Anti-money laundering guidance for remittance service providers

304 E 45th Street,
New York, United States

Email: info@uncdf.org

ACKNOWLEDGMENTS

On behalf of the migrant women and men originating from, and receiving remittances in, their wider communities in least developed countries, the UNCDF Migrant Money programme team would like to thank the many partners and collaborators who are contributing to our efforts to advance the work on challenges and frictions facing remittance flows. This appreciation is not their endorsement of this paper and is extended to many stakeholders, including programme staff, implementation partners, knowledge leaders, expert influencers, wider global advocates and advocacy organizations, United Nations colleagues, collaborators in the wider fields of international and development finance and the financial and remittance industries, research participants, regulatory and policymaking leaders, and many other individual or organizational stakeholders.

The drafting of this Anti-Money Laundering Guidance for Remittance Service Providers was led by Mercy W Buku, Legal, Risk Management, and Digital Financial Services Consultant. Invaluable inputs and support were also made by Albert Mkenda, Bisamaza Mukankunga, and Doreen Ahimbisibwe. Additionally, Djeinaba Kane, Jacqueline Jumah, and Tewodros Besrat from AfricaNenda, along with Amadou Cisse and Lydia Kinyanjui from the African Institute of Remittances (AIR), offered invaluable insights. Officials from the Central Banks of the ECCAS and IGAD Member States also played a crucial role in this process. Amil Aneja and Eliamringi Mandari provided overall guidance and coordination.

The authors would also like to thank John Powell and Justine De Smet for editorial and design support.

The UNCDF Migrant Money programme has been made possible by the generous funding support from the Swiss Agency for Development and Cooperation and from the Swedish International Development Cooperation Agency. This work is a product of the staff of the UNCDF with external contributions. The findings, interpretations, and conclusions expressed do not necessarily reflect the views of the UNCDF, its executive board and donors, or the governments they represent. UNCDF does not guarantee the accuracy of the data included in this work.

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS **V**

EXECUTIVE SUMMARY **VI**

PART I - INTRODUCTION **9**
Applicability *9*
Interpretation *9*
The Money Laundering Process, Terrorism and Proliferation Financing *10*
Types of Remittance Channels *11*
Vulnerability of RSPs to Money Laundering and Terrorist Financing Activity *11*

PART II - GENERAL PROVISIONS FOR COMBATTING MONEY LAUNDERING AND THE FINANCING OF TERRORISM **13**
FATF Recommendations 13

PART III - AML/CFT SYSTEMS AND CONTROLS **14**
AML/CFT Programme *14*
AML/CFT Policies and Procedures *14*
Customer Due Diligence *14*
Risk-based Approach to Combatting Money Laundering and Terrorist Financing *16*
Enhanced Due Diligence *17*
Transaction Monitoring *17*
Sanction Screening *18*
Suspicious Transaction Reporting *18*
Tipping Off *19*
Traning of Employees, Third Parties, and Agents *19*
Record-Keeping *19*
Additional Measures *20*
Roles and Responsibilities for the AML/CFT Programme *20*
General Responsibilities of RSPs *23*

PART IV - GENERAL DISCLOSURES AND CUSTOMER PROTECTION **24**
Corporate Legal Personality and Goverance *24*
Disclosure of Organizational Structure and Operations *24*
Audit, Inspecting, and Supervision *25*
Fair Market Practices and Customer Protection *25*
Data Protection *25*

KEY REFERENCES **26**

APPENDIXES **27**

ACRONYMS AND ABBREVIATIONS

AML	anti-Money Laundering
AML/CFT	anti-money laundering/combating the financing of terrorism
ATM	automatic teller machine
CDD	customer due diligence
CFT	combatting the financing of terrorism
ECCAS	Economic Community of Central African States
EDD	enhanced due diligence
e-KYC	electronic know your customer
FATF	Financial Action Task Force
FIU	Financial intelligence unit
ID	identification document
IGAD	Intergovernmental Authority on Development
KYC	know your customer
ML	money laundering
MLRO	money laundering reporting officer
ML/TF	money laundering/terrorist financing
MVTS	money or value transfer services
NPPS	new payment products and services
PEP	politically exposed person
RBA	risk-based approach
RSP	remittance service provider
STR	suspicious transaction report
SDD	simplified due diligence
TF	terrorism financing
UN	United Nations
UNCDF	United Nations Capital Development Fund

EXECUTIVE SUMMARY

UNCDF's Migration and Remittances for Development Programme, or the Programme, aims to contribute to sustainable development by making remittances more accessible and affordable while helping build resilience for migrants and their families. For remittance service providers (RSPs), the Programme seeks to build the capacity to understand the financial needs and preferences of migrants and their families and design and deliver responsive products considering gender.

AML/CFT regulatory frameworks have been in place across most countries, and these countries are committed to improving their AML/CFT regimes. Most regulatory frameworks cover vital AML/CFT aspects, including cross-border cash transportation, bearer negotiable instruments, and financial transaction transparency. The frameworks also specify rules, procedures, and conditions for conducting CDD and/or KYC processes for all financial services. However, a lack of clarity regarding regulatory expectations and burdens, including compliance with sanctions, sometimes leads big banks from dealing with smaller players in the market and customers perceived as high risk. Moreover, existing AML/CFT frameworks lack standardized and transparent licensing requirements for international mobile money transfers (incoming and outgoing) and criteria for obtaining licenses to connect new corridors. Additionally, these regulations lack risk-based transaction limits, and mobile wallet balance and transaction limits fluctuate between international and domestic transactions.

Despite risk variations and country-specific environments, the FATF principles are frequently interpreted or applied differently, resulting in inconsistent supervisory practices. The AML/CFT regulatory frameworks do not treat low-risk money remitters and/or small-value remittances differently. Different documentation requirements and interpretations of the risk-based approach, with certain countries allowing streamlined CDD in a constrained and prescribed number of circumstances. For instance, some countries collect the beneficiary's name, address, account number, original government-issued IDs, reference number, work permits, tax identification numbers, and the personal information of the remittance sender. In some countries, acceptable IDs are valid and original government-issued documents, including national identity cards, refugee cards, birth certificates, passports, driving licenses, and employment cards, regardless of the sum involved. These pieces of identification must be copied for remittance service providers' records. Many women and men migrants encounter additional obstacles because of the internal policies and practices of RSPs, such as asking customers to provide additional documents that may not be legally prescribed. Asking customers to present multiple documents for KYC could be a disincentive, especially for self-employed individuals in the informal sectors and women, who comprise over half of the low-income countries' informal traders.

Checking documentary addresses hinders access to remittance services, especially for women and men migrants on the move and who lack the required documentary proof of address. Countries use different address formats, and in some instances, RSPs disagree on what constitutes a legitimate address. Similarly, while some countries require a payee's full name without any initials, others accept names with initials included. Factors such as these result in further complications and incompatible IT systems.
Additional challenges exist in interpreting and implementing data protection and privacy regulations, sometimes producing conflicts with AML regulations.

Another divergent practice is the prohibition of cash deposits from migrants to third-party accounts, including local transfers made by 'walk-in' customers or those without accounts. This is a customer barrier because, in such cases, the migrant's purpose may be to send money rather than open an account with the RSP.

Aside from FATF rules, governments have national security objectives or a foreign policy agenda regarding CDD. At the same time, each country wishes to maintain its correspondent banking relationships while avoiding de-risking[1] at the expense of restricting relationships with countries perceived as high-risk jurisdictions. There have been instances where some remittance service providers received notices of termination of correspondent banking relationships from international banks without explanations. In this regard, big remittance service providers, especially banks, sometimes avoid dealing with customers, both individuals and small remittance service providers, that are perceived as high risk because of low profitability and the possibility of being de-risked. Low profitability may result from the requirement to invest additional resources for implementing AML/CFT compliance measures and systems for high-risk customers and the possibility of heavy fines in case of AML/CFT screening failures.

All these factors, primarily caused by the inconsistent interpretation and disjointed implementation of the FATF recommendations on AML/CFT regulations, complicate remittance flows, contributing to the four main challenges facing remittances, namely high costs, limited speed, difficult access, and opaque transactions. The high cost of remittances is the primary consequence of divergent AML/CFT policy frameworks and practices. [2] This is likely to exclude users of remittance services from the regulated channels, increasing their vulnerability to sources of money laundering and the financing of terrorism, such as corruption, human trafficking, and organized crime.

Lack of focused cooperation and collaboration wastes resources and makes it even harder for RSPs to provide access to more efficient services at low costs. Negligible collaboration and harmonization and the inability to rely on compliance processes performed by other RSPs mean that incidences of duplication are higher, especially regarding CDD, and the interoperability of payment infrastructures becomes even more difficult.

As technology improves and broadens its scope, countries are adopting and strengthening regulations for licensing and supervising the activities of electronic money issuers, including mobile wallets. Under the

[1] According to the definition used by the Financial Action Task Force (FATF), 'de-risking' is the practice of financial institutions terminating or restricting business relationships indiscriminately with broad categories of customers rather than analysing and managing the risk of clients in a targeted manner, i.e., without careful consideration of their risks and the ability of the financial institutions to mitigate those risks.

[2] FATF, (2021). Cross-Border-Payments. FATF, Paris, France. Website: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/cross-border-payments.html.

Financial Action Task Force (FATF) Recommendations,[3] countries must implement effective risk management frameworks and guidance for accountable institutions[4] (including RSPs) in compliance with AML/CFT legislation without imposing an unwarranted burden on lower-risk RSPs.[5] In this regard, RSPs must implement robust AML/CFT programmes to facilitate compliance with their AML/CFT obligations under relevant AML/CFT Legislation in their countries.[6]

This AML/CFT guidance outlines best practices and processes to guide RSPs in compliance with the FATF recommendations and national AML/CFT legislation.

[3] The Financial Action Task Force is the global standard setting body for AML/CFT Compliance. FATF has developed globally accepted standards for combatting money laundering, terrorist and proliferation financing known as the FATF recommendations.

[4] Also referred to as reporting institutions, reporting entities, or responsible institutions depending on the jurisdiction.

[5] FATF Recommendation 1. This obligation extends to proliferation financing under Recommendation 7.

[6] FATF Recommendation 18.

PART I – INTRODUCTION

Digitally enabled remittance services have increasingly become the most efficient method of sending and receiving remittances. Various market players now use web- and mobile-based applications to send and receive remittances.

Remittance services are potentially at risk of being misused for money laundering and financing terrorism activities. The speed with which a remittance transaction takes place means that these platforms are vulnerable to abuse by those seeking to use them for money laundering and financing terrorism. These guidelines are intended to provide practical guidance to RSPs on dealing with the various money laundering and financing of terrorism risks in their business and assist them in doing business without placing undue restrictions that may lead to the financial exclusion of migrants and their families.

The guidelines cover the AML/CFT measures and controls RSPs should incorporate into their business model and general risk management practices.[7]

RSPs may use these guidelines as a template for establishing internal controls and programmes for managing money laundering and financing of terrorism risks they may face, considering existing regulations for RSPs in the relevant jurisdictions.

APPLICABILITY

These guidelines will apply to the following:

1. Non-bank RSPs and their agents.
2. Money or value transfer service providers, including mobile money and virtual assets service providers.
3. Registered *hawala* money transfer agents

INTERPRETATION

In these Guidelines, except where the context otherwise requires,

Beneficial owner means the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted.

Customer refers to the user of an RSP's services. A customer may be a legal (corporate) entity or a natural (individual) person.

Customer due diligence (CDD) is the process of obtaining and verifying prescribed information to properly identify customers.

[7] The mitigatory measures set out herein should also apply to the mitigation of proliferation financing risks as required by FATF Recommendation 7.

New payment products and services refer to prepaid cards, mobile payments, Internet-based payment services, and virtual assets services within the FATF guidance on the risk-based approach for prepaid cards, mobile payments, Internet-based payment services,[8] and virtual assets and virtual asset service providers.[9]

Remittance Services, in the context of these Guidelines, are cross-border financial services through which cash, cheques, other monetary instruments, or stored value are received. A corresponding sum in cash or other monetary instruments is paid to a designated recipient using a communication, message, transfer, clearing network, or remittance hub. Remittance services are also known as money or value transfer services.

A remittance service provider or RSP is an individual, banks, business or organization that accepts instructions from customers to transfer cash, cheques, other monetary instruments, or stored value to a designated recipient. Non-bank remittance service providers are referred to as money transfer businesses.

Risk-based approach refers to the process of identifying, assessing, and understanding ML/TF risks facing an RSP's business and the application of proportionate measures to mitigate these risks effectively and efficiently.

THE MONEY LAUNDERING PROCESS, TERRORISM AND PROLIFERATION FINANCING

i. Money Laundering is the process of "making dirty money clean". It involves criminals engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.[10]

ii. Such Criminal acts are called predicate or designated offences and can generate huge amounts of money. Examples include but are not limited to corruption and bribery, drug trafficking, terrorist and proliferation financing, illicit wildlife trafficking or poaching, illegal arms sales, counterfeiting, extortion, and cyber-crime.[11]

iii. Money laundering enables criminals to enjoy the financial profits of such crimes without revealing their sources.

iv. Terrorism financing is the financing of terrorism and terrorist acts.

v. Proliferation financing is he provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or

[8] FATF RBA-NPPS-2013.html.

[9] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (fatf-gafi.org)

[10] Also see The FATF Recommendations (fatf-gafi.org)

[11] Also see FATF Glossary (fatf-gafi.org)

use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

vi. Proceeds of crime can be used to fund both terrorism and proliferation financing and other criminal activities.

TYPES OF REMITTANCE CHANNELS

Types of channels used for remittance services include but are not limited to bank money transfer channels, international money remittance channels, mobile money platforms, credit card platforms, Internet applications, and virtual assets platforms.

VULNERABILITY OF REMITTANCE SERVICE PROVIDERS TO MONEY LAUNDERING AND TERRORIST FINANCING ACTIVITY

Remittance services are vulnerable to various risk factors, which make them a target for exploitation by those seeking to use them for money laundering and terrorism financing. A summary of these factors is provided below:

i. ***Speed, portability, and anonymous nature:*** The speed and portability of remittance channels make them attractive to criminals as conduits for money laundering. The anonymous nature of some remittance services means that money launderers can engage third parties to conduct transactions on their behalf and to send or receive money via remittance services to protect the identity of the launderers.

ii. ***Complex nature:*** Technological advances in digital financial services have given rise to a complex domestic and cross-border remittance ecosystem, which creates challenges in supervising online money remittance services and makes it easier for criminals to circumvent identity verification processes.

iii. ***New payment products:*** Certain new payment products,[12] such as prepaid cards, can be used to send and receive money and to withdraw cash from ATMs with funds loaded anonymously over the Internet, e.g., through non-bank remittance applications. Fraudsters can also steal and use Debit and credit cards to transfer funds through legitimate RSPs. These cards can also be used via open-loop remittance systems to transfer money worldwide, pay for goods and services or withdraw cash with no face-to-face transaction requirement. Other remittance channels which can be used as conduits for money laundering are mobile payment and virtual currency platforms, either directly or through linkages to RSP platforms through partnership arrangements.

iv. ***Regulatory risk:*** Supervision of remittance service providers varies depending on jurisdiction, and money launderers may seek to exploit that disparity by moving illegal funds using cross-border

[12] As defined in the FATF Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services FATF RBA-NPPS-2013.html.

remittance services. The lack of communication between supervisory authorities in different countries may make it difficult to track such remittances.

v. *Compliance risk:* The speed and portability of remittance services necessitate RSPs to put in place sophisticated automated real-time transaction monitoring systems to enable them to detect and monitor suspicious money laundering activity. These systems are expensive and require heavy capital expenditure, and not all RSPs can afford them, particularly non-bank RSPs. In recognition of this risk, RSPs are designated reporting entities under the FATF recommendations.

PART II - GENERAL PROVISIONS FOR COMBATTING MONEY LAUNDERING AND THE FINANCING OF TERRORISM

This guidance is based on the FATF recommendations, internationally accepted guidelines issued by the Financial Action Task Force (FATF). Countries should also refer to the provisions of their relevant AML/CFT legislation when developing guidance for the remittances sector.

FATF RECOMMENDATIONS

The FATF Recommendations[13] criminalize the offence of money laundering and terrorist financing and set out various measures to prevent money laundering and terrorist financing. These measures include the following:[14]

a. Know your customer (KYC) and customer due diligence (CDD) at entry level and in ongoing customer relationships (including the establishment of beneficial owners for corporate customers)

b. Transaction monitoring to detect suspicious activity

c. Watchlist screening against FATF-recommended sanction lists to detect possible terrorism financing activity. Examples of such lists include those issued by the United Nations, European Union, His Majesty's Treasury (United Kingdom) and the US Office of Foreign Assets Control

d. Reporting suspicious activity, both internal and regulatory

e. Training of staff on AML awareness

f. Proper record-keeping

g. Sanctions/penalties for non-compliance

With specific reference to RSPs, FATF Recommendation 14 on money or value transfer services requires countries to take appropriate measures to ensure that natural or legal persons providing money or value transfer services (MVTS) are licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

FATF has issued a number of guidance notes, including trend reports detailing AML/CFT risk management processes and encouraging a risk-based approach (RBA) when carrying out due diligence on remittance services customers.[15] The RBA to customer due diligence is set out under Part III herein.

---

13 FATF recommendations 2012 updated March 2022.

14 Recommendations 9-25.

15 References to these guidance notes may be found in the Key References section.

PART III: AML/CFT SYSTEMS AND CONTROLS

This section covers the responsibilities of RSPs, systems, and controls for combatting money laundering and terrorism financing.

AML/CFT PROGRAMME

Designated reporting institutions must have AML compliance programmes with adequate systems and procedures to comply with AML/CFT obligations.

AML/CFT POLICIES AND PROCEDURES

i. An RSP should ensure that it has in place adequate policies, procedures, and controls for managing money laundering and terrorism financing risks. The policies and procedures are living documents and should be subjected to regular effectiveness reviews.
ii. The AML/CFT programme should include the designation of an AML compliance officer (AMLCO) or money laundering reporting officer (MLRO) responsible for internal management and training of money laundering and terrorism financing risk controls and handling reporting obligations. The AML policy must also detail the responsibilities of the board of directors, AML compliance officer, staff and third-party agents for compliance with the law.
iii. An effective AML programme for RSPs will comprise policies and procedures incorporating the following controls:
    a. Customer due diligence for customers, agents, and business partners
    b. Transaction monitoring
    c. Sanction screening
    d. Suspicious activity reporting
    e. Training and awareness for staff, agents, third-party partners, and customers
    f. Risk assessments for products and customers
    g. Agent management and compliance monitoring
    h. Complaints recourse channels and redress mechanisms
    i. Technical controls
    j. Transactional controls for international money transfers, border transfers
    k. Provision of information for ML/TF investigations and law enforcement

CUSTOMER DUE DILIGENCE

i. RSPs are required to undertake customer due diligence (CDD) measures:
    a. when establishing business relations or carrying out occasional or one-off transactions;
    b. for transactions above the designated thresholds ranging from 10,000 to 15,000 US dollars/euros, depending on the jurisdiction;[16]
    c. when sending wire transfers as set out in this guidance;
    d. where there is a suspicion of money laundering or terrorist financing; and

[16] FATF recommendations 10 and 22 prescribe a threshold of 15,000 US dollars/euros for occasional transactions, however many jurisdictions impose a lower threshold of 10,000 US dollars/euros, which is also applicable for reporting purposes.

e. where the RSP doubts the veracity or adequacy of previously obtained customer identification data.

ii. RSPs should implement effective customer due diligence (CDD) to obtain and verify the requisite details to properly identify new customers. These requirements should extend to customers, agents, and business partners. The requisite details may differ from one jurisdiction to another as set out in their AML/CFT laws.

iii. These procedures should at least require RSPs to take reasonable measures to ascertain the identity of all persons seeking to use their services, whether or not the services are offered over the counter or through established accounts, pursuant to FATF Recommendation 14. Such reasonable measures include the following:
   a. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data, or information. Examples of customer due diligence documentation include the following:
      - The name, physical address, and occupation of the person
      - The national identity card or passport or other applicable official identifying document bearing a photograph, including a refugee card or status permit for migrants
      - Such other documentation may be allowed under the relevant legislation.
   b. Identifying the beneficial owner and taking reasonable measures to verify the beneficial owner's identity, such that the RSP is satisfied that it knows who the beneficial owner is and understands the ownership and control structure of the customer.[17] Ultimate ownership or control can be determined by various criteria, including natural persons with shareholding above a minimum percentage[18] or with shareholding or voting arrangements that give them such control or persons in senior management or other positions that influence a company significantly.[19]
   c. Understanding and, where appropriate, obtaining information on the purpose and intended nature of the transaction and business relationship.
   d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout that relationship to ensure that the transactions are consistent with the RSP's knowledge of the customer, their business and risk profile.
   e. Verifying all transactions conducted over the counter or through web-based or mobile applications.
   f. Setting of limits for international and cross-border transactions. Prescribed limits under the FATF Recommendations are 15,000 US dollars/euros. However, lower limits, e.g., 10,000 US dollars/euros, may be set under local legislation.

[17] FATF Recommendation 24 and 25.

[18] The FATF Guidance on Transparency and Beneficial Ownership proposes a threshold of 25 percent. However, the threshold may vary from 10-25 percent depending on the jurisdiction.

[19] FATF Guidance on Transparency and Beneficial Ownership.

iv. The following information should be collected from customers using the RSPs for wire transfers, pursuant to FATF Recommendation 16:
    a. Accurate originator information should include:
        - the name of the originator;
        - the originator account number where such an account is used to process the transaction;
        - the originator's address;
        - national identity/passport number; and
        - date and place of birth.
    b. Accurate beneficiary information which should include:
        - the name of the beneficiary;
        - the beneficiary account number where such an account is used to process the transaction; and
        - a unique transaction reference number to enable tracing of the transaction in the absence of an account number.
    c. The collected information should be kept with the wire transfer or related message throughout the payment chain.

v. Where an RSP establishes customer accounts, it must maintain no anonymous accounts or accounts with fictitious names.

vi. Where it becomes apparent to the RSPs that a customer with an account or person seeking to undertake a single transaction in the case of over-the-counter services is a sanctioned person, it must take steps to cease the business relationship with such person.

RISK-BASED APPROACH TO COMBATTING MONEY LAUNDERING AND TERRORIST FINANCING

i. Under FATF Recommendation 1, the risk-based approach to combat money laundering and terrorist financing refers to adopting **proportionate** risk management processes for dealing with money laundering and terrorist financing risks. This process encompasses recognizing the existence of the risk(s), undertaking an assessment of the risk(s), and developing strategies to manage and mitigate the identified risks. It invariably requires a risk analysis to determine where the money laundering and terrorist financing risks are the greatest. It is in this context RSPs are recommended to share their risk identification, monitoring, and mitigation frameworks with the regulators as a demonstration of their capacity to undertake appropriate ML/FT risk management.

ii. In the context of RSPs, institutions must **identify higher-risk customers, products, and services, including delivery channels and geographical locations.** Higher risk areas should be subject to enhanced procedures, such as enhanced customer due diligence checks and transaction monitoring. It also follows that in instances where risks are low, simplified, or reduced controls may be applied.[20]

[20] FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures (fatf-gafi.org)

iii. The Risk-based approach, however, does **NOT** apply to wire transfers where full due diligence requirements must be met for the transaction's originator and beneficiary.

ENHANCED DUE DILIGENCE

i. According to the FATF guidance, RSPs should perform enhanced due diligence for higher-risk customers, business relationships or transactions and continuously monitor all high-risk customers.

ii. RSPs should identify individual high-risk categories and apply specific and appropriate mitigation measures. Higher risk scenarios include politically exposed persons (PEPs) as defined under the relevant AML/CFT legislation, correspondent banking relationships, and cross-border transactions between known terrorism hot spots.

iii. While applying the proportionality principle, care should be taken to ensure that the customer due diligence procedures established to comply with CDD requirements are not too demanding for customers wishing to use the services of the remittance service provider.

iv. In the circumstances, the enhanced due diligence may take the form of levels (tiers) of CDD, with higher levels requiring the most stringent CDD, further approvals for establishing relationships, and increased levels of review of relationships. The intensity and extensiveness of risk management functions should be proportionate to the nature, scale and complexity of the remittance service provider's activities and money laundering/terrorist financing risk profile.

TRANSACTION MONITORING

i. RSPs are required to take steps to monitor transactions for suspicious activity. Such monitoring enables the early detection of money laundering activity and the consequent taking of steps to prevent and/or deal with such activity.

ii. Suspicious transactions may be detected from actual customer dealings or through monitoring transactions on the remittance platforms.

iii. Under FATF Recommendation 16, RSPs are also required to monitor wire transfers to detect those which lack required originator and/or beneficiary information and take appropriate measures such as freezing actions and prohibition against conducting transactions with designated persons and entities.

iv. Appropriate measures should be implemented to monitor transactions, focusing on high-risk customers. A remittance service provider should establish internal processes to detect suspicious activities and monitor customers and transactions against those activities. Such processes should include documenting internal threshold reporting requirements and relevant suspicious activity indicators and implementing an automated transaction monitoring system.

v. The transaction monitoring system should identify suspicious activity, including smurfing, transactions inconsistent with prior behaviour, transfer of funds to/from high-risk areas, transfer of funds to/from

previously dormant accounts, employee activity on customer/merchant/agent accounts, transactions with no apparent economic value, etc. The transaction monitoring system should also flag transactions that appear to have been deliberately split into small amounts equivalent to 15,000 US dollars/euros (or such lower limit as the case may be) to avoid the requirement of reporting to the relevant financial intelligence unit.

vi. Once a suspicious activity alert is triggered on the system, it is investigated by the AML team. Appropriate action is taken to mitigate the risk, including blocking or reversing the transaction, terminating the business relationship, and reporting the suspicious activity to the relevant financial intelligence unit.

SANCTION SCREENING

i. RSPs should conduct regular watchlist/sanction screening of financial transactions against FATF-recommended sanction lists to detect possible terrorist financing or PEP activity. The sanction lists contain the names of known or suspected terrorists and PEPs.

ii. FATF recommended lists include the United Nations, European Union, His Majesty's Treasury (United Kingdom), and the Office of Foreign Asset Control (USA).

iii. Therefore, it is important to have an automated sanction screening system in place to screen transactions for suspect terrorist or PEP activity. In this regard, the sanction screening tool should simultaneously access all the FATF recommended lists for screening purposes.

iv. RSPs can reduce the costs of automated transaction monitoring tools by exploring partnerships with vendors to access shared transaction monitoring systems and sanction screening databases under multi-licencing arrangements.

v. Examples of categories of high-risk customers in the sanction lists may be found in Appendix C of this guidance.

SUSPICIOUS TRANSACTION REPORTING

i. RSPs and their third-party contractors, remittance hubs and agents should ensure that they have adequate systems, policies, and procedures to undertake suspicious activity reporting. The procedure should incorporate the internal reporting of suspicious activity to the AML compliance officer and externally by the compliance officer to the relevant financial intelligence unit (FIU).

ii. Where an RSP, its third-party contractor, remittance hub, or agent becomes aware of suspicious activities or transactions which indicate possible money laundering or terrorism financing, the RSP must ensure that it is reported to the relevant FIU immediately and within seven days of the date of the transaction or occurrence of the activity considered suspicious.

iii. The Suspicious Activity Report should be made by the AML compliance officer when:
   a. the AML compliance officer suspects the integrity of a transaction; and
   b. when the AML compliance officer knows that a transaction relates to money from a criminal source.

iv. Suspicion should be created in the mind of an alert staff member and or an agent. A single indicator is not necessarily indicative of reasonable grounds for money laundering suspicion. However, if several suspicious indicators or red flags exist during a transaction, it may be worth examining it more closely.

v. When reporting suspicious activity, the AML compliance officer does not need to be certain that a crime has occurred. The requirement to report suspicious activity is based on suspicion and knowledge.
   a. Suspicion – The circumstances of the transaction are so unusual as to create suspicion in the mind of a reasonable person that a crime had been committed.
   b. Knowledge – The circumstances of the transaction are such as to raise the expectation that the person knew or ought to have known that a crime had been committed.

vi. Suspicious activity indicators for money laundering activity in remittance services are set out in Appendices A and B of this guidance.

TIPPING OFF

i. An RSP or its third-party contractors, remittance hubs, or agents must not disclose to the person undertaking a transaction that it suspects the transaction or activity is suspicious. Tipping off occurs where an RSP, its third-party contractor, remittance hub, or agent:
   a. knows or suspects that a suspicious activity report has been made;
   b. makes a disclosure which is likely to prejudice any investigation which might be conducted following the suspicious activity report; or
   c. falsifies, conceals or destroys documents relevant to the investigation or causes the concealment or destruction to happen.

TRAINING OF EMPLOYEES, THIRD PARTIES AND AGENTS

i. The RSP should ensure a robust recruitment and training programme for its employees, third parties, and agents. The training programme should be undertaken frequently to ensure that all staff, including newly on-boarded ones, have been trained and longer-serving staff have had refresher training. The Programme should be the responsibility of the AML compliance officer.

ii. Front-line staff should undergo more frequent training, as should third-party contractors and agents coming into direct contact with customers or managing transaction processing.

RECORD-KEEPING

i. RSPs should keep records of all transactions and reports as required by law for at least seven years or otherwise as prescribed under the relevant AML legislation.

ii. The transaction records and reports should be readily available for regulatory inspection or to assist in investigations.

iii. Records kept should include, where applicable:
   a. customer due diligence information, including originator and beneficiary information for wire transfers;
   b. employee due diligence information;
   c. contracts with third parties, remittance hubs, and agents;
   d. single transaction records;
   e. suspicious transaction reports (STR); and
   f. internal investigation reports.

ADDITIONAL MEASURES

Depending on the size, nature, and complexity of their business, other internal controls that RSPs should consider putting in place include the following:

i. Risk Assessments, i.e., the following:
   a. Undertaking product risk assessments covering new and existing products to identify risks and recommend mitigatory controls on an ongoing basis, including risk-based CDD.
   b. Undertaking divisional risk assessments covering all business operations to identify potential risks which may expose the RSP to ML/TF Risks.
   c. Documenting the risk assessments undertaken under (a) and (b) above.

ii. Compliance monitoring comprising agent management and risk-based compliance checks on branches and agents to confirm compliance with procedures.

iii. Complaints recourse channels to receive and handle customer complaints and facilitate recourse measures, e.g., hotlines for fraud and other complaints.

iv. Technical controls, including independent (external) information system audits to ensure there are appropriate safeguards against cybercrime and hacking, e.g., user access and PIN controls

v. Liaison with law enforcement agencies in providing information, profiling, arresting, and prosecuting suspects.

ROLES AND RESPONSIBILITIES FOR THE AML/CFT PROGRAMME

Board of Directors

The board of directors has overall governance responsibility for the RSP's AML/CFT programme and should have sufficient awareness of relevant risk controls. The board members are required to be "fit and proper" to carry out their AML/CFT responsibilities effectively, based on the following criteria at minimum:

- probity, personal integrity, and reputation; and
- competency and capability

The board has the following key responsibilities:

a. Maintaining accountability and supervising AML/CFT policies, procedures, and control measures
b. Approving AML/CFT policies regarding AML/CFT measures
c. Establishing appropriate mechanisms to ensure the AML/CFT policies are periodically reviewed and assessed
d. Maintaining adequate oversight of the overall AML/CFT measures undertaken by the RSP
e. Defining the lines of authority and responsibility for implementing the AML/CFT measures and ensuring role separation between those implementing the policies and procedures and those enforcing the controls
f. Ensuring an effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF
g. Assessing the implementation of the approved AML/CFT policies through regular reporting and updates by the senior management and audit committee

Key Officers/Senior Management

The senior management is responsible for the execution and implementation of the AML/CFT Programme established and approved by the board of directors, including any legal or regulatory requirements. The senior management is required to be "fit and proper" to carry out their AML/CFT responsibilities effectively, based on the following criteria:

- Probity
- Personal integrity
- Reputational integrity
- Competency
- Capability

Their key roles and responsibilities include the following:

a. Awareness of and understanding the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business.
b. Formulating AML/CFT policies to ensure that they align with the risk profiles, nature of business, complexity, volume of the transactions undertaken by the RSP and its geographical coverage.
c. Establishing appropriate mechanisms and formulating procedures to effectively implement AML/CFT policies and internal controls approved by the board, including the mechanism and procedures to monitor and detect complex and unusual transactions.
d. Ensuring review and proposing the necessary AML/CFT policy enhancements to reflect changes in RSP risk profiles, institutional and group business structure, delivery channels and geographical coverage to the board.

e. Providing timely periodic reporting to the board on the level of ML/TF risks facing a given RSP, the strength and adequacy of risk management, and internal controls implemented.
f. Allocating adequate resources to effectively implement and administer AML/CFT compliance programmes that reflect the size and complexity of the RSP's operations and risk profile.
g. Ensuring all the remedial actions proposed by the Financial intelligence unit and the regulator on AML/CFT compliance issues are implemented.
h. Appointing an AML compliance officer at the management level with sufficient authority and establishing effective compliance mechanisms across the RSP.
i. Providing appropriate AML/CFT training levels for its employees throughout the RSP.
j. Ensuring that there is a proper channel of communication in place to effectively communicate the AML/CFT policies and procedures to all levels of employees.
k. Ensuring that AML/CFT issues raised are addressed promptly.
l. Ensuring the integrity of employees by establishing appropriate employee recruitment and vetting systems.
m. Formulating an AML/CFT training programme for staff, third parties and agents.

AML Compliance Officer

- The AML compliance officer is usually a statutory position provided for under the AML Legislation.
- The AML compliance officer is the point of contact at the RSP level for all matters related to AML/CFT controls, training, and reporting.
- The AML compliance officer must have sufficient knowledge, resources, stature, authority, and seniority within the RSP to participate and effectively implement decisions of the Board and the Senior Management relating to AML/CFT.
- The AML compliance officer is required to be "fit and proper" to conduct AML/CFT responsibilities effectively, based on at least the following criteria:
  - » Probity
  - » Personal integrity
  - » Reputational integrity
  - » Competency
  - » Capability

The AML compliance officer's role includes:

a. ensuring and overseeing the RSP's compliance with the AML/CFT requirements;
b. ensuring proper implementation of the AML/CFT policies;
c. ensuring the appropriate AML/CFT procedures, including CDD, record-keeping, ongoing due diligence, reporting of suspicious transactions and combatting the financing of terrorism, are implemented effectively;
d. ensuring the AML/CFT mechanism is regularly assessed to ensure that it is effective and sufficient to address any change in ML/TF trends;
e. ensuring channels of communication across the organization are appropriately secured, and that information is kept confidential to avoid tipping off;

f. ensuring all employees are aware of the RSP's AML/CFT control measures and have been sufficiently trained;
g. ensuring internally generated suspicious transaction reports are appropriately evaluated before submitted to the Financial intelligence unit;
h. ensuring the identification of ML/TF risks associated with new products or services or arising from the RSP's operational changes, including the introduction of new technology and processes;
i. providing regular management reports to the board and senior management on compliance violations and other pertinent issues
j. acting as the main contact person for the relevant Financial intelligence unit on behalf of the RSP on AML/CFT measures.

GENERAL RESPONSIBILITIES OF REMITTANCE SERVICE PROVIDERS

Managing Operational risks

RSPs are responsible for their organizational management and mitigation of operational risks through procedures and controls. The procedures and controls facilitate monitoring and reporting suspicious activities, verifying customer identity, documenting customer records and establishing internal reporting procedures.

Managing Customer Complaints

RSPs should implement strong operational policies, procedures, and controls to handle and resolve customer complaints. This includes but is not limited to:

a. providing dedicated hotlines for complaints and fraud reporting;
b. recording sufficient information to create an audit trail and storage of records for a minimum period of seven years from the date of the transaction; and
c. providing information on complaint redress mechanisms as set out under Part IV.

Organizational Management: Accountability for Third-Party Contractors, Remittance Hubs and Agents.

a. RSPs should have clear accountability for actions and omissions of third-party contractors, remittance hubs, and agents (where applicable) through appropriate agreements.
b. Adequate contract documents are signed between payment service providers and third parties, remittance hubs, and agents, clearly setting out the roles and obligations of the parties involved in preventing money laundering and terrorism funding.
c. RSPs should regularly supervise compliance with policies, procedures, and controls as stipulated in the agreements to ensure that the requirement to maintain such procedures has been discharged.

PART IV: GENERAL DISCLOSURES AND CUSTOMER PROTECTION

This section covers the general aspects of governance, disclosure, and customer protection.

CORPORATE LEGAL PERSONALITY AND GOVERNANCE

Some elements of digital financial service providers are becoming increasingly involved in money laundering activities, fraud and misuse of customer funds with reckless indifference to the customers they serve. It is necessary to interrogate the corporate governance structures of remittance service providers to assuage any general or specific money laundering or terrorism financing risks associated with the leadership or governance of the remittance service provider.

To this end, an RSP should conduct the following:

i. Provide an updated list of major shareholders, directors and officers of the entity seeking to undertake remittance services business. This aims to ensure that the governance of the RSP is above board and that the key officers and directors meet the relevant "fit and proper" requirements.

ii. Provide a matrix of key related parties or entities, such as holding companies, subsidiaries, sister companies, etc., to disclose material relationships that may impact the performance or governance of the remittance service provider.

DISCLOSURE OF ORGANIZATIONAL STRUCTURES AND OPERATIONS

To protect the market from speculative dealers, RSPs should undertake transparency and disclosure procedures to enable customers to make informed choices on using their services and allow financial regulatory and supervisory authorities to interrogate their business model and associated risks.

To this end, the RSPs should carry out the following:

i. Provide regulators with detailed descriptions of the remittance services. This may take the form of a business plan or a white paper. The detailed description should contain information on the following:
   a. The operations of the RSP.
   b. The organizational structure of the RSP, including any information on the use of agents or outsourced third parties or remittance hubs. Where agents, third parties, or remittance hubs are in use, the RSP should provide adequate information, including the contracts, to the regulator for review.
   c. The RSP governance includes key officers and directors' suitability, capability and integrity.
   d. The risk identification, monitoring and mitigation framework of the RSP.

ii. Communicate to the public its product/service offerings. This may be a published white paper or information memorandum on its website or otherwise publicly available.

AUDIT, INSPECTION AND SUPERVISION

i. RSPs should ensure adequate preparedness for regulatory on-site inspections or supervisory technology-enabled inspection and supervision. To this end, its systems must be capable of being subjected to such audits and inspections.

ii. Depending on the size and complexity of its business and transactional volumes, RSPs should periodically conduct independent information system audits that test the robustness of their systems against external and internal vulnerabilities (cyber-threats) and penetration attempts. The audit reports should be sent to the relevant regulator during inspection visits.

FAIR MARKET PRACTICES AND CUSTOMER PROTECTION

To protect customers and assure customers of the transparency of its remittance services, the remittance service provider should ensure that it publishes information on:

a. fees and charges, including the foreign exchange rate and spread and which party bears the cost;
b. customer terms and conditions in plain language, avoiding jargon, which should be easily available to customers at the point of service, e.g., on its website for web-enabled services, on the mobile application or platform for mobile-based services, and at the counter for over-the-counter remittance services;
c. customer redress mechanisms for both senders and recipients; and
d. complaints handling procedures for both sender and recipient, e.g., dedicated fraud reporting hotlines, contact centre numbers, email or social media handles, escalation matrix for resolution of complaints, etc.

DATA PROTECTION

Customer data must be treated with due care and attention and always with the consent and knowledge of the customer. To this end, the remittance service provider should ensure adherence to the data protection legislative or regulatory framework governing personal data use, processing, and archiving. This should be built into the customer terms and conditions and specific data policies for online or mobile application-based services. Where no data protection rules have been legislated, the remittance service provider should detail how customer data would be handled (protection from abuse, conditions for its use, etc.).

KEY REFERENCES

1. Financial Action Task Force Recommendations (updated March 2022) FATF recommendations.

2. FATF Guidance for a Risk-Based Approach for Money or Value Transfer Services (2016). RBA-money-value-transfer-services.pdf

3. FATF High-Level Principles and Procedures on the Risk-Based Approach (2007). FATF High-Level Principles and Procedures on the Risk-Based Approach.pdf.

4. FATF Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services (2013) FATF RBA-NPPS-2013.html.

5. FATF Methods and Trends Money laundering through money remittance and currency exchange providers (2010) FATF Methods and Trends Money laundering – MVT and CEs.

6. FATF Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (2021) FATF Guidance – RBA - Virtual Assets and VASPS.

7. Proportional risk-based AML/CFT regimes for mobile money: A framework for assessing risk factors and mitigation measures, GSMA (2015) Proportional-risk-based-AMLCFT-regimes-for-mobile-money 2015.

APPENDIX A: SUSPICIOUS ACTIVITY INDICATORS IN REMITTANCE SERVICES

Typical Examples of Suspicious Transactions/Activity for Remittance Services are:

1. A single transaction in a substantial amount or several interrelated transactions in a substantial amount if it is beyond expectations for the customer or the country of the originator.
2. A customer is a beneficiary of two transactions or more where an originator is from a country that does not apply AML/CFT standards. The customer receives funds from one person or more with seemingly no logical connection.
3. A customer is a beneficiary of several transactions from different countries. However, the reasons for them are inconclusive.
4. A customer is a beneficiary of several transactions in a short period, originated by one person or more, without a logical connection between them.
5. A situation where a customer makes a point of withdrawing funds in different RSPs.
6. Frequent transactions or transactions in a substantial amount to/from countries known for drug trafficking or to be transit routes.
7. Transactions not in line with money remittance services so far are not in line with the customer's history.
8. Use of several originators of a transfer, presumably for the same beneficiary.
9. A customer receives funds in small amounts and subsequently originates a further transfer in a substantial amount.
10. A customer receives funds and immediately originates the transfer of the same or approximately the same amount to another person.
11. A customer conducts multiple transactions regularly through money remitters in amounts below the recording threshold prescribed by AML/CFT regulations.
12. One customer or more sends money to the same beneficiary or persons affiliated with the beneficiary to avoid the recording threshold prescribed by internal procedures or regulations of the state authority.
13. When withdrawing received funds, a customer always presents different identification documents.
14. A customer often conducts transactions in a substantial amount, although it is customary for the business involved to use bank accounts rather than prompt money transfers.
15. A customer avoids providing information on transactions. They comment about your requirement to record them, give up on a transaction if they are required to provide additional information or documentation or display any other unusual behaviour.
16. A customer attempts to conduct transactions using unsuitable identification documents, or their credibility is questioned.
17. A customer enters another person's company or receives instructions from another person when conducting a transaction.
18. A customer known to have had a criminal past (known, for example, from publicly available information) or the one with a bad reputation conducts numerous transactions.
19. A transaction in high amounts is paid for in small denominations.

20. Transactions to countries with no visible family, business or any other relation to the client, or the ones which are not usual emigration destinations.

An RSP may wish to refer to:

- FATF Methods and Trends Money laundering through money remittance and currency exchange providers FATF Methods and Trends Money laundering – MVT and CEs.
- FATF Virtual Assets Red Flag Indicators Virtual-Assets-Red-Flag-Indicators.pdf (fatf-gafi.org).

APPENDIX B: SUSPICIOUS ACTIVITY INDICATORS IN MOBILE MONEY SERVICES

Typical Examples of Suspicious transactions/activity for mobile money include the following:

- Multiple registrations of SIMs using one ID
- Multiple registrations of mobile money wallets with no economic rationale
- Failure to provide identification/use of fake ID
- Frequent deposits or withdrawals with no apparent business source
- Multiple accounts with numerous deposits hitting the transaction limit
- Accounts with high volume/high-value activity
- Large deposits and balances without justification
- Deposits and immediate requests for withdrawal or transfer
- Multiple/inconsistent deposits and withdrawal activity
- Remote withdrawals and frequent direct deposits
- Multiple accounts with numerous deposits hitting the transaction limit
- Accounts with high volume/high-value activity
- Large deposits and balances without justification
- Deposits and immediate requests for withdrawal or transfer
- A customer attempting to transact on behalf of other customers
- A customer making a series of daily deposits through different agents
- Suspicious/frequent international/cross-border money transfers
- Stated customer occupation is not in line with the level of activity in mobile wallet

APPENDIX C: CATEGORIES OF HIGH-RISK CUSTOMERS

High-risk customers are categorized in the sanction lists as follows:

- Sanctioned individuals and entities - These are the individuals and entities appearing in the sanction lists. This list is updated daily in the system. RSPs are not permitted to open accounts for these customers.
- Politically or publicly exposed persons (PEPs) are politicians or persons holding senior government positions. New accounts for these customers should be authorized by senior management. No automatic account activation and the accounts should be monitored closely for suspicious activity (e.g., unusually large deposits and multiple transfers without economic rationale).
- Prominent and influential persons (PIPs) are not politicians but are known to be influential. These should be segmented from the other customers to make continuous monitoring easier.
- Jurisdictions with inadequate AML/CFT regimes.

These categories are updated by FATF regularly.

ABOUT UNCDF

UNCDF mobilizes and catalyzes an increase in capital flows for SDG impactful investments to Member States, especially Least Developed Countries, contributing to sustainable economic growth and equitable prosperity.

In partnership with UN entities and development partners, UNCDF delivers scalable, blended finance solutions to drive systemic change, pave the way for commercial finance, and contribute to the SDGs. We support market development by enabling entities to access finance in high-risk environments by deploying financial instruments, mechanisms and advisory.

For more information, please contact:
Albert Mkenda
albert.mkenda@uncdf.org

Follow @UNCDF