identified. A key factor in having efficient and well-calibrated regulatory frameworks in the remittance corridor countries is the implementation of risk-based anti-money laundering/combating the financing of terrorism (AML/CFT) measures, in line with the Financial Action Task Force (FATF) standards. This will enable prioritization of AML/CFT measures and calibration of regulatory frameworks to reduce the costs of compliance and risk-mitigating measures for lower-risk transactions. To support sustainable development and poverty reduction, it is crucial not to impose on the remittance sector more stringent measures than are warranted to mitigate ML/TF risks.

Effective ML/TF risk assessments are a critical underpinning for having a risk-based regulatory framework for a remittance corridor. ML/TF risks in a corridor can be identified, analyzed, and assessed by the authorities, including the ML/TF threats and vulnerabilities in the corridor, the likelihood of risk events in the corridor, and their possible consequences. The risk assessment would then be the basis for adjusting the regulatory framework and the supervision of the remittance sector on a risk basis.

Correspondent Banking Relationship Pressures on Remittances

In recent years, global correspondent banks have been terminating or restricting business relationships with certain client categories. Some key drivers behind this decline in correspondent banking relationships are changes in banks' operational and financial risk appetites (risk and return considerations) due to changes in the regulatory and enforcement landscape, increased supervisory pressure and sanctions for non-compliance with AML/CFT regulations, bilateral economic and trade sanctions, rising AML/CFT compliance costs,

[1] "Low risk" and "lower risk" have specific meanings in FATF Recommendations. While "low risk" refers to absolute and proven low risk which can be the basis for exemptions (see Interpretive Note for Recommendation 1 of the FATF Recommendations) in limited circumstances, "lower risk" implies relativity and can be the basis for simplification but not exemptions. The Financial Stability Board (FSB) Roadmap refers to low risk in a more generic way. Considering that the focus of this project is not on the exemptions from the application of certain anti-money laundering/combating the financing of terrorism requirements contemplated by FATF, the authors followed the FATF terminology and used "lower risk" throughout the report.

increased demands for tax transparency, and unclear regulatory expectations and difficulties in managing and mitigating cross-border ML/TF risks associated with correspondent banking relationships (CBRs). In some cases, local/national banks have assessed that the level of risks posed by their clients is acceptable but still decided to terminate some business relationships due to their correspondent banks' risk appetite.

Withdrawal of CBRs has affected the remittance service providers (RSPs) and created new challenges in the provision of remittance services in some countries. In some countries and regions, smaller remittance players have been forced to close, to become agents of larger businesses, or to continue remittance transactions through unregulated channels or alternative arrangements such as nested correspondent relationships and cash couriers.

G20 Roadmap for Enhancing Cross-Border Payments

The G20 has made enhancing cross-border payments a priority in order to achieve faster, cheaper, more transparent, and more inclusive cross-border payment services, while maintaining their safety and security, thereby facilitating economic growth, international trade, global development, and financial inclusion. At its October 2020 Finance Ministers and Central Bank Governors meeting, the G20 endorsed the Roadmap for Enhancing Cross-Border Payments, which comprises 19 building blocks (BBs). The IMF and the World Bank were assigned to cover BB7 on "safe payment corridors," which involves the development of a framework for remittance corridors' risk assessments. BB7 is part of focus area B within the G20 cross-border payments roadmap. Focus area B is aimed at coordinating and streamlining regulatory, supervisory, and oversight frameworks across jurisdictions and at fostering efficiencies in customer due diligence processes by facilitating cross-border data flows and fostering usage of digital identification (ID) and shared customer due diligence infrastructures.

BB7 on "Safe Payment Corridors" has two phases: The first phase is about the development of a framework and methodology for the assessment of the ML/TF risks in remittance corridors and the identification of potential "lower risk corridors," as part of or consistent with a country's national ML/TF risk assessment (NRA). In the second phase, the proposed framework is expected to be piloted in some corridors with a view to testing and further refining the assessment methodology.[2] To reflect the scope more accurately, this report uses the term "safe remittance corridor" (SRC) [3] rather than "safe payment corridor."

The Objective of this Report

This report proposes a draft framework and methodology for the ML/TF risk assessment in remittance corridors having the potential of being identified as SRCs. The content of this

[2] Financial Stability Board, *Enhancing Cross-border Payments; Stage 3 Roadmap*, October 13, 2020, pp. 20, https://www.fsb.org/wp-content/uploads/P131020-1.pdf.

[3] The term "Safe Remittance Corridor" does not imply an absence of ML/TF risks in the corridor, but rather a lower risk level.

report is the deliverable of the first phase of BB7 and is expected to facilitate ML/TF pilot risk assessments in one or more remittance corridors to be determined in the next phase of the project. The final version of the framework will incorporate findings and insights from the pilot risk assessments and stakeholder consultations. This report proposes an assessment framework that can be applied jointly or separately by the sender and the recipient corridor countries.

Some Key Concepts in the Report

In the context of this report, "international remittances" refer to cross-border person-to-person and non-commercial payments of relatively low value. Due to the wide variety of cross-border transactions it is difficult to have precise boundaries and a definition of remittance transactions. The main sources that attempt to define the scope of international remittances are the International Monetary Fund's (IMF) *Balance of Payments Manual* and the Committee on Payments and Market Infrastructures' (CPMI) *General Principles for International Remittance Services*. For simplicity, this report mainly adopts the definition by the CPMI. The qualifier "non-commercial" has also been added to this definition to make clear that commercial transactions are out of the scope of this project. Throughout this report, "remittances" refers to "international remittances" and "remittance corridor" to the formal international remittance channels between a sender and a recipient country. In some sections, the report refers to "cross-border payments" when it is needed to cover non-remittance transactions in the discussion. The sender country is sometimes referred to as the "home country" that conducts the assessment. A "third country" means any other country than the sender and the recipient country.

Overarching Considerations for a Remittance Corridor Risk Assessment

1.1 Objective of a Remittance Corridor Risk Assessment (CRA)

In the context of BB7, the objective of a CRA is assessing and understanding the ML/TF risks of remittances in a corridor, with the aim of simplifying AML/CFT measures in lower risk remittance transactions. If the CRA assesses that the overall ML/TF risk level in the corridor is lower, the corridor can be treated as an SRC[4] and subject to simplified customer due diligence (CDD) measures by regulatory authorities, which can be implemented by the private sector. This process is mainly about the assessment and identification of lower risks as the basis for CDD simplifications on a policy and regulatory level, and communication of the assessment results to the private sector to assist with their own customer risk assessment. It does not necessarily require formal declaration of a "safe remittance corridor" by any national or supranational agency. Even if the corridor as a whole is not lower risk, the assessment may find that some remittance sub-categories in the corridor are lower risk and these could qualify for CDD simplifications (e.g., as they relate to remittances below a certain value, to a lower risk remittance product, or to a lower risk region in a country of the corridor). Such simplifications are eventually expected to reduce the regulatory requirements and associated costs for service providers and end users. Low levels of organized crime and terrorism on both sides of the corridor, low average transaction values, remittances between family members, and a reliable ID infrastructure are some of the factors that may contribute to lower ML and TF risks.

The identification of SRCs based on a robust CRA can reconcile two important policy goals in relation to remittances: first, to support poverty alleviation and economic growth in low-income countries by safeguarding cost-effective transfer mechanisms; and second, to minimize the risk that these mechanisms will be used for criminal or terrorist purposes. Implementation of the SRCs has the potential to lower compliance costs of lower risk remittances, but its effectiveness will ultimately depend on the ability of SRC frameworks to inform regulatory and supervisory oversight of global and regional banks and other financial institutions that facilitate the remittances.

1.2 Defining the Scope of the Assessment

The CRA process should begin with defining the scope of the assessment. The scope should clarify the following:

a) Corridor(s) to be assessed:

The first step is identifying the corridor to be assessed. In the context of remittances, a particular pair of a remittance origination jurisdiction (sending) and a remittance recipient jurisdiction is collectively referred to as a "corridor." A corridor assessment can be carried out

[4] To qualify a payment corridor as safe, it would also be relevant to conclude a lower risk of proliferation financing or illicit finance, including tax evasion.

jointly or unilaterally by the "sender" or the "receiver" country in a corridor. In practice, it can be expected that in most scenarios it will be conducted by a sender country with contributions from the recipient country, as feasible. The assessment may cover a single corridor or multiple corridors where the risk factors are similar. A sender or a recipient country should consider the following factors when identifying the remittance corridors that may necessitate a focused CRA:

- Potential for the corridor to be classified as lower risk. It would not be recommended to engage resources in a CRA when there are clear indications of higher ML/TF risks.
- Importance of the corridor for the immigrant community (e.g., number of people supported, amount of support as a share of GDP of the recipient country) and the host country (e.g., labor market contributions of the immigrant community).
- How vital is the corridor for the immigrant community (and their dependents) and the host country?
- How important is the corridor for the economic development of the recipient country?
- Are there challenges in sending or receiving remittances? If yes, what are the challenges?
- High remittance costs in the corridor.
- Indications of de-risking of the clients or the service providers in the corridor.
- The extent of the informal money transfer channels in the corridor.
- Prevalence of cash couriers in the corridor (declared or undeclared).
- Feedback/requests from private sector.
- Complaints/requests from migrant communities that use the corridor.

b) Uni-directional or bi-directional assessment:

A CRA can be unidirectional or bidirectional. In other words, the CRA may focus on the analysis of the remittances in one direction (i.e., from home country to country X) or in both directions (as well as cover the transactions from country X to home country). The unidirectional CRA would be of particular use for corridors dominated by transactions in one direction or where the risk profile of remittance flows varies significantly based on the direction. In most cases, the assessment can be expected to be unidirectional, as most corridors are heavily dominated by remittances in one direction.

c) Overall remittance corridor assessment vs. assessment of sub-categories of remittances in the corridor:

The risk assessment may target the evaluation of the overall risk level of a remittance corridor and/or sub-categories of remittances in the corridor. It is recommended that countries conduct the CRA in a way that will distinguish the risk levels of different sub-categories of remittances in the corridor. These sub-categories can be based on the amounts of the transactions, origin and destination of the remittances, senders and receivers of the transactions, type of an RSP and remittance products, their delivery channels, as well as combinations of any of these. Even if the overall ML/TF risk in a corridor is rated medium or high, the risk in some of the sub-categories may be lower. For example, the overall TF risk in a corridor can be ranked medium, but the likelihood of raising funds for terrorists can concentrate only in a specific region.

1.3 Domestic and International Cooperation

a) Domestic cooperation

For the success of a risk assessment, domestic and international cooperation amongst stakeholder agencies is particularly relevant. In the domestic context, the following can contribute to the CRA:

- the financial intelligence unit;
- relevant financial sector regulators and supervisors (of banks, money transfer operators (MTOs), and other non-bank financial institutions);
- financial inclusion unit or team at the central bank (or another agency);
- payment systems, national accounts, and other relevant departments of central banks;
- law enforcement, prosecutorial, and intelligence agencies (as necessary);
- customs and immigration authorities; and
- the statistics agency.

Depending on their functions and the information they collect, some of these stakeholders should play a key role, while others can contribute data or viewpoints. The involvement of the private sector is also important. Relevant non-governmental organizations (NGOs) can also contribute to the understanding of the risk level of immigrant communities, existence of informal remittances and channels, and challenges related to CDD, specifically regarding the movement of funds for humanitarian purposes. In countries where the centralized collection of remittances data is problematic, collaboration with the relevant private sector players is essential. It is recommended to assign a lead agency, a project leader, and a team for a CRA.

b) International cooperation

Ideally, the corridor countries should carry out CRAs jointly. Each country in a corridor has access to their own data and information on the transactions and ML/TF risks in the corridor and is aware of the issues relating to that country's side of the corridor. Doing the assessment jointly will maximize access to data and information, including from the NRA, and will bring the two perspectives together which can eventually lead to a more complete, comprehensive, and robust risk assessment. Furthermore, such a joint assessment will facilitate commitment and coordination in addressing the challenges and recommendations made, mitigating the risks and introducing more harmonized regulations and supervisory approaches as appropriate for both sides of the corridor. If a joint assessment is impossible, the country that conducts the risk assessment should continue its efforts to coordinate with the other country to keep it informed as well as to obtain inputs and data from that country. Having bilateral meetings and inviting the counterpart country to participate in some of the project activities or to be part of the project team can be effective ways of facilitating coordination and the exchange of information.

1.4 Data Requirements and Sources

Quantitative as well as qualitative data sources are important components of remittance CRAs. A good risk assessment is one that balances the use of quantitative and qualitative data. Like all ML/TF risk assessments, a remittance CRA will also have a subjective element and will ultimately require analysis, evaluations, and judgements by the experts who conduct the assessment. Adequate and reliable quantitative and qualitative data will reduce the subjectivity in the evaluations and lead to informed judgements. The countries need to take the necessary measures to ensure the involvement of qualified experts in the assessment process and to have mechanisms in place for the quality control of the assessment. Annex 1 contains a list of possible qualitative and quantitative data sources that can support a CRA. The list does not imply that all data in the list should be collected for any CRA. Rather, the data collection for a CRA should be a focused and efficient process that makes the best use of existing data and considers additional data and information based on the value they can add to the assessment.

1.5 National ML/TF Risk Assessment

NRAs can be used as a foundation of remittance CRAs. If a country already has a recent and reliable NRA,[5] the authorities can use its analysis and conclusions to inform the CRA. As per FATF Recommendation 1, understanding and assessing the ML/TF risks is a mandatory requirement and constitutes the backbone of the AML/CFT regime in any country. Since 2014, almost all countries have already conducted their first NRAs and many countries tend to update their risk assessments every 3 to 5 years. The CRA can rely on the corridor countries' NRAs for the analysis of the general ML/TF risk environment in the country, including the typologies and trends in the generation and the laundering of the proceeds of crimes (POC), funding of terrorist activities and organizations, abuse of various sectors and products for ML and TF, as well as the

[5] FATF Guidance on the National Money Laundering and Terrorist Financing Risk Assessment outlines general principles for the conduct of risk assessment at the country level: https://www.fatf-gafi.org/media/fatf/content/images/national_ml_tf_risk_assessment.pdf.

threats and vulnerabilities at the national and sectoral levels.[6] The NRA findings can enable the CRAs to focus on the extent to which national ML/TF threats and vulnerabilities are present in the assessed corridor and the level of risk in the remittance sector and in the given corridor relative to other sectors and corridors. If an NRA is currently being conducted or is about to be conducted, the timing of the corridor risk assessment may be planned accordingly so that the outputs of the NRA can inform the corridor risk assessments. Doing two assessments in parallel may also lead to some synergies.

Ideally, the corridor risk assessment should consider the NRAs of both countries in the corridor. In the cases where a corridor country has not publicized its NRA, it is important for the comprehensiveness of the CRA to exchange and incorporate in the CRA relevant information on the assessment of ML/TF risks in both countries. A memorandum of understanding between the two countries and the involvement of a wider group of stakeholders from both countries may also contribute to smoother cooperation and coordination in conducting the risk assessment.

[6] Some countries may have conducted sectoral risk assessments (e.g., of financial sector) as a part of or in addition to the NRA. References to NRAs throughout the report also apply to such sectoral risk assessments.

Assessing the Environment of the Two Countries and Relevant Contextual Factors

Understanding the nature and the extent of economic and other links between the two corridor countries is an important component of the CRA. In addition to the analysis of country-specific risk factors, which informs threat assessments (Section 4) and vulnerability assessments (Section 5), a CRA should also focus on the analysis of links between the corridor countries. Description of economic and other links between the countries, such as trade, investment, remittances, and predicate crimes spanning both countries, is a useful starting point, providing a backdrop to analyze the level and nature of risks in the corridor as well as their relevance specifically to the remittances and may also help to isolate lower risk activities. Moreover, the CRA can focus only on the country's ML/TF risk factors relevant for the assessment of risk in a specific corridor.

The CRAs should analyze migration and other sources of data to provide context and estimate potential for the remittance flows. Statistics on the number of naturalized citizens, permanent residents, seasonal workers, and longer-term visitors, and estimates of illegal migrants originating from the recipient corridor country can be analyzed to identify possible sources of remittances and to estimate their potential maximum value. This potential value of remittances can be used to approximate an upper bound for the corridor's value and number of remittances, providing an indicator that is useful when examining the discrepancy between the potential and the actual value of remittance flows in the corridor and for understanding and monitoring the corridor's flows. For example, the size of a migrant community, its geographic distribution, and average income can be cross-checked with the value, volume, and location of remittances sent through the respective corridor. Information about existing labor market and other policies, such as guest worker policies, can provide additional understanding of the sources of remittances.

Characteristics of remittance payments in a corridor, such as their volume, value, periodicity, purpose, and currency composition, should be included in a CRA. These characteristics impact the level of ML/TF vulnerability of a remittance corridor and are also useful when evaluating the potential of the corridor for abuse for larger-scale ML/TF activities. In addition, the currency composition of remittance flows may impact the settlement arrangements, the CRA's stakeholders, and, possibly, the need to consider actions of supervisors and regulators of other countries. Understanding the specific context of a migrant community, including their access to banking services, can provide additional insights regarding the purpose of remittances and other characteristics and enable a more accurate assessment of ML/TF risk. For example, seasonal employment programs may lead to less frequent but higher value remittances.

CRAs need to consider risks related to organized crime groups, terrorist organizations, and predicate crimes that span both countries. Organized crime and terrorist groups active in both countries can potentially misuse the payment corridor for ML/TF and move funds to support their operations. Relatedly, commission of some predicate crimes, such as smuggling or trafficking in human beings, drugs, and arms, may involve both corridor countries, posing

ML/TF risks specific to the payment corridor. Thus, the information on the existence, nature, and operations of serious and organized crime groups, terrorist organizations, and the predicate crimes that span both countries can help assess the likelihood of the remittance corridor being abused for moving proceeds or instrumentalities of crime. For example, evidence of the existence of cross-border organized crime groups that are active in the remittance corridor combined with high volumes and average values of remittance payments may preclude identification of a corridor as lower risk.

Some countries may have geographic variability in the ML/TF risk profiles of their regions that can be included in the CRA. For some originator countries, ML/TF risks can be specific to a certain region where, for example, the likelihood of raising funds for terrorists or the placement of proceeds of crime (e.g., due to illegal mining of precious stones or illegal logging activities) are higher. Similarly, some regions of beneficiary countries can pose higher ML/TF risks, for example, from the use of funds for terrorist purposes or due to their attractiveness for integrating illicit proceeds in the economy, such as for real estate investment. In addition, activity of the organized crime groups and predicate crimes that span both countries can also be concentrated in certain regions rather than spread uniformly across the country. To the extent that such higher ML/TF threats and vulnerabilities can be identified at the regional level and isolated in the remittance services' operations, CRAs can provide more granular information to help delineate the lower risk activities.

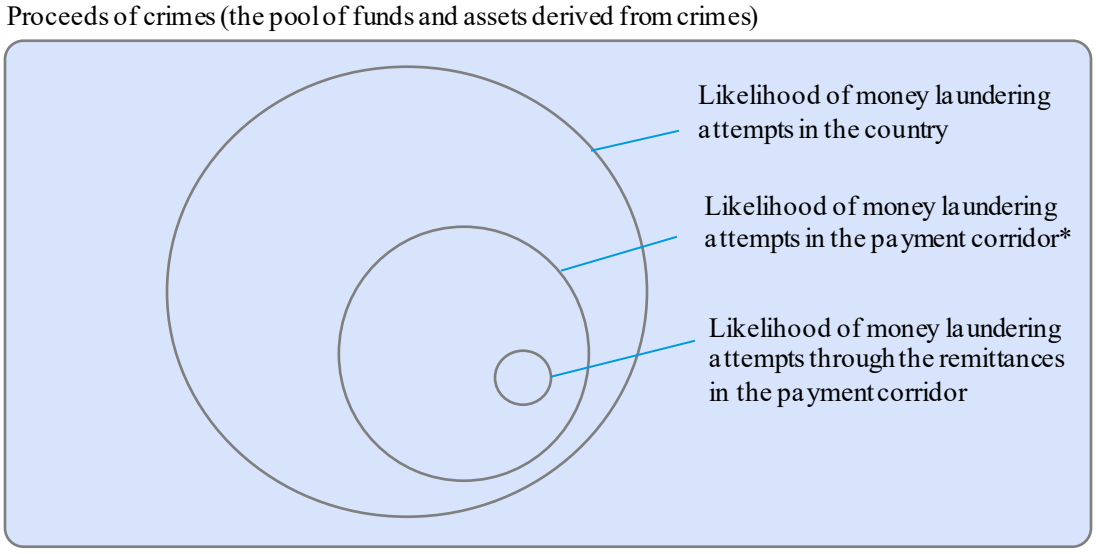
Assessment of Threats in the Remittance Corridor

1.6 Money Laundering Threat

The estimated volume of the proceeds of crimes in a country broadly determines the overall potential for money laundering. By its definition, money laundering is linked to an underlying crime, namely a predicate offense. Therefore, the analysis and understanding of the proceeds of crime (POC) constitutes a logical starting point for an ML threat assessment. POC include funds and assets derived directly and indirectly from domestic or foreign predicate offenses.

An ML threat assessment is based on the types of crimes that generate the most proceeds and the likelihood that they will pass through the assessed corridor. The ML threat assessment can consist of two elements: a list of various types of crimes with an estimate of their importance in generating proceeds in the country and an analysis of factors that impact the probability that proceeds of the main types of crimes would be laundered through the remittance corridor. Hypothetically, a threat assessment may conclude that corporate tax evasion and corruption, despite being the main proceed-generating crimes in a country, pose a lower ML risk to the remittance corridor. In the country that conducts the assessment, there may be typologies of abuse of cross-border payments for ML/TF. However, this does not necessarily increase the ML/TF risks in the remittance corridor that is being assessed. Even if there are indicators of money laundering in the cross-border payments between two countries (through corporate or trade-related transactions), risks related to remittances may still be lower.

Figure 1. Different Layers of Assessing the ML Threat in a Payment Corridor



** "Payment corridor" in this chart refers to the broader group of cross-border payments that include non-remittance transactions.*

There are several layers of a threat assessment which may help identify and assess the ML threat to remittances in a corridor. As illustrated in Figure 1, the assessment of all these layers impacts the "likelihood" of a money laundering attempt through the remittances in a corridor.

Understanding the Proceeds of Crimes and the Overall Threat of Money Laundering

If possible, the CRA should describe the nature and scale of predicate crimes in the country and the POC generated by these crimes. A CRA is not expected to undertake a full-fledged POC assessment in the country and can rely on the NRA, credible academic studies, experts' perceptions, and reports and inputs from competent authorities. This analysis needs to be broader than confiscation records and should capture POC that may not have been confiscated. Records of and estimations about the criminal goods (such as smuggled drugs or arms) and activities may be useful in estimating the proceeds of crimes. Consideration of the amount of proceeds generated by different categories of predicate offenses and understanding what the most important economic crimes are in the country context can form the basis to analyze the predicate offenses, although material in the originator country is unlikely to pose ML risks to the assessed corridor. In addition to the domestic ML threat, the CRA can explore the attractiveness of the corridor countries for foreign proceeds of crime to analyze the risk to the corridor countries from the layering stage of money laundering.

Understanding the ML Threat in the Payment Corridor in General

After an understanding of the proceeds of crimes in one or two countries has been formed, the next layer of the assessment is the ML threat in the assessed payment corridor. This threat can be defined as the probability of money laundering attempts in the payment corridor from the home country to the recipient country. The demographic, geographic, or socioeconomic relationships between two countries as well as the attractiveness of the recipient country, for example due to its role as a regional or a global financial center or its links to organized criminal groups, can raise this likelihood for money laundering.

The assessment needs to analyze the quantitative information available and complement the analysis with qualitative information. The quantitative information may include money laundering cases, information exchange requests, and suspicious transaction reports that involve the use of the payment corridor. These figures need to be analyzed in absolute terms as well as in comparison with other payment corridors of the home country to understand the relative level of the threats in the corridor. Money laundering typologies (if available) can provide information on whether the types of financial institutions, products, and services present in the corridor were used for ML purposes. Limited information and data will make the CRA more challenging.

Assessing the ML Threat to Remittances in the Payment Corridor

ML threat to the remittances in a payment corridor may differ from the overall ML threat in a country. In addition to the magnitude of POC, the CRA should consider remittance corridor -specific factors that influence the probability that POC generated by various types of crimes are

likely to pass through the remittance corridor. Analysis of the country context; typologies; serious and organized crime assessments; data on the demographic aspects of detected crimes such as the nationality, age, or gender of the perpetrators may allow a focus on the types of crimes most relevant to the remittance corridor. For example, migrant work programs that withhold income tax reduce the threat of tax evasion through the corridor. In addition, such factors as the nature of the underlying crimes (i.e., petty vs. organized crimes), use of POC (i.e., consumption vs. laundering) and composition of POC (i.e., financial vs. physical assets) of various types of crimes influence the level of ML threats to remittances.

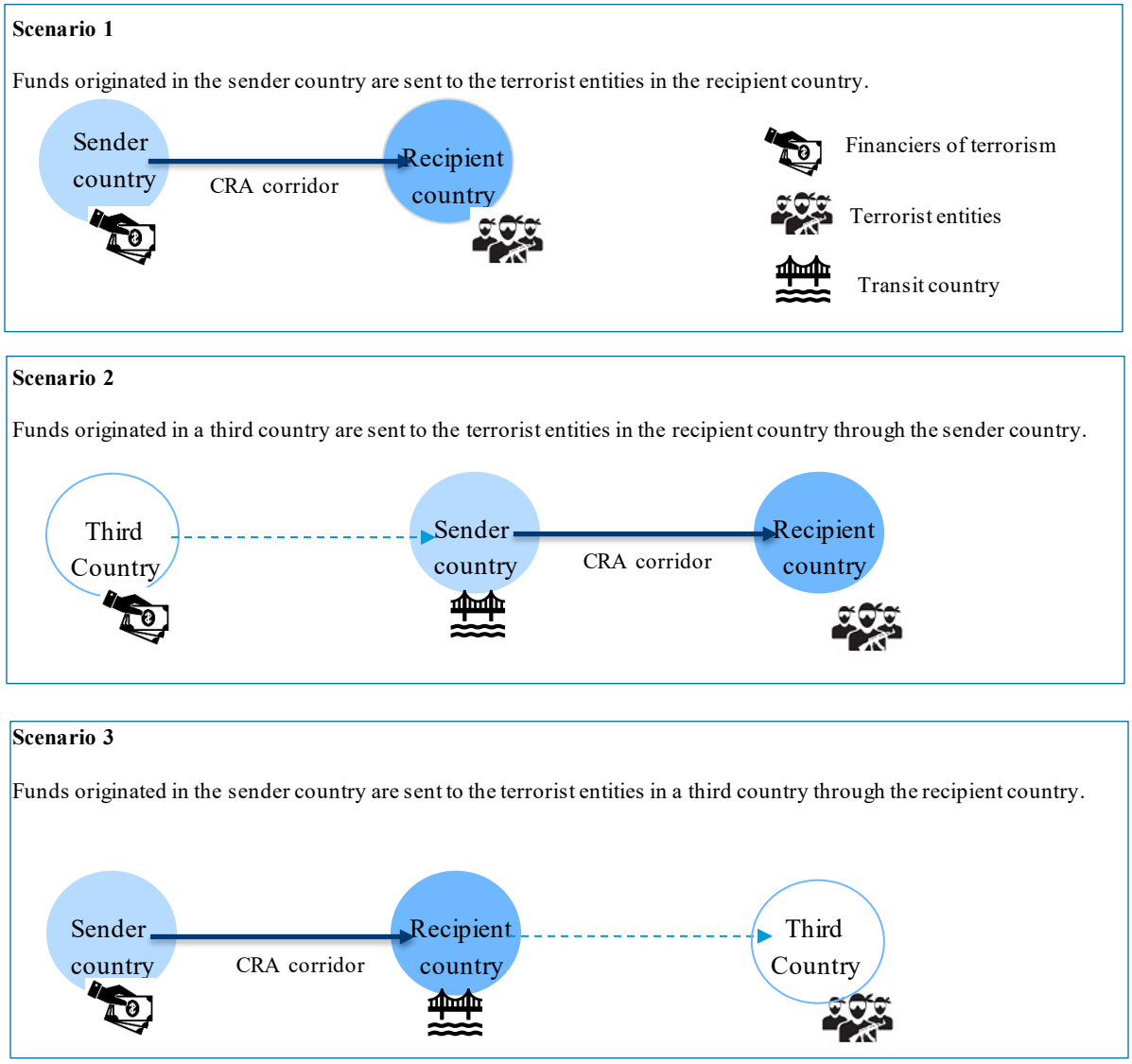
Assessing the likelihood of risk events and typologies that involve the use of remittances in the corridor is an important component of an ML threat assessment. Because of their low amounts per transaction, the utility of remittances, especially for large money laundering operations, can be very limited. Laundering money through remittances would require numerous low amount transactions which may not be feasible for most money launderers. Globally, there are examples of micro-scale money laundering methods such as the use of smurfing (a network of seemingly ordinary account owners or occasional senders) or structuring (dividing the funds into smaller amounts through the same or different people) for money laundering especially by organized crime groups. However, this also depends on factors such as the identification infrastructure and the demographic links of the organized crime groups and may not be feasible in all corridors. The CRA should also look at past money laundering cases and typologies to examine the existence and the extent of smurfing and structuring types of money laundering patterns in the corridor and other corridors linked to the sender and the recipient countries.

The threat assessment should also be supported by an overall strategic analysis of the remittances in the corridor. It is also important to analyze the threat level by questioning and verifying whether the pattern of remittance flows in the corridor is in line with the rationale provided for the remittances. This may involve a strategic analysis of the total remittances in the corridor; their seasonal patterns, purposes, senders, and receivers; and the relationships with macroeconomic and demographic indicators. Analyzing the frequency of transactions in different monetary tranches, the average amounts remitted, and their relationship with average income can be a useful tool in understanding and verifying the rationale of the remittances.

1.7 Terrorist Financing Threat

Like money laundering threats, terrorist financing threats in a payment corridor may have domestic or foreign origins. Therefore, it is important for the terrorist financing threat assessment to cover the possibilities of domestic and international terrorist financing. The payment corridor may be abused for terrorist financing in different ways. The illustration in Figure 2 shows different basic scenarios.

Figure 2. Basic Scenarios for TF in a Payment Corridor (That Is Being Assessed)



The terrorism context in the recipient country is one of the most important factors that will determine the level of TF threats in the payment corridor. It is critical to understand whether there are any consequential terrorist activities and terrorist organizations in the recipient country. The input of the counter-terrorism and intelligence authorities and close cooperation and information exchange with the recipient country authorities are key for this analysis.

If terrorism risks are present in the recipient country, implications on the TF threat in the payment corridor need to be further examined. The existence of terrorist groups and/or terrorist activities in the recipient country does not necessarily correspond to a high TF threat in the payment corridor. It is necessary to question whether there is the potential and a rationale to

use the payment corridor for TF purposes. The assessment should consider the following questions:

- Are terrorist activities and organizations in the recipient country mostly funded domestically or internationally?
- If the latter, why would these terrorist organizations prefer the payment corridor that is being assessed and how would they use it?

In a TF threat assessment, the cultural, demographic, and socioeconomic factors in the assessed payment corridor countries should be carefully considered. If there is an immigrant community in the sender country, which is to be expected in most corridors, does this community include people who may be linked to or sympathetic with terrorist organizations in the recipient country? Furthermore, besides the immigrant community, there may be ethnic or ideological proximity between the nationals of the sender country and the terrorist organizations in the recipient country that would need to be considered.

The principles on the use of quantitative and qualitative information in ML threat assessments apply to TF threat assessments as well. It is important to understand the patterns and behaviors in terrorist financing in the sender country and in the recipient country. Past typologies and detected cases need to be analyzed carefully to understand patterns in the use of different sectors, institutions, services, and products in the financing of terrorism. The quantitative information needs to be supported with qualitative information, which may include typologies, observations and experiences of subject matter experts, interviews with NGOs or immigrant communities, and interactions/interviews with the authorities of the recipient country.

Understanding the attractiveness of the home (sender) country as a transit point for TF transactions is an important part of the CRA (scenario 2 in Figure 3). If a recipient country with identified terrorism risks has limited access to the global financial system and the home (sender) country constitutes its main gateway to the global financial market, this may increase the TF threat to the payment corridor. Close socio-economic relations with and frequent transactions from third countries that are known or suspected to have sympathizers of terrorist organizations in the corridor (recipient) country is another factor to be considered. Scenario 2 will be more likely if the home (sender) country is a global or a regional financial hub.

The third scenario in the TF threat assessment relates to the use of the recipient country as a transit to support terrorist organizations in a third country or countries. Scenario 3 in Figure 3 will eventuate if there is a potential that the home (sender) country (based on ethnic, demographic, and ideological factors) will use the assessed corridor to support terrorist organizations in a third country or countries. This possibility will increase if the home (sender) country has limited direct access to the financial systems of the third country, or the recipient country in the corridor is attractive for TF transactions.

Assessment of Vulnerabilities in the Remittance Corridor

Vulnerability in ML/TF risk assessments is defined as the properties of various aspects of the AML/CFT regime that can be exploited by ML/TF threats to enable ML/TF abuse. ML/TF vulnerabilities comprise intrinsic properties of products, services, distribution channels, customer bases, private sector entities, systems, institutions, and jurisdictions (such as weaknesses in AML/CFT-relevant measures and controls) that enable the occurrence of ML/TF risk events. The identification of ML/TF vulnerabilities is based on the examination of specific factors in these areas that are associated with successful ML/TF. The vulnerability indicators can be grouped into categories such as geography, financial and non-financial services and products, levels of informality in various sectors, weaknesses in the AML/CFT systems and the adequacy of existing AML/CFT controls, general levels of corruption, the effectiveness of law enforcement agencies and the criminal justice system, and other characteristics of the jurisdiction that could facilitate successful ML or TF.

Only some ML/TF vulnerabilities are applicable and sufficiently relevant to remittances corridors, allowing a targeted ML/TF vulnerabilities assessment in the CRA. The CRA can limit the analysis of vulnerabilities only to the ones that are relevant to the RSPs and the bilateral remittance corridor. For example, the vulnerability of legal entities can fall outside the scope of the CRA that focuses only on payments by natural persons. Moreover, only some components of vulnerabilities may be relevant for the CRA—for example, instead of analyzing broader international cooperation, the CRA can focus on the effectiveness of cooperation between the two corridor countries. In addition, the CRA can benefit from the analysis of country vulnerabilities not directly related to the remittance corridor but which may affect the reputation of the jurisdiction and the country risk assessments of intermediary financial institutions.

The CRA should consider the extent to which low vulnerability in one corridor country can mitigate the corresponding vulnerability in another corridor country. Some of the vulnerabilities of remittance corridors are applicable to both countries; for example, preventive measures should be applied by the RSPs on both sides of the corridor. The CRA can consider the extent to which effective implementation of preventive measures by one side of the remittance transfer, particularly by the RSP originator, can mitigate the vulnerabilities related to the RSP preventive measures on the other side of the corridor. Some other examples where higher vulnerability in another country can potentially be mitigated to some extent are the effectiveness of criminal justice, supervision, ML/TF detection, and control of corruption.

The CRA should consider the risk profiles of the types of financial institutions that are active in the remittance corridor. Understanding the types of financial institutions involved in the remittance corridor and their market shares as well as how the remittance market between the corridor countries operates can serve as a starting point for the analysis of the corridor vulnerabilities. Analysis of the market shares of individual institutions in the remittance corridor would provide an understanding of possible concentrations of flows in certain RSPs and the degree of specialization of RSPs on the assessed corridor, which is relevant for the ML/TF vulnerabilities assessment. This understanding is useful for the ML/TF vulnerabilities assessment as different categories of financial institutions face different inherent risks of ML/TF misuse,

which can be particularly relevant for countries where new technologies and approaches to remittances are being implemented and "fintech" firms control a material market share.

The CRA should also analyze the role and the importance of banks in the operations of the remittance corridor as providers of banking services to non-bank RSPs. In addition to providing remittance services themselves, banks play a key role in transferring funds to settle RSPs' positions and sometimes provide liquidity services. Significant reliance of non-bank RSPs on the banks to transfer the funds makes the banks key actors in the operations of the remittance corridor. Moreover, as banks conduct their own AML/CFT risk assessments of the RSPs that are their clients, which impacts the level of the banks' scrutiny of RSP operations as well as onboarding and offboarding decisions, banks are also key stakeholders in the CRA.

The vulnerability assessment in the CRA can include the ML/TF vulnerabilities related to the following elements:

Various products and services offered in the remittance corridor. This element of the CRA focuses on the aspects of products and services that are attractive to money launderers due to the opportunities to store value or transfer POC. Analysis of the nature, size, and sophistication of the jurisdiction's products and services facilitates the assessment of the inherent risk that products and services used in the remittance corridor will be exploited for ML/TF purposes. In addition to the traditional use of cash for both accepting and disbursing remittances, other products and services potentially used in the corridor can include debiting or crediting a bank account, other debit instruments such as checks, use of pre-paid products such as electronic money, near cash instruments (travelers checks, money orders, pre-paid cards), and ATM networks. A starting point for the ML vulnerability assessment of the remittance products and services can be the analysis of the data on the overall value and number of remittance transactions across different products and services, which can provide an understanding of the relative importance and potential attractiveness of various remittances products and services to launder POC. The CRA can also explore whether ML vulnerability of remittance products and services is mitigated by RSP policies that limit the value of single or connected cash and non-cash transfers. The CRA can also consider expert perceptions on the relative ease of the use of remittance products and services as well as the identification of relevant remittance products and services in the FATF and FATF-Style Regional Bodies' (FSRBs) ML and TF typologies.

Remittance delivery channels between the two countries. The CRA should analyze various channels to transfer remittances, identifying delivery channels with perceived higher risk, for example due to the possibility of a higher degree of anonymity or low traceability of transfers. As the use of cash is a higher risk delivery channel, which is often prevalent in remittances, the CRA should analyze the share of cash in accepting and disbursing remittances. Similarly, higher risks can be posed by the possibility of conducting transactions on behalf of another person and some types of non-face-to-face transactions. Extensive use of agents for both accepting and disbursing remittances, which also represents a higher risk delivery channel, is common for the RSPs, and the CRA should assess potential ML/TF vulnerabilities of the agent network. The

number of RSPs' branches or agents may also provide a useful insight into potential ML/TF vulnerability of remittance delivery channels. The importance of electronic money, virtual assets, and new financial technologies in remittances has increased in recent years and the CRA should consider whether corresponding delivery channels are sufficiently material to be included in the vulnerability assessment. The CRA would also benefit from an approximation of the share of higher risk remittance products and services in the overall value and number of transactions.

RSP customer base. The CRA should assess the risk posed by various types of RSP customers, distinguishing between higher risk for ML and TF customers. As detailed data on the RSP customer base may not be available, the CRA can rely on expert perceptions or customer surveys to approximate the share of various types of customers. Some of the types of customers that pose higher ML risk are politically exposed persons, their family members and associates, trustees and other persons operating on behalf of others, traders in high value goods, and real estate agents, all under the guise of ordinary individual clients. Based on the TF corridor threat assessment, the CRA can potentially identify types of customers at higher risk of attempting TF in this specific corridor, such as certain types of non-profit organizations that may be misused for TF purposes. Where the origin country of remittances is at risk of raising funds for TF, the CRA can identify the likely profile of donors and recipients, where possible, and approximate whether the share of potentially higher-risk clients is material in the remittance corridor. If certain goods and services are sold or crimes committed to raise funds for TF, the CRA can consider whether the types of customers that pose a higher risk of attempting TF can be identified.

Preventive measures applied by RSPs. The CRA should assess on a sectorial level the extent and effectiveness of preventive measures applied by various types of RSPs operating in the corridor. The CRA can focus on the quality of the implementation of key preventive measures, such as the identification of the originator and the beneficiary of remittance payments, reporting of suspicious transactions (STRs), and record-keeping. The CRA can usefully consider to what extent the effective implementation of preventive measures by one side of the remittance transfer can mitigate the vulnerability of the counterpart financial institution.

- The CRA should assess whether required and accurate originator information, and required beneficiary information, is always immediately available across various types of RSPs. The CRA should also consider the existence of thresholds below which only the names of originators and beneficiaries and a transaction number are required and where the effectiveness of implementation may differ within the remittance corridor. It would be useful to distinguish vulnerabilities of ordering and beneficiary financial institutions due to their different responsibilities. The CRA can also consider such vulnerabilities as the degree of reliability of national identification documents commonly used in the remittance corridor and the ease of conducting transactions using false names or front persons.

- For remittance corridors where TF threats are material, the CRA should assess the quality of implementation of targeted financial sanctions related to the prevention and

suppression of terrorism and terrorist financing. Specifically, the CRA should assess whether RSPs can and are freezing, without delay and without prior notice, the funds of designated persons and entities and the effectiveness of the national mechanism for the timely communication of designations and providing guidance on the corresponding obligations.

- The CRA should consider the vulnerability related to record-keeping and secrecy measures that can lead to a total lack of or insufficient records on transactions in RSPs or the denial of timely access to the records.

- The CRA can also analyze the adequacy of the number of STRs submitted by RSPs regarding payments in the assessed corridor and incorporate feedback from the relevant authorities (e.g., financial intelligence unit, law enforcement agencies) on the quality and the usefulness of these STRs for AML/CFT efforts.

- If there is material reliance on agents in the remittance corridor, the CRA can consider the effectiveness of implementation of preventive measures in the agent network and whether any of these functions are outsourced. Given the impact of low amounts of average remittance transfers on the determination of lower ML risk, it would also be useful to consider any measures RSPs are applying to detect structuring schemes, whereby a large transaction is split into a series of small transactions, intended to circumvent the thresholds and suspicious activity reporting requirements. If the CRA identifies specific ML threats to the remittance corridor, the CRA can include the analysis of the impact of preventive measures for specific customers and activities.

Cross-border cooperation between the two countries. The strength of the cooperation between the two corridor countries improves the ability for both countries to combat criminal flows in the corridor. The CRA can assess whether international cooperation delivers timely access to information and evidence located in the other corridor country and facilitate action against criminals and their assets. In addition to international cooperation in the context of investigation and prosecution of ML and TF offenses, the CRA can cover other relevant aspects of cooperation, such as cooperation between the countries' financial intelligence units (FIUs) and supervisors. In addition to formal cooperation on criminal matters, administrative cooperation and informal sharing of strategic analyses, typologies, information on trends and emerging risks can also assist in mitigating ML/TF risks in the corridor. If the CRA concludes that other countries are relevant for the operations of the corridor, for example due to the involvement of a third country's financial institutions in the settlement of remittance flows, the CRA can assess the relevant aspects of cooperation with these countries (e.g., between the countries' supervisors).

Level of corruption in the society. Corruption is not only a crime that generates proceeds that need to be laundered (ML threat), but also a structural factor, which may undermine the effectiveness of the AML/CFT regime. A high level of staff integrity and ethics and an absence

of corruption in the law enforcement agencies, FIUs, the criminal justice system, supervisory agencies, and other relevant public agencies reduces the probability that ML and TF would be attempted and that ML and TF perpetrators would not be caught and sanctioned. The CRA should also consider the level of corruption in the financial sector, as corruption can potentially compromise the effective application of preventive measures.

Effectiveness of the law enforcement agencies, the FIU, and the criminal justice system. Efforts aimed at overall crime suppression, detecting, and investigating ML and TF activities, analysis and dissemination of quality financial intelligence, and prosecution and sentencing all contribute to reducing ML/TF risk in the corridor. The CRA can focus specifically on the level of effectiveness of the types of efforts mentioned above, as related specifically to the ML/TF threats in the remittance corridor. For example, the CRA can focus on the analysis of STRs from the RSPs specifically related to the remittances in the assessed corridor. An assessment of the effectiveness of these efforts takes into account the powers and resources of the relevant agencies but is mostly based on the performance of these agencies, evidenced by metrics such as the number and complexity of ongoing investigations and cases sent to trial, the number of convictions, and the value of asset recoveries.

Effectiveness of AML/CFT supervision. Effective AML/CFT supervision promotes stronger compliance with AML/CFT measures by RSPs and prevents criminals from controlling an RSP, indirectly contributing to a reduction of ML/TF threats in the corridor. The CRA can focus on the quality of the supervision of the implementation of key preventive measures as identified by the CRA, such as the identification of the originator and the beneficiary of a remittance payment, the reporting of suspicious transactions, and record-keeping. For the corridors with material TF risks, the CRA can also cover supervision of the implementation of TF-specific preventive measures (targeted financial sanctions). The CRA should be focused on the effectiveness of AML/CFT supervision of RSPs and can benefit from engagement with the AML/CFT supervisors for banks, if different, as banks' risk assessments of their RSP clients can provide valuable information, especially given the critical role of banking services in RSP operations.

Deficiencies in legal and regulatory frameworks.[7] The CRA should identify gaps in laws and regulations that are exacerbating in a material way any of the vulnerabilities mentioned above or identified by the CRA. The CRA can focus on the legal framework deficiencies related to the preventive measures applied by RSPs, powers of relevant agencies, secrecy, and international cooperation. Compliance with relevant elements of the FATF Recommendations 6, 9–11, 14, 15, 16, 20, 26, and 27 appears to be particularly relevant.

Assessment of Consequences

[7] FATF and FSRB mutual evaluation and follow-up reports can include valuable information on and reliable assessments of some of the vulnerability factors.

A CRA should consider the economic, political, and social consequences of ML or TF risk events in the remittance corridor. Overall, risk can be analyzed as a function of the likelihood of the risk events occurring and their consequences. The threat and vulnerability assessments described above are combined to deduce the likelihood of occurrence of a risk event, and analysis of the consequences completes the overall risk assessment. Consequences can be defined as the negative economic, political, and social outcomes that result from the risk event occurrence, related to both the acts of ML or TF themselves as well as the longer-term and indirect consequences of ML and TF.

An analysis of the ML/TF consequences examines the impact of ML/TF risk events on national objectives. ML/TF risk events can impact various national objectives in the corridor countries, such as reducing predicate crime and terrorism, protecting the integrity and soundness of the financial system and public institutions, meeting international obligations and foreign policy goals, as well as avoiding misallocation of resources, unfair competition, and destabilizing financial flows. The CRA should evaluate how ML/TF risk events in the assessed remittance corridor can impact national objectives, taking into account the nature of threats and vulnerabilities most likely leading to the ML/TF risk events. The consequence analysis can be derived from the opinions and judgments of officials and other experts as well as from using data relevant to ML/TF consequence indicators, such as the number of economic crime victims, terrorism-related deaths and other terrorism-related damages and costs, and the estimated value of ML/TF transactions relative to the financial sector assets and GDP.

The consequences of ML risk events can be limited for the low value and low volume remittances. CRA can start with an approach to consequence analysis that directly links the amount of funds successfully laundered and the ML consequence—the lower the value of the laundered funds, the lower the ML consequences. In addition, larger-scale criminal activities, which can pose a particularly serious threat to various national objectives, require laundering of funds in significant amounts, which may not be possible in some remittance corridors, for example due to the low overall size of the corridor or RSP operational constrains. Overall, the remittance corridors with low average value and volume of remittances relative to the size of the countries' economies may have a lower level of ML consequences.

A CRA can further consider how ML consequences differ in the remittance corridor for various types of predicate crimes. As social and other harm caused by various types of economic crimes can differ, ML consequences can be driven not only by the amount of funds successfully laundered, but also by the proceeds of the specific categories of crimes laundered. For example, the authorities can conclude that the consequence of laundering proceeds of drug trafficking is higher than laundering proceeds of low scale personal income tax evasion by under-stating income by a foreign worker. To the extent that laundering proceeds of certain types of predicate crimes is more likely in the remittance corridor, the CRA can consider potentially different levels of ML consequences of different types of crimes. The CRA can also consider how other characteristics of a risk event specific to the remittance corridor, such as the types of services and institutions abused for ML/TF, can impact the ML consequences.

Unlike ML, potentially even low amounts of successful TF can have significant consequences. As a result, for the TF consequence analysis, intended use of TF funds can be more important than their amount. The examination of TF consequences, similar to the ML consequences, can be based on the analysis of cost, damage caused, and the significance of outcomes that result from the occurrence of TF, as well as the consideration of the negative impact of TF on the national objectives. The CRA should analyze the nature of possible TF risk events in a corridor, as various TF risk events may impact different national objectives, resulting in different materiality of TF consequences.

TF consequences vary depending on the stage of TF at which the risk event occurred. The CRA should consider the conclusions of TF threat and vulnerability analysis on the likelihood of the payment corridor being abused at any of the TF stages (raising, pass-through, and utilization of funds). For example, if the only material likelihood of abuse of the corridor for TF is related to pass-through of funds to third countries, such a TF risk event can have lower consequences as compared to raising or utilizing funds in the corridor countries. In addition to the likelihood of misuse of a corridor at various TF stages, the CRA can analyze the impact on TF consequences of such factors, if applicable, as terrorists or terrorist organizations that will use the funds, the intended purpose of TF, the profile of donors, the crimes used to raise funds, and the source and the destination countries for pass-through TF.

A CRA also needs to consider the potential consequences of applying risk-mitigating measures that are incommensurate with the ML/TF risk in the remittance corridor. A risk-based approach to designing and implementing a jurisdiction's AML/CFT regime allows for the efficient use of scarce public- and private-sector resources. For a CRA, it is important to assess whether measures to prevent or mitigate ML and TF are commensurate to the risks identified in the corridor and to identify the consequences of not applying the risk-based approach appropriately, resulting in the application of stricter risk-mitigating measures than are warranted by the identified level of risk. This is an important consideration as it is recognized that applying risk-mitigating measures has associated compliance and other cost impacts on the private sector as well as regulatory, supervisory, and enforcement cost impacts on the public sector.

The application of regular or enhanced risk-mitigating measures to remittance corridors with lower ML/TF risks increases costs and leads to unintended AML/CFT-relevant consequences. Increased compliance costs resulting from treating a remittances corridor as posing a more significant ML/TF risk than warranted impose higher barriers of entry for RSPs and may reduce competition, thus increasing costs for the sector that is in most cases important to achieving national objectives in the areas of social, labor, and foreign policies. In addition, as non-bank RSPs mostly rely on banks to access financial sector services to facilitate their operations, applying an insufficiently risk-sensitive or a blanket policy to all remittances can result in difficulties for the non-bank RSPs, even in the lower risk payment corridors, in establishing or maintaining access to banking services. The CRA should also consider the consequences of an ML/TF risk event on the reputation of financial institutions—there may be

no negative consequences (e.g., reputational, pecuniary) for the RSPs and banks that facilitated the remittances if required ML/TF measures were applied appropriately.

The CRA can also consider the riskiness of informal remittance channels that are becoming more attractive due to the application of risk-mitigating measures that are not commensurate to the identified risks in the formal channels. To the extent that additional compliance costs resulting from the inappropriate risk-insensitive application of ML/TF mitigating measures in the formal sector are passed on to the clients, remittances are more likely to be channeled through informal remittance mechanisms. Various alternative channels to transfer remittances can include hawala-type networks, cash couriers, and barter exchanges, and the CRA can take into account the informal remittance channels that exist in the country and the relative level of ML/TF risk associated with each remittance channel. In this context, the CRA can assess structural factors that can exacerbate or mitigate risks related to informal remittance channels, such as cash border controls and the extent of the country's cash-based economy and informal sector. The CRA can analyze AML/CFT consequences of such potential shifts to informal remittances mechanisms, including difficulties in detecting, tracing, and confiscating proceeds of crime and funds intended for terrorists. Overall, the CRA can benefit from a discussion of the importance of balancing the mitigation of ML/TF risks present in a lower-risk remittances corridor against the potential negative consequences resulting from inappropriately applying risk-mitigating measures that are not commensurate with the identified risks.

Conclusions

Consolidation of the ML/TF threats, vulnerabilities, likelihood, and consequences will determine the overall ML/TF risk level for the assessed remittance corridor. The first step involves understanding the ML/TF threat indicators originating from domestic as well as foreign sources for the remittance corridor as discussed in Section 4 of the report. Similarly, the second step will determine the overall ML/TF vulnerabilities of the remittance corridor, which is a function of the inherent vulnerabilities and factors such as products, channels, and customers and the effectiveness of preventive measures as outlined in Section 5 of the report. The threat and vulnerability assessments are combined to deduce the likelihood of the occurrence of a risk event. An analysis of direct and indirect short- and long-term negative consequences of the occurrence of a risk event determines the overall risk of the remittance corridor as discussed in detail in Section 6 of the report. Overall, ML/TF risk can be analyzed as a function of the likelihood of the ML/TF risk events occurring and their consequences. Although the CRA is based mainly on the assessment of inherent risks, some control factors and monetary thresholds or restrictions on users may be integral elements that define the risk associated with the remittance corridor for purposes of making the SRC determination.

In some instances, the ex-ante perception of lower risk of the remittance corridor will not be confirmed by the CRA. Although "lower risk" is a desired situation in the context of a CRA, the assessments may result in medium or higher ML/TF risks. For an SRC, both ML and TF risks need to be "lower" as either of these categories being assessed as medium or higher may undermine the safety of the corridor. However, even if the overall ML or TF risk level of the remittance corridor is medium or high, some sub-categories of remittances can still be lower risk. Therefore, in some instances, the CRA should be expanded to include more granular assessments of sub-categories.

Based on the CRA conclusions, certain remittance activities can be insulated and designated as an SRC. The CRA will provide a granular understanding of the main factors that drive the ML/TF risks, allowing targeted identification of the threats or vulnerabilities that contribute the most to the ML/TF risks in the corridor. In cases where the overall remittance corridor does not pose a sufficiently lower risk, the authorities can use the CRA's detailed analysis of various risk factors in the corridor to isolate products, delivery channels, types of RSPs, and customers that pose lower risk. An SRC can then be achieved by imposing a combination of monetary thresholds and some restrictions on the riskiest type of remittance activities in the corridor that can be practically distinguished and isolated, thereby achieving a lower level of risk at the jurisdictional level. The monetary threshold can apply to both single occasional transactions as well as the annual value of transactions.

Establishing the lower risk nature of the remittance corridor would allow a prioritization of the risk mitigation measures by RSPs, their banks, and correspondent banks. The CRA will assist RSPs to accurately identify and assess ML/TF risks related to their operations, allowing the effective implementation of a risk-based approach by the RSPs in the application of

AML/CFT preventive measures. For example, understanding the threats, vulnerabilities, and risk events specific to the remittance corridors would allow the RSPs to identify and report suspicious transactions more effectively. The CRA conducted by the authorities represents an important source of information for the RSPs as these assessments are based on information, some of which may not be available to the private sector, notably related to TF risks. The CRA is also particularly useful to smaller RSPs and those that do not have the capacity to conduct adequate risk assessments, thereby enriching RSPs' understanding of ML/TF risks in their remittance corridors. The CRA will also assist banks to conduct accurate risk assessments of their business relationships with RSPs operating in the SRC and with respondent banks that facilitate the corridor remittance payments.

It is important that CRA findings and conclusions are internalized by relevant AML/CFT authorities, in particular by AML/CFT supervisors. AML/CFT supervisors need to incorporate the results of the CRA into their supervisory strategy and activities, ensuring that their level of attention to RSPs' activities in the SRC is commensurate with the identified risk. Supervisors should also communicate their supervisory expectations regarding the extent and intensity of risk mitigating measures to be applied by RSPs, for example by providing examples of what documents are acceptable for identification and verification of customers in the corridor context. Considering the important role of banks in the settlement of positions by RSPs, the CRA conclusions should also be taken into account by banking supervisors in their guidance on and assessment of the adequacy of the bank's management of ML/TF risks associated with RSP clients. In the corridor countries where financial institutions in third countries facilitate remittance payments, the results of the CRA can be usefully communicated to the supervisors of the corresponding financial institutions to inform their risk-based approach to AML/CFT supervision. Some countries may decide to formalize the SRC in a regulation/secondary legislation, which can provide additional legal certainty to the private sector. Such regulation can define the SRC based on the conclusions of the CRA, outlining the corridor countries, monetary thresholds, eligible products, delivery channels, types of RSPs, and customers as well as simplified measures or exceptions that can be applied.

The CRA would also allow a prioritization of the risk mitigation measures at the national level to achieve lower ML/TF risks for an SRC. Some of the identified threats and vulnerabilities may require efforts at the national level, while other vulnerabilities can be addressed with specific measures by a single agency. For example, strengthening the supervision of RSPs and enhancing key preventive measures identified in the CRA as a vulnerability can contribute to the reaching of a lower level of risk in the remittance corridor. For the recipient countries with significant reliance on remittances, the CRA can provide a roadmap of the aspects of their AML/CFT regime which need to be strengthened to lower ML/TF risks.

For safe, lower risk remittance corridors, the customer due diligence requirements can be simplified in a risk-based manner. RSPs can be allowed to simplify some of the customer due diligence measures commensurate with the lower risk factors as identified by the CRA. For lower risk remittance transfers, such simplified due diligence measures can consist of some basic

controls that may include identification (and verification) of originator, beneficiary, and suspicious transactions; monitoring against the targeted financial sanctions lists for terrorism and TF; and the prohibition against structuring.[8]

The CRA conclusions may also be used to exempt RSPs from some AML/CFT requirements. If the CRA identified absolute and proven low ML and TF risks, countries may consider exemptions from certain AML/CFT requirements. In such "proven low-risk scenarios," application of the full range of AML/CFT measures, in addition to the SRC required simplified CDD measures, to the RSPs may not be in line with risks in the remittance corridor.

Streamlined and centralized processes may facilitate AML/CFT compliance and reduce costs. Leveraging IT technologies, countries can establish central electronic know your customer (e-KYC) and transaction databases which can facilitate faster and more efficient verification of ID information; the development of customer profiles; and the monitoring of politically exposed persons (PEPs), international and national lists under UN Security Council TF Resolutions, and unusual and suspicious transactions. Such industry-wide solutions can have a significant impact on reducing remittance costs.

A handful of regulators are providing relief from liability to financial institutions in low risk scenarios/transactions. Current examples[9] of safe harbor policies have been focused on customer identification and verification and relate to breaches that are administrative in nature. These safe harbors have been provided to incentivize continuing operations of bank accounts, information exchange, simplified due diligence, and application of other AML/CFT measures. In the context of safe remittance corridors, one country is considering introducing similar types of liability protections in lower risk scenarios for RSPs, under certain conditions, including that all simplified measures required in the safe payment corridor (e.g., low amounts, identity verified, customers monitored against relevant lists) are fully implemented. This country is also reviewing extending such liability protections to banks with RSP clients, provided that the banks implement

[8] FATF Interpretive Note to Recommendation 10 contains useful information on the ML/TF lower risk situations and examples of possible simplified CDD measures.

[9] For more information about the case of New Zealand please see https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/guidance-and-publications/4512701.pdf?la=en&revision=089b99ec-7b95-45e9-a415-0091c12cc8dd. The New Zealand example is also useful as it is mentioned in the 2017 FATF guidance on AML/CFT measures and financial inclusion: https://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

Australia also has safe harbor policies for the lower/medium risk customers' identification and verification: https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/customer-identification-and-verification-easy-reference-guide.

The US AML Act of 2020 establishes a safe harbor from the Banking Secrecy Act (BSA) liability and from adverse supervisory action for maintaining accounts on the basis of law enforcement "keep open" letters. Before that, Section 314(b) of the Patriot Act and its implementing regulations provided a limited safe harbor for financial institutions to share information with one another in order to better identify and report potential money laundering or terrorist activities.

measures to ensure that RSP clients are operating strictly in the safe payment corridor and applying the required simplified measures.

The CRA can be instrumental in ensuring the consistency of the intensity of national AML/CFT measures for the same level of risk across various sectors and products. Using a methodology comparable to the one used in the national or sectorial risk assessment to conduct the CRA would ensure that the same levels of risks are treated similarly. If the corridor countries allow for exemptions or simplified due diligence measures based on the results of the national risk assessment, countries can compare the level of risk identified in the remittance corridor by the CRA with the exempted activities or where simplified due diligence is allowed. It is also important to compare the level of risk and benchmark the CRA against other corridors or overall cross-border remittance payments, which will provide additional insight into the relative level of ML/TF risk of the assessed corridor and whether the measures applied are consistent with the risk.

ANNEX 1. Possible Data and Information Sources for a Corridor Risk Assessment

a) Quantitative Data Sources:

- Granular data on international funds transfers undertaken by all remittance service providers in the assessed remittance corridor. If this data is not readily available, data collection specifically for the CRA can be considered.
- Statistics on suspicious transaction reports (STRs) and transaction threshold reports (TTRs) submitted by remittance service providers to the financial intelligence unit in the assessed remittance corridor.
- Data on money laundering cases (law enforcement database, Prosecutor's Office database, Financial Intelligence Unit database) and ML typologies in the assessed remittance corridor.
- Data on terrorist financing cases (law enforcement database, Prosecutor's Office database, Financial Intelligence Unit database) and TF typologies in the assessed remittance corridor.
- Statistics on ML- and TF-related international legal assistance requests made and received by the countries in the assessed remittance corridor.
- Enforcement and intelligence data on sources of terrorism threats, terrorism financing threats, as well as financial flows related to the assessed remittance corridor.
- Enforcement data on the most relevant predicate offenses for money laundering in the assessed remittance corridor.
- Information on the national identification infrastructure database and its suitability and availability for ID verification purposes in the assessed remittance corridor.
- Statistics concerning the frequency of cases involving the use of fraudulent ID documents in the assessed remittance corridor.
- Information on the quality and effectiveness of customer due diligence (CDD) measures, transaction monitoring systems, and other AML/CFT systems and processes in place for all the remittance service providers in the assessed remittance corridor.
- Data on customers, products, delivery channels, and transactions (value and volume of transactions, use of cash) profile for all remittance service providers in the assessed remittance corridor.
- Data and criminal intelligence reports on ML/TF threats from governmental and public sources in the assessed remittance corridor.

- Data/information on the effectiveness of supervisors, law enforcement agencies, and the criminal justice system (overall crime suppression, detecting ML and TF, analysis and dissemination of financial intelligence, prosecution and sentencing) in the assessed remittance corridor.

- Data on the effectiveness of the AML/CFT controls by the private sector.

b) Qualitative Data Sources:

- Findings from the mutual evaluation reports of the Financial Action Task Force (FATF) and FATF-style regional bodies (FSRBs) can be included, especially when they provide information on the prevalence and details of predicate offenses and money laundering associated with remittance service providers for the assessed remittance corridor.

- National ML/TF risk assessment reports of both the countries in the assessed remittance corridor. Sectoral risk assessments for the relevant sectors (such as money or value transfer services (MVTS), money service businesses (MSBs), electronic money issuers, and banks). Institutional risk assessment reports that are available to the supervisory authorities.

- Reports by international organizations (e.g., United Nations, World Bank Group, International Monetary Fund, World Customs Organization, and World Trade Organization) on the crime environment and ML/TF trends and illicit financial flows in the assessed remittance corridor.

- Interviews and focus group meetings with relevant AML/CFT authorities, police, law enforcement agencies, and criminal intelligence agencies regarding ML/TF cases, trends, and quality of AML/CFT supervision in respect to the assessed remittance corridor.

- Consultations with remittance service providers, industry experts, and industry association on ML/TF trends, methodologies, AML/CFT systems, and the effectiveness of supervision and the challenges encountered in doing business in the assessed remittance corridor.

- Surveys of the relevant AML/CFT authorities, service providers, private sector, NGOs, immigrant communities, and the households that depends on remittances in the assessed remittance corridor.

- Literature on remittance businesses in the assessed remittance corridor.

- Information on ML/TF methods, typologies, and trends collected from informal credible sources for the assessed remittance corridor.

- Credible news reports and other public information on the assessed remittance corridor.