FATF

FATF GUIDANCE

Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures

June 2025

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

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

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

Citing reference:

FATF (2025), *Guidance on Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures,* FATF, Paris, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Financialinclusionandnpoissues/guidance-financial-inclusion-aml-tf-measures.html

Photocredit coverphoto: Melnikov Dmitriy/Shutterstock.com

Table of Contents

Abbreviations and acronyms

	Definition
AML/CFT	Anti-money laundering and countering the financing of terrorism
CDD	Customer due diligence
DFS	Digital financial services
DNFBPs	Designated Non-Financial Business or Professions
DPI	Digital public infrastructure
EDD	Enhanced customer due diligence
FATF	Financial Action Task Force
FI	Financial institution
FIRM	Financial Inclusion Product Risk Assessment Module
FIU	Financial intelligence unit
ID	Identity
IMF	International Monetary Fund
INR.	Interpretive Note to Recommendation
KYC	Know your customer
ML	Money laundering
MVTS	Money or value transfer services
NPO	Non-profit organisation
NRA	National risk assessment
PF	Proliferation financing
RBA	Risk-based approach
R.	Recommendation
SDD	Simplified customer due diligence
TF	Terrorist financing
UN	United Nations
VASPs	Virtual asset service providers

Executive Summary

The promotion of regulated financial systems and services is central to any effective and comprehensive AML/CFT regime. However, applying an overly cautious approach to anti-money laundering/countering the financing of terrorism (AML/CFT) safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the regulated financial system. Advancing financial inclusion is a long-standing goal for the Financial Action Task Force (FATF)and the risk-based approach (RBA) is central to FATF's approach to financial inclusion.

The FATF has updated its Guidance on financial inclusion to provide support in designing AML/CFT measures that meet the national goal of financial inclusion, without compromising the measures that exist for the purpose of combating crime. The main aims of the document are to develop a common understanding of the FATF Standards[1] that are relevant when promoting financial inclusion and underscore the flexibility that the Standards offer, in particular the RBA), enabling jurisdictions to craft effective and proportionate controls.

The Guidance paper was initially published in 2011 and was revised and enhanced in 2013 and 2017 respectively. In 2025, the Guidance is further updated based on the revisions to Recommendation 1 and Interpretative Notes to Recommendations 1, 10 and 15 to encourage countries to promote financial inclusion and take a proportionate RBA in implementation. It is non-binding and does not override the purview of national authorities. It highlights the need to better inform the countries and regulated entities of the financial inclusion dimension of the AML/CFT frameworks.

The Guidance primarily focuses on facilitating access to and usage of formal services by unserved and underserved persons. These include unserved persons in low-income and rural groups or in fragile contexts who may lack easy means to verify their identities or the funds to access costly regulated services, as well as those who have limited access to regulated financial services and products (thereafter simplified as financial services), and are viewed as underserved. It extensively explores the initiatives taken in developing countries, where the challenge of pursuing financial inclusion is the greatest. The analysis is based on a number of countries' experiences and initiatives to address financial inclusion within the AML/CFT context.

The Guidance is based on the important assumption that unserved and underserved persons, in both developing and developed countries, should not be automatically classified as presenting lower risk for ML/TF, but that appropriate risk assessments often conclude that they present a lower risk.

The Guidance gives an overview of the RBA which is a central element of the FATF Standards. The greater recognition of a risk-sensitive approach to implementing AML/CFT measures – including in particular an approach that takes into consideration the risks of financial exclusion and the benefits of bringing people into the regulated financial system – will be a key step for countries that wish to build a more inclusive financial system. The application of the RBA will be based on an assessment of risks which will help countries and regulated entities understand, identify and assess risks and apply mitigation and management measures that are risk sensitive. This includes both enhanced measures for higher risk scenarios and simplified measures for lower risk situations.

The Guidance outlines ways in which policymakers, supervisors and regulated entities can leverage the flexibility embedded in the RBA to foster financial inclusion while safeguarding financial integrity. Examples of best practices in applying the RBA, including enabling efforts and encouragement from supervisors, and simplified measures and exemptions adopted by regulated

1 The FATF Standards comprise the FATF Recommendations and their Interpretive Notes.

entities can be found in the Annex. These examples aim to provide helpful reference and insights for countries and regulated entities seeking to enhance their implementation of RBA and ensure an effective and inclusive AML/CFT regime.

The FATF will continue to work to ensure that financial inclusion and AML/CFT objectives mutually reinforce each other.

Introduction – Background and Context

The FATF and Financial Inclusion

Mutually Reinforcing Goals

1. The Financial Action Task Force (FATF) is committed to supporting financial inclusion[2], and has long considered financial inclusion and anti-money laundering/countering the financing of terrorism (AML/CFT) measures as mutually supportive and complementary policy objectives.[3] Enabling more individuals and entities to access and use regulated financial services increases the reach and effectiveness of AML/CFT measures and enhances financial sector transparency and integrity.[4] Conversely, financial exclusion represents a real risk to achieving effective implementation of the FATF Standards.[5]

FATF Financial Inclusion Efforts

2. Recognising that AML/CFT measures can be implemented in a way that undermines financial inclusion, the FATF was the first financial sector intergovernmental standards setting body to integrate financial inclusion into its mission.[6] In 2011, the FATF adopted its first Guidance on "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion" (the Financial Inclusion Guidance),[7] which identified financial exclusion as an important money laundering (ML)/terrorist financing (TF) risk.

3. In 2012, the FATF adopted revised Recommendations, which included strengthening and clarifying the FATF's risk-based approach (RBA) to AML/CFT regulation, supervision, and compliance and made the RBA mandatory. In 2013, the FATF revised the 2011 Financial Inclusion Guidance to reflect the RBA and provide support for designing AML/CFT measures that advance financial inclusion without compromising their effectiveness.[8]

4. In 2017, the FATF adopted an extensive supplement to the 2013 Financial Inclusion Guidance, with country examples of simplified customer due diligence (SDD) measures adapted to the context of financial inclusion.[9] In 2019, the FATF formally articulated its long-standing commitment to "promote financial inclusion and encourage proportionate and effective implementation of the FATF standards by countries in line with the risk-based approach" in its Mandate.[10]

5. In addition, practical guidance on financial inclusion issues has been incorporated into other guidance documents, for example, the FATF's Guidance on

2 See FATF (2019b):13 and FATF (2024):18.
3 First acknowledged by the then FATF President Paul Vlaanderen at the ESAAMLG 9th Council of Ministers Meeting, Maseru, Lesotho, 21 August 2009, referenced in G-20 Global Partnership for Financial Inclusion White Paper, see World Bank (2011):20.
4 See FATF (2012a)
5 See FATF (2012b)
6 See Global Partnership for Financial Inclusion (2016b):25.
7 See FATF (2011)
8 See FATF (2013a)
9 See FATF (2017)
10 FATF (2019b):13

Digital Identity[11] and Guidance on Risk-Based Supervision.[12] The FATF's extensive work on de-risking[13] also aligned with its financial inclusion objectives.

6. In 2021, the FATF launched a project to study and mitigate the unintended consequences resulting from misapplication of the FATF Standards, including de-risking, financial exclusion and undue targeting of Non-profit Organisation (NPOs).[14] In response to the findings of the project's initial stocktaking exercise, in 2023 FATF reviewed R.8 and issued a new Best Practice Paper on Combating the abuse of NPOs.[15] In 2025, FATF revised the FATF Standards to further promote understanding and adoption of the RBA in implementing the FATF Standards.

Purpose of the Guidance

7. The FATF has updated the 2017 Financial Inclusion Guidance to reflect the 2025 Amendments to Recommendation (R.)1/Interpretative Note to Recommendation (INR.)1 and consequential amendments to INR.10 and INR.15 (hence forth 2025 revision of the FATF Standards). It also takes into account findings of FATF's work on Unintended Consequences, and recent developments in digital transformation and digital identity. It seeks to facilitate a better understanding of how to leverage the RBA to AML/CFT measures to advance financial inclusion. It also seeks to help countries, competent authorities, and regulated entities, including financial institutions (FIs), Virtual Asset Service Providers (VASPs) and Designated Non-Financial Businesses and Professions (DNFBPs), implement an effective regime that employs an RBA with AML/CFT measures proportionate to risk, with a view to helping align AML/CFT safeguards and financial inclusion policy objectives.

8. R.1 recognises the RBA as an essential foundation to the efficient allocation of resources across a country's AML/CFT regime and the implementation of risk-based measures throughout the FATF Standards. It requires both countries and regulated entities to identify, assess, and understand their ML/TF risks and implement proportionate action to mitigate the identified risks effectively. The general principle of an RBA is that, where there are higher risks, countries should ensure that their AML/CFT regime adequately addresses such risks. Correspondingly, where the risks are lower, countries should allow and encourage simplified measures as appropriate to manage and mitigate those risks.[16] The RBA focuses AML/CFT resources on higher risk areas and provides flexibility to apply simplified measures to lower risk areas.

9. The RBA is a way to ensure efficient allocation of resources to fight ML/TF more effectively, and it is also crucial for financial inclusion. The Guidance reflects the FATF's understanding that applying overly cautious, non-proportionate

11 See FATF (2020b).
12 See FATF (2021a).
13 Defined as the "phenomenon of financial institutions' terminating or restricting business relationships with customers or categories of customers to avoid, rather than manage, risk". See FATF (2014a), FATF (2015a) and FATF (2015b).
14 See FATF (2021c).
15 See FATF (2023).
16 For example, encouragement can take the form of guidance issued by the government, supervisor, or other competent authority to improve understanding of the circumstances when simplified measures may be appropriate and what form they may take, or outreach or other forms of engagement with regulated entities to promote the use of simplified measures in appropriate circumstances.

AML/CFT safeguards when providing financial services can exclude legitimate consumers and entities from the regulated financial system or can underserve them by limiting or increasing the cost of their access to and/or use of regulated financial services. When individuals or entities lack access to regulated financial products and services that meet their needs, they are forced to resort to cash or unregulated channels, which limits transparency, undermines the effectiveness of AML/CFT safeguards, and increases the risk of crime, ML, and TF. It is central to the FATF's mandate to ensure that the global AML/CFT standards are well understood and correctly implemented, and that countries and their regulated entities are provided with clarity to support designing and implementing AML/CFT measures that proportionately mitigate ML/TF risks and promote financial inclusion.

10. To this end, and in line with efforts by the FATF to require jurisdictions to allow and encourage simplified measures, the Guidance explains in greater detail how to apply the RBA in lower risk situations to enable simplified measures, including SDD, or exemptions. It also expands on the focus of the prior Financial Inclusion Guidance to highlight the importance of the RBA to supervision of customer due diligence CDD measures and addresses existing and perceived obstacles to financial inclusion.

Scope of the Guidance

11. The updated Guidance makes reference to the FATF Standards that are most relevant when considering the link between AML/CFT policies and financial inclusion. The Guidance does not provide a single model for promoting financial inclusion in the AML/CFT context. Instead, it seeks to share country experiences from both developed and developing countries to highlight different ways to promote financial inclusion through the RBA. The inclusion of such examples and case studies are for illustrative purposes only and does not represent an endorsement by FATF. The extent and causes of financial exclusion and appropriate approaches to financial inclusion may vary from country to country. Leveraging the RBA, each country should assess its own ML and TF risks, including its financial exclusion risks, and take into consideration its financial inclusion policies and strategies, when developing and implementing an AML/CFT regime that mitigates the identified risks and promotes broader financial inclusion.

12. While this Guidance aims to promote appropriate access to regulated financial services for all individuals and entities (i.e., natural and legal persons), it focuses on facilitating access for financially unserved and underserved persons (henceforth un/underserved persons).

13. The Guidance explains the importance of financial exclusion for understanding a country's risk and context and the impact that disproportionate implementation of the FATF Standards can have on an effective AML/CFT regime. The 2025 revision of the FATF Standards require countries to allow and encourage simplified measures in assessed lower risk scenarios, but do not require countries to compel regulated entities to adopt simplified measures in all lower risk scenarios.

14. The Guidance also addresses de-risking, occurs when regulated entities refuse to provide, terminate, or restrict business relationships with, and services for customers or categories of customers, to avoid risk rather than sufficiently understanding and managing the risk in line with the FATF's RBA. Wholesale de-risking is contrary to the RBA and contributes to broader financial exclusion risk within a country. While both wholesale de-risking and an overly conservative

application of the RBA on a case-by-case basis contribute to financial exclusion, different regulatory, supervisory, and policy responses may be required to correct de-risking. This Guidance discusses approaches to address the issue of de-risking, but not other denials of financial services[17] for reasons unrelated to AML/CFT risks.

15. The concept of financial inclusion has evolved from access to regulated financial services to also include appropriate usage of those services and products and financial literacy.[18] This Guidance considers the broadened concept of financial inclusion, noting that earlier editions reflected the original, access-focused understanding of financial inclusion.

16. This Guidance is informed by various studies dealing with the broader aspects of financial inclusion, as well as experts' views, consultation with interested parties and stakeholders and countries' experiences by way of questionnaires. Along with the information set out in this document, countries should refer to existing[19] as well as new and emerging research on financial inclusion and to their own financial inclusion policies and strategies. After an extensive consultation with both the public and the private sectors, it was adopted by the FATF at its June 2025 Plenary.

17. This Guidance is composed of four parts:

- Chapter 1 discusses the concept of financial inclusion and its relevance to protect the integrity of the financial sector / achieve AML/CFT objectives.
- Chapter 2 presents an overview of the RBA inherent to the FATF Standards.
- Chapter 3 provides detailed guidance on the practical application of the RBA to leverage the flexibility allowed under the FATF Standards to support financial inclusion.
- The Annexures provide examples of implementation of risk-based measures supporting financial inclusion to support implementation of R.1 objectives by countries and private sector.

18. The Guidance should be read in conjunction with the amended FATF Standards. It is non-binding and does not create new obligations or change existing obligations established by the FATF Standards. Rather, it clarifies and reinforces the RBA, and the flexibility provided in the FATF Standards. This Guidance does not address FATF Standards that establish mandatory and non-risk-based measures such as the implementation of targeted financial sanctions, record keeping requirements, or reporting suspicious transactions. However, it should be noted that some jurisdictions may impose requirements beyond what is called for in the standards, that are excessively rigid and unduly add to financial exclusion risk.

17 Also referred to by some as "de-banking", used as a general term for description of the situation where regulated entities terminate or restrict services to a customer/client or counterpart (e.g. respondent banks and FinTechs), or to whole groups or categories of customers, or sectors. Depending on the underlying reason, denials of financial services may or may not be de-risking.

18 See Global Partnership for Financial Inclusion (2016b):6; Independent Evaluation Group of World Bank (2023); Frost, Gambacorta and Shin (2021); Alliance for Financial Inclusion (2017); Atkinson and Messy (2015):11; Sirtaine (2023); For the importance of extending FATF's access definition to include usage, see De Koker (2018).

19 See Bibliography and sources.

Target Audience

19. The Guidance is intended for:

- The public sector, specifically policymakers, regulators and supervisors involved in implementing the FATF Standards or promoting financial inclusion.
- The private sector, in particular, regulated entities that provide financial services to disadvantaged and other vulnerable groups, including low-income and undocumented groups, in both developed and developing countries.

20. Financial inclusion is an important determinant for all economies and a critical determinant for sustainable development, as reflected in Goal Eight of the United Nations(UN)' sustainable development goals.[20] It has been a key priority for the G20[21] [22] since 2010, when the Global Partnership for Financial Inclusion was created, and is a priority for work on financial stability and economic development by the International Monetary Fund (IMF), World Bank and UN.[23] Accordingly, many aspects of this document may also be useful to a broader audience, including organisations providing support to un/underserved persons;[24] those engaged in providing technical assistance; and other stakeholders dealing with the subject of financial inclusion and sustainable development. Their work, in turn, can contribute significantly to the FATF's financial integrity objectives.

20 See United Nations (2015)
21 See Global Partnership for Financial Inclusion (2010)
22 See Global Partnership for Financial Inclusion (2023); G20 (2024)
23 The IMF and the World Bank both produce comprehensive trend data on financial inclusion, and financial inclusion issues can be covered at the country level in Financial Sector Assessment Programs (IMF and World Bank) and in Article IV Surveillance (IMF). The World Bank assists countries to design and implement National Financial Inclusion Strategies. See IMF (2023); World Bank (2025) and Asli et al. (2022).
24 Including those that lead financial literacy program and campaigns.

Chapter 1. Financial Inclusion and its Implications for Financial Sector Integrity

21. Financial inclusion and AML/CFT objectives are mutually supportive. This Chapter briefly examines the concept of financial inclusion, and its relevance to financial sector integrity (Section 1.1) and provides an overview of the state of financial inclusion (Section 1.2). It then discusses the main drivers of financial exclusion broadly (Section 1.3) and possible solutions to address these barriers in the AML/CFT context (Section 1.4.). Finally, the Chapter discusses de-risking as a separate concept, including drivers, implications and possible ways to address the issue (Section 1.5). Specific examples can be found in Annex A1.

1.1. What is financial inclusion and why does it matter for protecting financial sector integrity?

1.1.1. What is Financial Inclusion?

22. In general terms, financial inclusion refers to both access to and active use of an adequate suite of regulated, appropriate, safe, convenient and affordable financial services by individuals (including households) and entities that would benefit from such services. "Appropriate" means that the products and services are tailored to the customer needs and delivered transparently and fairly.[25] The concept of financial inclusion has evolved, from access to regulated financial services to also include appropriate usage and quality of those services and products, financial literacy, financial resilience and financial well-being of end-users.[26] [27]

23. Financial inclusion efforts seek to address the needs of individuals and entities that either have no access to regulated financial services (unserved) or have access, but only in a limited manner (underserved). For example, unserved individuals tend to engage in small numbers of lower-value transactions in cash or use unregulated financial services and their transaction patterns tend to be less complicated than underserved or standard included populations. An underserved individual or entity may have access to regulated Money or Value Transfer Services (MVTS) providers, but not to bank payment, savings, or lending products and services. The underserved also include individuals or entities who technically have access to financial services (for example, they have a bank or mobile money account) but do not use it for most of their transactions due to factors such as cost, limited knowledge, lack of trust, or lack of utility. Fully included customers may become underserved or even unserved, for example, when a bank closes physical branches, and some existing

25 See Consultative Group to Assist the Poor (2023).

26 See Global Partnership for Financial Inclusion (2016b):6; Independent Evaluation Group of World Bank (2023); Frost, Gambacorta and Shin (2021); Alliance for Financial Inclusion (2017); Atkinson and Messy (2015):11; Sirtaine (2023); For the importance of extending FATF's access definition to include usage, see De Koker (2018).

27 See Alliance for Financial Inclusion (2016):13; Consultative Group to Assist the Poor et al. (2024); See also G20 and OECD (2022) for importance of Quality Financial Products. Quality financial products are those that are designed to meet the interests and objectives of the target consumers and to contribute to their financial well-being.

customers are unable to navigate or access the remote digital financial services[28] (DFS) offered instead of in-person services.

24. Together, the un/underserved population constitutes a very diverse category, with significantly different risk profiles in different jurisdictions. Typically, in both developed and developing countries, un/underserved populations disproportionately include members of disadvantaged and other vulnerable communities, such as low-income individuals and households, financially fragile people (e.g. those experiencing temporary financial difficulties), displaced persons, persons in geographically remote locations, persons with disabilities, persons in high crime- or conflict-impacted communities, and undocumented migrants and residents, who often lack the means to prove their identities and/or the funds to access and use regulated financial services.

1.1.2. Why Financial Inclusion Matters for Financial Sector Integrity

25. Financial exclusion may arise from multiple factors that limit access to and usage of formal financial services, and can be an unintended consequence of inappropriate or insufficient application of RBA to ML, TF and PF risks. Financial exclusion not only harms individuals and businesses, but can also represent a real risk to achieving effective implementation of FATF Standards by driving financial activity into unregulated channels. The risks of financial exclusion on these grounds are mitigated through financial inclusion measures that increase reliance on regulated, registered or licensed financial services, ultimately strengthening the integrity of the financial system.

26. Financial inclusion enhances financial sector transparency and integrity by increasing the reach and effectiveness of AML/CFT measures that help keep criminals out of the financial system and facilitate law enforcement investigations.

27. Financial inclusion helps combat underlying crime by providing safe, cost effective and reliable financial services to customers who would otherwise be forced to resort to cash or unregulated financial services.[29] Financial inclusion provides more visibility to supervisors as regulated entities identify suspicious transactions, and narrows down the grey economy which creates opportunities for concealment of criminal funds. Use of unregulated services significantly increases the vulnerability of legitimate un/underserved individuals and entities to become victims, unintentional facilitators or even coerced perpetrators of fraud, theft, other proceeds-generating crimes, and other forms of criminal exploitation. For example, initial indebtedness to unscrupulous underground loan sharks can lead to becoming a victim of human trafficking, which generates billions of dollars worldwide in illicit proceeds. Criminals can also exploit un/underserved persons by tricking or forcing them to conduct illicit financial transactions, such as serving as a money mule, on the criminals' behalf to evade AML/CFT controls and law enforcement scrutiny.

28. Proportionate AML/CFT measures therefore enable more individuals, microentrepreneurs, small and medium enterprises to save money securely, access credit safely, and manage risks more effectively, helping to keep otherwise vulnerable persons out of the clutches of criminal organisations.

28 "Digital financial services" cover financial products and services, including payments, transfers, savings, credit, insurance, securities, financial planning and account statements.

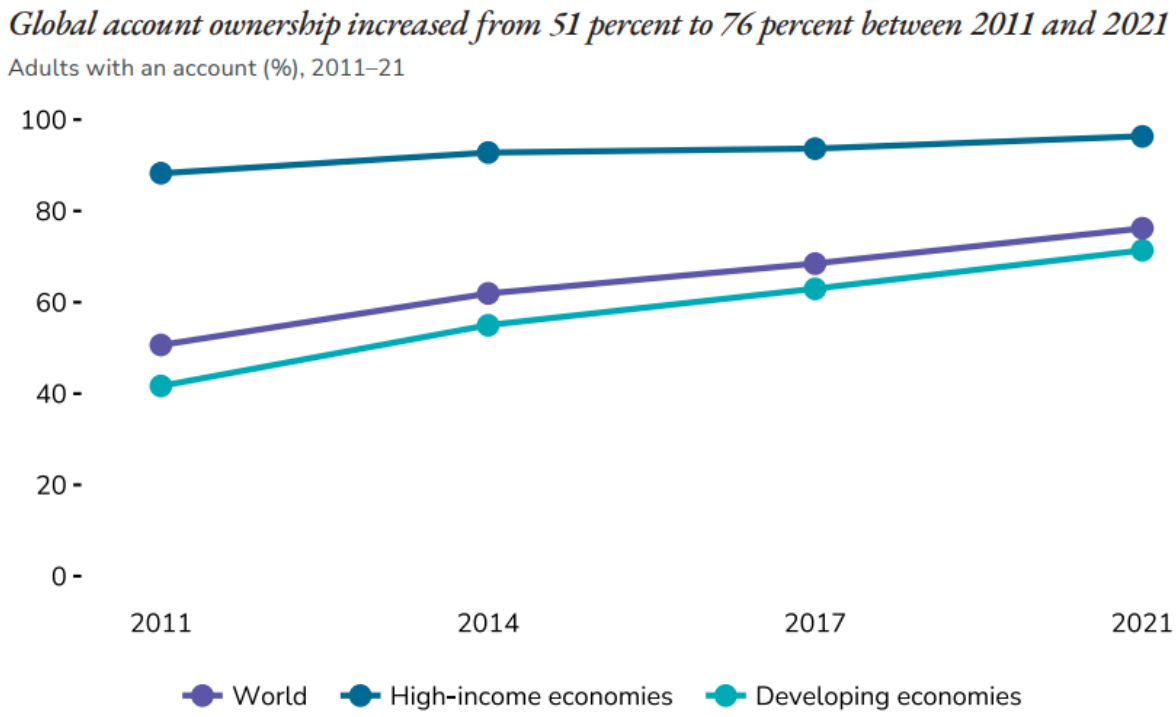
29 See Global Partnership for Financial Inclusion (2016b):25.

1.2. State of Financial Inclusion

29. Understanding the state of financial inclusion is important to determine the progress made in this area and where more work is needed. While access to financial services has increased in recent years, use of financial services has somewhat lagged behind, and differences between groups remain. A range of quantitative indicators can be used to analyse a country's level of financial inclusion. These include: account ownership; account usage; the making and receiving of digital payments; and access to remittances. These indicators can be contextualised by other factors, such as income group, gender and geography (e.g. global/regional and rural/remote versus urban).

30. Financial inclusion increased rapidly over the last ten years. Account ownership around the world grew by 50% from 2011 to 2021.[30] Despite that increase, approximately 1.4 billion adults worldwide still lacked access to a formal bank or mobile money account in 2021 (down from 2.5 billion in 2011).[31] As reflected in Figure 1, account holding differed between high-income and low-income countries, with the latter lagging.

Figure.1. Global Account Ownership Trends between 2011 and 2021



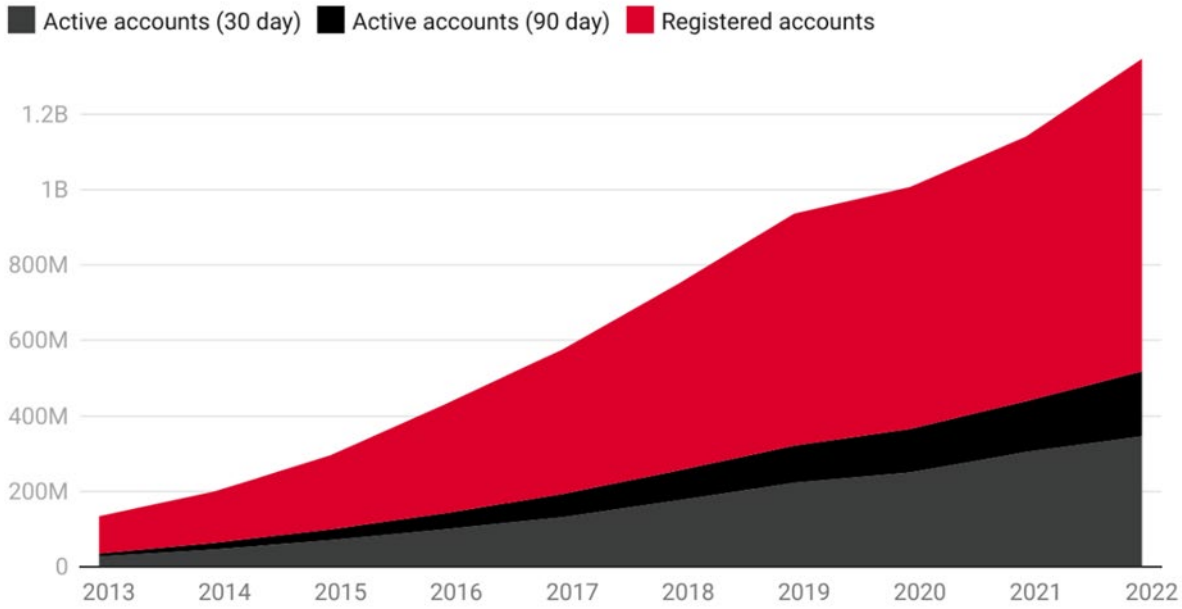
Source: Asli et al. (2022)

31. While the number of accounts increased globally (see Figure 1), usage of the accounts lagged in some cases. Accounting to 2021 data, new account holders continued to use unregulated financial services to conduct many of their

30 See Asli et al. (2022) :2.
31 See Asli et al. (2022):33.

transactions,[32] while some accounts were left entirely dormant after account opening.[33] Account usage rates are a valuable indicator of the appropriateness of the available financial products and services. Mobile money accounts have been a primary type of account opened to increase financial inclusion in developing economies. However, by the end of 2023, only 26% of these accounts were active on a monthly basis, and 38% were active on a 90-day basis (see Figure 2),[34] indicating problems with the appropriateness or usefulness of the account and/or other ongoing barriers to sustained usage.

Figure.2. Mobile Money Account Ownership and Usage Trend between 2012 and 2021



Source: GSMA (2023)

32. In developing economies, the share of adults making or receiving digital payments grew from 35% in 2014 to 57% in 2021, which is greater than the increase in account ownership over the same period.[35] During the COVID-19 pandemic, which increased the necessity for "remoteness" (i.e. non-face-to-face account opening and transactions) globally, increased use of mobile money and digital payments in turn fuelled financial inclusion growth. In Africa, for example, the value of digital transactions rose from 26% to 35% of Gross Domestic Product between 2021 and 2022.[36]

33. In many developing countries, remittances are vital sources of funds for individuals and households, and play an important role in driving financial inclusion. Officially recorded flows to developing economies are estimated to have reached

32 See De Koker and Jentzsch (2013):267.
33 See GSMA (2023).
34 See GSMA (2024):7.
35 See Asli et al. (2022):55.
36 See IMF (2023).

USD 669 billion in 2023.[37] However, the cost of remitting funds erodes their value and acts as a drag on financial inclusion. In 2023, the global average cost of sending a $200 remittance to developing regions was 6.2%, more than double the target of 3% by 2030 set by Sustainable Development Goal.[38] Hence, the international community is committed to lowering remittance costs.[39] Other factors – such as the regulatory environment – are important determinants of the time it takes to remit funds. Delays in sending and receiving vital funds further impact on the social value and economic impact of remittances.

34. Income group is a factor affecting account ownership worldwide. Among adults in the richest 60% of households, 79% have an account, while only 72% of the poorest 40% of households do, resulting in an income gap in account ownership of 7 percentage points.[40] This gap has halved since 2011. However, in many developing economies, the income gap in account ownership is still in double digits.

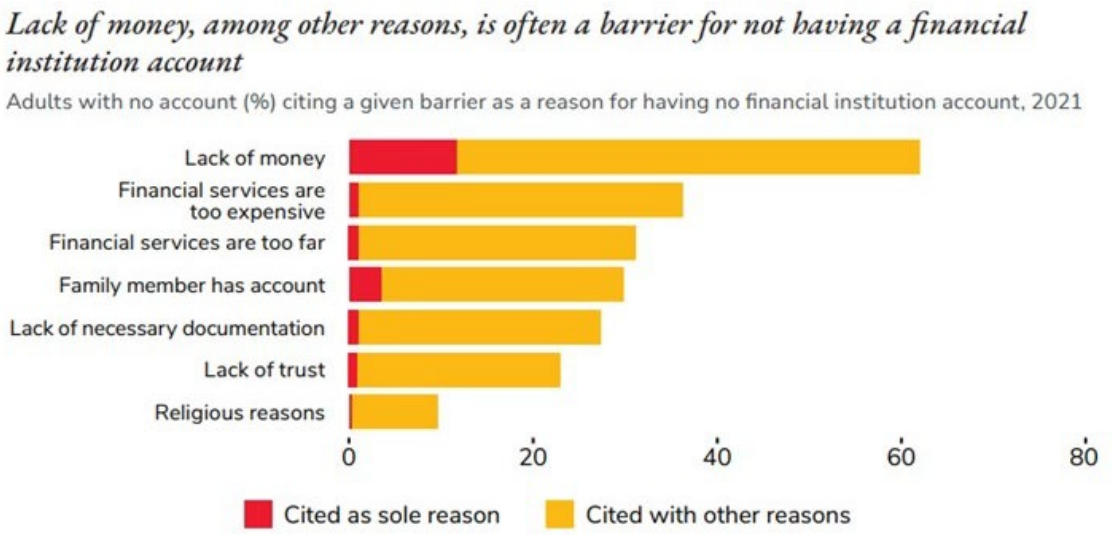
35. Globally and across multiple regions, studies identified ongoing gender gaps between financial access for men and women. According to 2021 data, while there is a global gap of 4%in in financial access between men and women, the gender gap climbs to 6% in developing economies. In 2021, (i) Sub-Saharan Africa and (ii) the Middle East and North Africa reported 12% and 13%gender gaps, respectively, twice as large as the developing economy average and three times larger than the global average.[41] Mobile money account gender gaps were particularly pronounced in some developing economies, with the gap ranging up to 28%.[42] In these contexts, developing economies, women are also more likely to have inactive accounts, reflecting barriers beyond access, including digital literacy and socio-economic constraints.[43]

1.3. Factors Driving Financial Exclusion

36. There are many reasons individuals or groups may be unable to access or take full advantage of regulated financial services.[44] Some are linked to the circumstances of the users (see Figure 3). Others are linked to the nature and design of the products and services or to the policies and practices of regulated entities, including profitability considerations and risk appetite. In some cases, domestic laws and regulatory/supervisory policies, or entities' interpretations thereof, may impede financial inclusion—for example, laws prohibiting the provision of financial services to undocumented persons or non-residents. This includes the interpretation of regulatory policies by supervisors during inspections, where FIs perceive inspection findings to deter regulated entities from pursuing financial inclusion initiatives.

37 See Ratha et al. (2023) :1
38 See Ratha et al. (2023):.10
39 In November 2020, the G20 leaders endorsed the roadmap for enhancing cross-border payments to make cross-border payments cheaper, faster, more transparent, and accessible. See Financial Stability Board (2020).
40 See Asli et al. (2022): 25.
41 See Asli et al. (2022): 21.
42 See GSMA (2024): 8.
43 See Asli et al. (2022): 112.
44 For specific barriers faced by the individuals who continue to be financially excluded, see also Consultative Group to Assist the Poor, BTCA, Global Partnership for Financial Inclusion, and World Bank (2024).

Figure.3. Self-reported barriers to use of formal accounts
Non-account-holders reporting barrier as a reason for not having an account (%)



Source: Asli et al. (2022)

Box 1. Private Sector, Spain and the United Kingdom - Implementation of AML/CFT regulations resulting in unintended financial exclusion or de-risking

In some instances, banks have indicated that unintended financial exclusion or de-risking may be linked to their implementation of the government's AML/CFT regulations. Examples include:

- Where "nationality" is indicated by competent authorities as a risk factor to consider when assessing customers, this may result in high-risk ratings, or de-risking, for customers who are first or second-generation immigrants from high-risk jurisdictions, despite their legal resident status in the host emigrating country (Spain).
- Where regulations do not permit individuals without legal status in a country to have a bank account, this may result in banks monitoring the visa status/expiration date of customers and closing accounts when visas expire, placing the individual in a vulnerable situation. The expectation of monitoring and verifying visa status itself creates a cost of compliance that serves as a disincentive for FIs to provide financial services to individuals where legal status may change (the United Kingdom).

37. The World Bank's Findex 2021 Report shows that globally, the most frequently cited reason for not having an account at a bank or other regulated institution, such as a credit union, microfinance institution, or mobile money service provider, is the lack of enough money to use one (62%), followed by costs of financial

services (36%).[44] The next most commonly cited reasons are that financial services are too far away (31%) and that another family member already has access to an account (30%). More than a quarter (27%) of the unserved adults cited lack of documentation as a barrier (see Figure 3). Other reasons include lack of trust in banks and religious reasons. Reasons specific to mobile money accounts mirror many of the above barriers to access to regulated financial services in general, including lack of funds, lack of appropriate documentation, and increased costs, but also included lack of access to a mobile phone.

1.4. Addressing Barriers to Financial Inclusion in the context of FATF Standards

1.4.1. Leveraging the flexibility afforded by the RBA to support financial inclusion

38. An appropriate application of the RBA that allows and encourages simplified measures where risks are lower can reduce unnecessary operational costs and thus costs for customers and remove some barriers to access and usage of financial services.

39. As discussed in greater detail in Chapters 2 and 3, the RBA calls for both countries and regulated entities to consider the diverse levels and types of ML/TF risks posed by different products, services, transaction or delivery channels (including DFS and products), and customers, as well as risk mitigation measures, to ensure that AML/CFT requirements are proportionate to identified risk, with a view to supporting financial inclusion.

40. In addition, in limited circumstances and when there is an assessed low ML/TF risk, the FATF Standards allow countries not to apply certain AML/CFT obligations to FIs or DNFBPs when an individual or an entity carries out a financial activity on an occasional or very limited basis (having regard to quantitative and absolute criteria), relative to its other, primary business activities.[45]

1.4.2. Broader Government Action to Align AML/CFT and Financial Inclusion Policies

41. The FATF recognises financial exclusion as an ML/TF risk factor and financial inclusion as a means to mitigate that risk to contribute to a more effective AML/CFT regime. It is therefore important for countries to ensure that their financial inclusion and AML/CFT policies and practices are aligned and developed in tandem. To this end, countries are encouraged to consider how the design and implementation of AML/CFT policies and measures should be integrated into national financial inclusion policies and strategies, and vice versa.[46] Countries should also consider integrate financial exclusion risks into their AML/CFT risk assessments and consider opportunities to mitigate those risks. In lower risk scenarios, countries should allow and encourage the implementation of simplified measures in lower risk scenarios to

45 The FATF Standards also provide flexibility to countries to exempt a particular type of regulated entities from the requirements to identify, assess, monitor, manage and mitigate PF risks, provided there is an assessed low risk of PF relating to such private sector entities. exclusion concerns. As risk profiles can change over time, countries should monitor such exemptions. Nevertheless, full application of the targeted financial sanctions as required by R.7 is mandatory in all cases. See FATF (2021b).

46 See Cooper et al. (2020): 9.

promote financial inclusion. Countries should collaborate with the private sector in developing strategies for financial inclusion to decrease overall ML/TF risk for the country, including joint approaches to transition away from a cash-based economy through the offering of basic bank accounts, noting that this may result in FIs taking on more risk within their own portfolios. These institutional implications should be considered in the country's strategic approach when implementing effective AML/CFT measures, including in its regulatory and supervisory approach.

42. In addition to implementing a risk-based AML/CFT regime that allows and encourages the application of simplified measures in lower risk situations , countries should also consider broader actions to drive financial inclusion, such as the digitalisation of government payments, addressing identity-related obstacles,[47] or building an appropriate financial consumer protection framework[48] to help ensure that AML/CFT requirements and financial inclusion policies are mutually reinforcing.

43. Digitalisation of payments broadly and particularly government payments, including Government-to-Persons social assistance payments, payments of wages, pension, and medical benefits can significantly increase financial inclusion while strengthening payments integrity.[49][50] Digitalising Government-to-Persons social protection benefit and other Government-to-Persons payments requires recipients to have some form of regulated account (e.g. bank account, mobile money account, or even a reloadable prepaid card) for electronic deposits of the payments. As part of digitalising Government-to-Persons payments, governments can encourage banks (or other regulated FIs) to rapidly open accounts, including limited-purpose accounts, for lower risk, unbanked government payments recipients, using appropriate SDD measures. Designed appropriately, digital Government-to-Persons payments can support both access and increased usage of regulated financial service by recipients while strengthening the effectiveness of AML/CFT controls.[51]

44. As part of digital Government-to-Persons payments or as a standalone policy, applying the RBA to CDD could support non-face-to-face account opening and transactions, reducing barriers related to physical distance from bank branches and point-of-sale terminals.[52] Indeed, during the global COVID pandemic, the FATF issued a statement encouraging governments to apply the RBA to enable non-face-to-face account opening and transactions,[53] and many governments adopted policies to

47 See World Bank Group (2022).
48 See G20 and OECD (2022).
49 See Cangiano, Gelb and Goodwin-Groen (2019):144.
50 For example, the Better than Cash Alliance worked with Indonesia's government and cocoa sector to propose a strategy for digitising payments throughout certified supply chains and tailored digital financial products to drive the financial inclusion of small cocoa farmers, who are almost exclusively paid in cash, underbanked, and face a significant credit gap that results in a negative cycle of reduced income and falling profits. Digitising payments in the cocoa sector provide end-to-end financial transparency and would also help global cocoa processors verify where their product is sourced. See Sivalingam et al. (2024).
51 See Morawczynski, O., Wallace, L. and May, M. (2022).
52 It is also important to address digital literacy gaps, which could post a distinct barrier to leveraging DFS to increase financial inclusion. For example, an insurance company in Hong Kong shared an example of a low-income construction worker with an old model mobile phone that could not support the latest version of the mobile app of the company, which was originally designed to improve accessibility and convenience. This technical incompatibility barring individuals to use digital banking solutions and preventing them from accessing the services that could significantly ease their financial burdens is a common scenario.
53 See FATF (2020d).

support social distancing by non-face-to-face account opening and DFS.[54] [55] The FATF still considers this position to be aligned with the RBA, where appropriately implemented. Governments can also promote financial literacy through programs tailored to un/underserved populations to encourage use of traditional financial services and DFS.[56]

45. The lack of proof of identity can present a significant obstacle to financial inclusion, with 850 million people globally lacking official proof of their identity.[57] This challenge disproportionately affect disadvantaged and vulnerable groups, such as those in geographically remote areas, undocumented migrants and those working in the unregulated economy and paid in cash, who are less likely to have an official proof of identity, an established address, and other information typically required by banks to verify customer identity. Women also disproportionately face challenges in accessing identity (ID). In low income countries, 44% of women lack any kind of formal ID, compared to 28% of men.[58] This obstacle to financial inclusion is more prevalent in low-capacity countries that do not have civil registration and vital statistics and (physical or digital) identity systems. Nevertheless, lack of official identity may also impede access to regulated financial services by un/underserved groups in developed economies, for example undocumented migrants.

46. Governments can take several steps to address identity-related obstacles to financial inclusion and support a healthy financial sector that services the population safely and inclusively, such as

- Establish inclusive, accurate civil registration and vital statistics systems that provide essential, core authoritative data for official identity.
- Adopt appropriate regulatory frameworks for government-provided digital identity systems and/or private sector-provided digital identity solutions, with appropriate governance (trust frameworks), technical standards, and assurance levels.[59]
- Develop and implement secure, interoperable, digital identity infrastructure and implement government-provided digital identity systems (and/or facilitate the implementation of private sector-provided solutions) that are secure, privacy-preserving, consent-based, inclusive and equitable.
- Establish appropriate regulatory frameworks for traditional and DFS. For example, a supportive regulatory environment could allow progressive customer identity verification (a.k.a. tiered accounts) to access and use financial services. In the case of a tiered account, a financial services account,

54 See FATF (2020a):13-15, setting out a range of actions governments are taking or could take in response to the pandemic, including actions to promote RBA and simplified measures for account opening and digital transactions.

55 See Jenik, Kerse and De Koker (2020).

56 See Consultative Group to Assist the Poor et al. (2024); and OECD Committee on Financial Markets (2022)

57 See Clark, Metz and Casher (2022): viii.

58 See World Bank (no date). The gender gap is particularly significant in the context of AML/CFT measures, since research suggests that women are more likely to lack the kinds of documents often required for onboarding and therefore stand to gain more from the appropriate application of simplified measures in lower risk scenarios. For more on this, see for example Newnham et al. (2018).

59 See World Bank (2022).

with restricted functionality, is opened with SDD measures and confidence in the customer's identity and the purpose of the account is ascertained over time through the customer's transaction pattern, enabling increasingly greater account functionality and access to a wider range of financial services.[60]

Box 2. The Trust Quotient: An Association of Southeast Asian Nations Policy Toolkit for Unlocking Responsible Digital Payments for Micro-Merchants[61]

To expand adoption and sustained use of digital payments by micro-merchants in ASEAN countries, the Association of Southeast Asian Nations Working Committee of Financial Inclusion collaborated with the Better than Cash Alliance and the Indonesian Ministry of Finance to develop a toolkit that:

- identified factors that build or erode trust in digital finance service,
- examined challenges to micro-merchant adoption (such as data privacy concerns, unexpected charges, and complex recourse mechanisms, that presented obstacles),
- provided concrete policy recommendations to help micro-merchants overcome obstacles to using digital payments and making recourse clear and responsive, in line with the UN Principles for Responsible Digital Payments[62] (including safeguarding customer data, ensuring funds are protected and accessible), and
- analysed gender-based barriers to digital payment adoption by female micro-merchants and offered actionable policies to better support digital financial inclusion of female micro-merchants.

1.5. De-Risking

47. Generally speaking, de-risking refers to the phenomenon of FIs' refusing to provide, terminating or restricting business relationships with, and services for, customers or categories of customers to avoid risk rather than sufficiently understanding and managing the risk in line with the FATF's RBA.[63] It is important to

60 See FATF (2020b):56: Box 3. Illustration of how the use of digital ID in tiered and progressive CDD can support financial inclusion.

61 See Sivalingam, Budiarso, et al. (2024).

62 The UN Principles for Responsible Digital Payments were developed by the United Nations-based Better Than Cash Alliance, guided by its member governments, companies and international organisations. See Better Than Cash Alliance (2024).

63 See, for example, the U.S. Anti-Money Laundering Act (AMLA) of 2020, defining de-risking for purposes of the Act as "actions taken by a financial institution to terminate, fail to initiate, or restrict a business relationship with a customer, or a category of customers, rather than manage the risk associated with that relationship consistent with risk-based supervisory or regulatory requirements, due to drivers such as profitability, reputational risk, lower risk appetites of banks, regulatory burdens or unclear expectations, and sanctions regimes." See also (European Banking Authority, 2023):9 defining de-risking as "a refusal to enter into or a decision to terminate business

note that at times, following an assessment of risk, FIs may reasonably conclude that they lack the ability to mitigate the risk of a particular customer and therefore deny services on a case-by-case basis and that is not counter to the RBA.

48. De-risking can include a variety of actions and impact a broad range of customers, directly or indirectly.[64] It may involve regulated entities' refusing, terminating or restricting financial services to categories of customers,[65] including refugees, asylum seekers, and other internally or externally forcibly displaced persons and returnees; lower socio-economic groups; members of particular religious, ethnic, or national groups; women; members of the LGBTQI+ community; individuals of nationalities linked to countries in a situation of conflict and/or economic sanctioning pressure, specific industries (e.g. MVTS providers, dealers in precious metals and stones, etc.). De-risking may also involve foreign banks' terminating correspondent banking relationships with banks in a jurisdiction (especially higher-risk), indirectly impeding access to the global financial system of other regulated entities in the jurisdiction, such as MVTS providers that rely on the terminated correspondent banks. This knock-on effect in turn impacts the ability of their customers to send or receive remittances.[66] De-risking may also involve banks' refusing to establish or terminating accounts for NPOs,[67] FinTech sectors including VASPs,[68]and/or MVTS providers which indirectly impact the financial inclusion of un/underserved individuals and entities, such as those who receive vital support services from NPOs.

1.5.1. Factors Driving De-Risking

49. De-risking results from a range of complex and interwoven factors, which vary in importance depending on the jurisdiction or region and particular case. The analysis in the FATF's 2021 Stocktake of the Unintended Consequences of AML/CFT Measures concluded that profitability concerns are the primary driver of de-risking, which can be impacted, in some situations, by high compliance costs (including in areas unrelated to AML/CFT).[69] Overly restrictive regulation and institutional failure to apply the RBA appropriately (including overly-conservative assessments of risk and the failure to consider potential mitigation actions) can result in disproportionally strict controls that contribute to higher compliance costs and reduce profitability.[70] Other factors that may drive de-risking include:

- real or perceived unclear regulatory expectations;

relationships with individual customers or categories of customers associated with higher ML/TF risk, or to refuse to carry out higher ML/TF risk transactions."

64 See De Koker, Singh and Capal (2017):119, 128

65 The offering of financial products or services that provide appropriately defined and limited services to certain types of customers so as to increase access for financial inclusion purposes as described in INR10.17, is supported and encouraged, and is not a form of restriction of services to specific persons or groups that constitute de-risking.

66 See World Bank (2015).

67 See FATF (2023); NYU Paris EU Public Interest Clinic (2021); Eckert, Guinane and Hall (2017); Van Broekhoven et al. (2023)

68 See Select Committee on Australia as a Technology and Financial Centre: Final Report (2021), chapter 4.

69 See FATF (2021c):2.

70 See Artingstall et al. (2016); FATF (2021c): 2; De Koker and Casanovas (2024).

- fear of legal or supervisory enforcement actions and potentially large fines by supervisors and compliance officers for AML/CFT and/or other compliance deficiencies;
- risk appetite and reputational risk concerns broadly.[71]
- challenges in sanctions compliance (including the lack of awareness of or capacity to leverage the humanitarian exemptions introduced in UN sanctions and other autonomous sanctions);[72]
- burdens related to mounting regulation of the financial sector (including new privacy regimes, data localisation requirements, and cybersecurity regulation); and
- the lack of incentives for banks to serve un/underserved groups, individuals and entities[73]

50. While the FATF is concerned about the financial inclusion and integrity impacts of all denials of service, it recognises that regulated entities are commercial enterprises and may, subject to applicable domestic laws (e.g. the right to a basic bank account and prohibiting discrimination in financial services), decline to provide services for commercial or other legitimate reasons.[74] Government actions to implement a risk-based AML/CFT regime that promotes an RBA to AML/CFT compliance by regulated entities (see Chapter 3) can help address factors contributing to de-risking.

1.5.2. Impact of de-risking on AML/CFT effectiveness and financial inclusion

51. De-risking undermines AML/CFT effectiveness by driving financial activity out of the regulated financial system, thereby reducing channels for formal oversight.[75] De-risking also undermines financial inclusion by preventing un/underserved persons from accessing or fully using the financial system, which in turn can hamper remittances and delay the unencumbered transfer of international development funds and humanitarian and disaster relief. De-risked customers resort to unregulated alternatives such as unregulated MVTS providers; cash, including the physical transportation of cash between countries; and the use of personal accounts to conduct business transactions by or on behalf of a de-risked business entity.[76] [77] The negative impact of de-risking tends to be most significant in smaller and more financially isolated economies, emerging market economies, and customers linked to conflict zones.

1.5.3. De-risking does not comply with the FATF Standards

52. The FATF has long recognised the harmful impact of wholesale de-risking and has consistently emphasised that the practice is not in line with the RBA mandated by the FATF Standards. In 2014, the FATF issued a statement clarifying that

71 See World Bank (2015); FATF (2021c):2; (The U.S. Department of the Treasury, 2023): 15-22.
72 See United States Government Accountability Office (2021):15; També and Alsancak (2024): 11.
73 See FATF (2015b).
74 Ultimately however, all restrictions of services and denials of services should be considered with care to ensure that undue impact on national AML/CFT objectives is prevented.
75 See Lowery and Ramachandran (2015); European Banking Authority (2022), para. 8; Durner and Shetret (2015).
76 See Durner and Shetret (2015); De Koker, L., Singh, S. and Capal, J. (2017): 119, 146.
77 See Chatain et al. (2018); Quak (2022):9.

the wholesale cutting loose of entire classes of customers, without taking into account, seriously and comprehensively, their level of risk or risk mitigation measures for individual customers within a particular sector is contrary to the RBA.[78] The FATF reiterated this message by providing information to help countries implement the RBA in the "FATF Guidance for a Risk-Based Approach: The Banking Sector".[79] In 2021, the FATF again declared that "de-risking is by …definition inconsistent with a proper application of the RBA promoted by the FATF, which is central to the effective implementation of the FATF Recommendations."[80]

53. The FATF identifies jurisdictions with strategic deficiencies in their system for fighting ML, TF and proliferation financing (PF). When the FATF places a jurisdiction under increased monitoring, often referred to as "grey listing", it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes. The FATF and FATF-style regional bodies work with these countries via a peer-led process to address the most strategic deficiencies in a country's AML/CFT regime that risk enabling illicit financial flows. Since October 2019 the FATF has repeatedly emphasised that it does not call for the application of enhanced customer due diligence (EDD) measures to these jurisdictions. In October 2022, the FATF further clarified that the FATF Standards does not envisage de-risking or cutting-off entire classes of customers.[81] Instead, it calls for the application of an RBA to consider actions based on the risk arising from the deficiencies identified in the grey-listing process. In doing so, countries/FIs should also ensure that flows of funds for humanitarian assistance, legitimate NPO activity and remittances are neither disrupted nor discouraged.

54. Over the last decade, the FATF has also specifically addressed the de-risking of correspondent banking relationships, MVTS, and NPOs as failing to comply with the RBA (See Box below.).

78 See FATF (2014a).
79 See FATF (2014b).
80 See FATF (2021c):2.
81 See FATF (2019c); FATF (2022).

Box 3. The FATF's efforts to combat de-risking of correspondent banking relationships, MVTS, and NPOs

Correspondent banking: The FATF has clarified that under R.13 countries should require correspondent banks to perform normal CDD on a respondent bank, gather sufficient information to understand its business, reputation, and the quality of its supervision, and assess its AML/CFT controls when establishing correspondent banking relationships. Correspondent banks are not required in standard risk situations to conduct CDD on the customers of respondent banks (i.e., on their customers' customers) when establishing and maintaining correspondent banking relationships.[82]

MVTS: The FATF explained that although some MVTS providers may serve as conduits for ML/TF funds, banks should identify, assess, and manage the ML/TF risks associated with individual MVTS, considering such factors as the extent and quality of the regulatory and supervisory framework to which it is subject and its implementation of risk-based AML/CFT controls and mitigating measures, rather than categorising all MVTS providers as inherently high ML/TF risk and avoiding this category of customer.[83]

NPOs: The FATF amended R.8 and its Interpretative Notes (2016, 2023) to clarify that countries are required to implement focused, proportionate and risk-based measures without unduly disrupting or discouraging legitimate NPO activities while protecting NPOs from TF abuse, in line with the RBA. It has also issued and updated its BPP on Combating The Terrorist Financing Abuse Of Non-Profit Organisations (2013, 2015, and 2023) to help countries, regulated entities, and NPOs apply an RBA to implementing measures to mitigate TF risk in the NPO sector and discourage whole de-risking of NPOs.[84] The Best Practice Paper emphasises that typically, only a marginal portion of NPOs present a "high risk" of TF abuse; that a "one-size-fits-all" approach is inconsistent with an RBA; and that countries should implement such measures based on identified TF risks. Recognising the importance to ensure that humanitarian aids reach populations in need, the United Nations Security Council adopted resolution 2761(2024) in December 2024 to extend on a standing basis the application of the humanitarian exemption created by Resolution 2664 (2022). The exemption provided clarity that the provision, processing or payment of funds, other financial assets, or economic resources, or the provision of goods and services necessary to ensure the timely delivery of humanitarian assistance or to support other activities that support basic human needs by the UN and other stakeholders defined in paragraph 1 of resolution 2664 (2022), are permitted and are not a violation of the asset freezes imposed by the UN Security Council or its Sanctions Committees.[85] Beyond the UN Security Council, sanctions emitters such as the United States and the European Union have adopted a similar humanitarian exemption for the vast majority of their autonomous sanctions.

82 See FATF (2016b).
83 See FATF (2016a).
84 See FATF (2023).
85 The exemption provided clarity that the provision, processing or payment of funds, other financial assets, or economic resources, or the provision of goods and services necessary to ensure the timely delivery of humanitarian assistance or to support other activities that support basic human needs by the United Nations, are permitted and are not a violation of the asset freezes imposed by the Security Council or its Sanctions Committees.

1.5.4. Potential Approaches to Address De-Risking

Specific examples relevant for this section can be found in Annex A1.

55. As mentioned above, de-risking increases financial exclusion and exacerbates related ML/TF risks. As part of a comprehensive understanding of risk, countries should identify instances of de-risking and seek to understand if de-risking is caused or exacerbated by the country's legal, regulatory and supervisory framework. It is important for countries to understand why regulated entities refuse to initiate, terminate, and/or restrict financial services and to identify instances/trends of de-risking. Depending on the extent and nature of de-risking, effective responses may require a holistic or targeted response.

56. Regulated entities should avoid de-risking by adopting an RBA to AML/CFT compliance. Countries' efforts to implement a risk-based AML/CFT regime and efforts to promote understanding of the RBA and adoption of proportionate CDD by regulated entities, can help reduce de-risking. Chapter 3 explores in greater detail actions that countries, particularly regulators and supervisors, and regulated entities can take to apply the RBA to their AML/CFT regime.

57. With respect to de-risking specifically, the most common intervention has been for competent authorities to clarify regulatory expectations. This is typically done through supervisory statements or guidelines cautioning regulated entities not to engage in large-scale terminations or restrictions of service, and encouraging risk-informed decisions after appropriate assessment of the risks posed by each customer.[86] Another way for supervisors to encourage policy commitments from regulated entities to prevent de-risking is to recognise and formally acknowledge, the positive efforts made by an FI to provide financial services to populations understood as not lower risk despite the effort borne by the regulated entity. In some contexts, heavily impacted by sanctions, some countries or regional organisations have introduced specific humanitarian exemptions to sectoral sanctions on the financial sector (e.g. on restrictions on establishing correspondent banking relationships).[87]

58. In addition, weaknesses in a country's AML/CFT regime, especially regulation and supervision, may contribute to decisions by banks to cut off correspondent relationships with that country's banking sector or to deny services to customers from that country. Countries' efforts to address gaps in their AML/CFT regime could reduce the risks perceived by regulated entities and significantly help reduce the de-risking of correspondent relationships, as well as the similarly motivated refusal by MVTS to serve certain remittance corridors that they assess as high risk.[88] Countries may need to seek technical assistance to support AML/CFT uplift, and may need to collaborate at a regional level to implement solutions. For example, the Pacific Islands Forum is leading a Pacific Island Correspondent Banking Relationship Roadmap project to stabilise and enhance correspondent banking

86 See European Banking Authority (2023), which provide that FIs should set out in their policies, procedures and controls all options for mitigating higher ML/TF risks that they will consider applying before deciding to reject a customer on ML/TF risk grounds, including where relevant the offer of limited services and products.

87 See for example the United Kingdom General Licence INT/2025/5810196 issued in February 2025 under all the Syria (Sanctions) (EU Exit) Regulations, which allows for payments to be made in respect of relevant humanitarian assistance activities.

88 See Financial Stability Board (2019):3.

relationships of Pacific Islands countries by improving their AML/CFT measures and the business environment.[89]

Box 4. Australia and the United States' efforts to reduce de-risking

This box provides an overview of the examples in Boxes 1.1 and 1.4 (Annex A1).

The Australian Transaction Reports and Analysis Centre has actively engaged to discourage FIs from de-risking classes of customers. A statement on de-banking (2021)[90] and a guidance on de-risking (2023)[91] were issued to encourage institutions to assess and respond to customer risk on a case-by-case basis, as ML/TF risks associated with individual customers in a given industry sector can vary significantly.

In April 2023, the United States Department of the Treasury published a De-risking Strategy, which examines the causes of de-risking for certain customer categories, including NPOs, foreign FIs with low correspondent banking transaction volumes, and money service businesses, which are often used by immigrant communities in the United States to send remittances abroad. The strategy proposed a dozen concrete actions designed to reduce de-risking, including revising FI AML/CFT programs, reviewing bank inspection (referred to as examination in the US) practices, modernising United States sanctions programs (including incorporation of baseline humanitarian-related authorisations), and reducing burdensome requirements for processing humanitarian assistance.

89 See Pacific Islands Forum and World Bank (2024), which is a regional multi-year plan developed by the Pacific Islands Forum Secretariat and the World Bank; Outcomes Statement of the Pacific Banking Forum (2024); D'Hulster et al. (2023).

90 See Australian Transaction Reports and Analysis Centre (2021).

91 See Australian Transaction Reports and Analysis Centre (no date).

Chapter 2. FATF's Risk-Based Approach (RBA) as a Facilitator of Financial Inclusion

59. This chapter clarifies the RBA and of key requirements of the FATF Standards that are most directly relevant to countries' efforts to develop an effective AML/CFT framework that fosters financial inclusion. It presents an overview of the RBA (Section 2.1), provides guidance on what to consider when developing country level and institutional level risk assessments (Section 2.2), explains how the requirements of the FATF Standards can be implemented to facilitate financial inclusion, including application of exemptions in low-risk situations under specific, limited conditions (Section 2.3). Section 2.3 focuses on the new elements of the relevant FATF Standards that have been revised since the last Financial Inclusion Guidance in 2017 – please refer to the 2017 Financial Inclusion Guidance (relevant part extracted in Annex B) for additional details on the implementation of other relevant FATF Standards with regard to financial inclusion.

2.1. Overview of the RBA of the FATF

60. The FATF Standards emphasise the RBA as a comprehensive, first-order principle that applies across the Standards and provides the overarching framework for establishing an effective AML/CFT regime that thereby facilitates financial inclusion. The FATF Standards require countries to first identify, assess, and understand ML and TF risks. Based on this understanding, countries should apply the RBA to inform the efficient allocation of resources across the AML/CFT regime to ensure that measures are proportionate to the identified risks. The FATF Standards also obligate countries to require regulated entities to identify, assess, and take effective action to mitigate their ML/TF risks. It is important to emphasise that that even with appropriate risk assessments, AML/CFT controls, and additional mitigation, ML/TF risks will never be zero for countries or regulated entities.

61. Under the RBA, countries and regulated entities should avoid a "one size fits all" solution, both to ensure proportionate responses to identified ML/TF risk, as well as to mitigate financial exclusion risks. Instead, the scope and rigor of AML/CFT measures should depend on the level and nature of the risks identified. Countries are required to take an enhanced approach where there are higher risks. Correspondingly, pursuant to the amendment to R.1 to be discussed in Section 2.3 below, where lower risks are identified, countries should to allow and encourage simplified measures.[92] In addition, countries may also, in limited circumstances and where there is an assessed low (not lower) risk of ML/TF, decide not to apply certain Recommendations to a particular type of regulated entity or activity.[93] Chapter 3, Section 3.3.3, explains how countries can apply these exemptions in limited, low-risk situations to facilitate financial inclusion.

92 Although it is not spelled out in the standards there is a third scenario where risks may be neither higher nor lower, but at "medium" or "normal" level, where the standard AML/CFT measures apply as a default.

93 "Low risk" situations refer to cases that may qualify for an exemption from the FATF Standards, while a simplified AML/CFT regime may apply to "lower risks" cases. Low risk also qualifies for simplifications, while exemptions are not applicable to lower risk.

2.2. Developing a Risk Assessment – Critical enablers of Financial Inclusion

62. The FATF Standards require both countries and regulated entities to assess risks and take proportionate mitigating measures. Well-developed and appropriately used risk assessments by governments and regulated entities are critical enablers of financial inclusion.

63. Risk occurs when a threat successfully takes advantage of a vulnerability to produce a consequence. To determine the level of risk the country or institution should consider matters such as the extent to which it may occur, and the likely consequence that such an ML/TF event may produce. The likelihood and extent of an event and its probable consequences may differ depending on a range of contextual factors, including types of predicate offences, channels, types of institutions and types of customers, products and services , etc.

64. Risk assessments should consider both inherent risk and residual risk. Inherent risk is the level of risk that exists before introducing any mitigating measures. Residual risk is the level of risk that remains after risk mitigation measures have been introduced. Lower risk situations can be identified either where risks are inherently lower or where the residual risks are lower due to appropriate mitigation by competent authorities and/or regulated entities.

2.2.1. Country risk assessment

65. The RBA requires countries to identify and assess the ML/TF risks[94] on an ongoing basis[95] to implement proportionate, risk-based measures and efficiently allocate AML/CFT resources to effectively mitigate their identified ML/TF risk (see Chapter 3 Section 3.2 for detailed guidance on the practical application of the RBA to support financial inclusion). The FATF recognises that the size and complexity of the country, its ML/TF environment, the maturity and sophistication of the AML/CFT regime, and its overall capacity and structural constraints may factor into the development of its understanding of ML/TF risks.

66. While there is no single or universal methodology for conducting an ML/TF/PF risk assessment, the FATF produced multiple guidance documents to provide jurisdictions information on conducting ML,[96] TF,[97] and PF[98] National Risk Assessments (NRAs) that defines key concepts and outlines the successive stages required to conduct an NRA. Countries should refer to these documents to ensure that they conduct appropriate risk assessments that enable the effective, proportionate implementation of the RBA. There is flexibility about what form these assessments should take, including a national risk assessment or sectoral, multi-sectoral or thematic risk assessments, which enable a deeper dive into sectors with emerging risks or higher risks. What is important is that the assessments are comprehensive in scope, reflect a strong understanding of the risks and are coordinated nationally, with supervisors or other competent authorities assessing specific risks relevant to their functions.

94 Following the October 2020 revisions to R.1, countries are also required to undertake PF risk assessments. See FATF (2020c).
95 INR1 para.5
96 See FATF (2024a).
97 See FATF (2019a).
98 See FATF (2021b).

67. A comprehensive risk understanding is crucial to ensure countries and FIs understand the specific ML/TF environment in which financial products and services are operating. To develop an adequate understanding of the risks associated with financial products and services, countries should consider the latest risk assessments, as well as the ML and TF typologies. Countries should also consider the presence and frequency of ML and TF schemes involving retail financial products and small transactions. Their occurrence, as well as their absence, has implications for the risk profile of financial products that are designed to facilitate financial inclusion (i.e. financial inclusion products). A lack of such typologies could suggest a greater scope and flexibility for financial inclusion products, and the reverse is also true.

68. Additionally, it is prudent for all countries to take into account the impact of financial exclusion on the size and risk of the informal economy (and the associated ML/TF risks), and the overall impact on ML/TF risks of bringing un/underserved people and activities within the regulated financial sector during their risk assessments. This is particularly relevant for countries with cash or unregulated economic activity (also known as grey or shadow economies). Such consideration could involve:

- obtaining data on the extent of cash usage for illicit purposes in the economy;[99]
- the existence and extent of unregulated MVTS;
- the size of the unregulated (underground) economy;
- barriers to access and usage of regulated financial services;
- how illicit actors are abusing unregulated financial services;
- the vulnerability of un/underserved people to financial and other crime and exploitation; and
- the effectiveness of any current national financial inclusion policy.

69. Effective risk assessments benefit from a regular dialogue with the private sector which can provide broad insights about the relative risk of particular financial products and services. Under the FATF Standards, countries are required to communicate the results of their ML/TF risk assessments to regulated entities, so that they can consider that information in conducting their own institutional ML/TF risk assessments and build an appropriate compliance framework.

2.2.2. Institutional risk assessment

70. As noted above, countries must require regulated entities to identify, assess and take effective risk-based action against the ML/TF risks relevant to their activities. Regulated entities should use relevant information from country risk assessments and understand the overall national risk environment. Regulated entities should independently examine the ML/TF risks specific to their operations, customer base, and products and services (see example in Box 5). They should factor in other risk indicators (e.g., the scale of their business, the countries or geographic

99 It is important not to confuse cash usage for illegitimate reasons (e.g. tax avoidance, ML, etc.) with general cash usage. Access to cash is also important from a financial inclusion perspective especially for vulnerable categories of people such as the elderly, uneducated and people with disabilities.

areas in which they operate, and the particular products, services, transactions or delivery channels they offer) to determine their own overall risk exposure. To assist regulated entities in conducting institutional risk assessments, SRBs/industry organisations may also consider pooling expertise from individuals and collaborating private sector efforts in producing sector-wide assessment of specific financial crime risks (see example of private sector in the Netherlands in Box 5).

Box 5. Private Sector, Canada and Netherlands– Individualised risk assessments by regulated entities and sector-wide risk assessment by industry organisations

In Canada, banks apply an RBA to understand and mitigate the risks inherent in their business and its customers with reference to the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* published by the Canadian Government. A bank's risk evaluation process may consider various individual factors, including ML/TF risk, sanctions risk, reputational risk, and credit risk of a customer. An individual factor or a combination of factors may cause a customer to be rated as higher/medium/lower risk. All customers of a bank are assessed individually, on a case-by-case basis and against a consistent framework employed by that bank. Independent decision making based on an RBA helps to preserve Canadians' access to banking services, while ensuring banks' AML/CFT controls, policies and procedures remain robust, protecting the integrity of Canada's financial system.

In the Netherlands, the Dutch Banking Association developed the Financial Crime Threat Assessment in 2024 with inputs from banks, public sector (including Fiscal Intelligence and Investigation Service, the Police and Financial Intelligence Unit (FIU)), selecting several threats as focus areas to create actionable input for the individual risk management processes of banks. For each threat, the assessment included why it had been selected, whether and how banks were exposed to the threat, and how banks can or cannot identify the threat. Additionally, each threat was linked to the Risk Scenario Library, resulting in an assessment tailored for the industry. The Association also planned to cover identify indications of lower risk in future publications to address the challenge of varying interpretations of lower risk and reduce experienced difficulties by lower risk customers.

71. A regulated entity's RBA does not need to be an overly complex process. It should instead consider its unique ML/TF risks to implement controls to manage, monitor and mitigate the risks, appropriately allocate resources in line to with the risks, improve the effective operation of these controls, and record what measures have been implemented and why. In cases where small financial services providers have limited understanding of sectoral risks, or risks outside of their own customer base, countries should consider opportunities to promote information sharing and to enable institutions to conduct joint risk assessments.

72. The risk assessment process should enable regulated entities to identify lower risk scenarios in relation to specific categories of customers or products. Regulated entities which have or are planning to introduce financial inclusion products, should ensure such products and services are in line with the RBA and adequately mitigate the assessed ML/TF risks.

73. Evaluating the risk-mitigating factors is critical for the development and implementation of financial inclusion products. This evaluation should encompass not only the controls specifically designed for AML/CFT purposes, but also anti-fraud measures, as well as limitations and characteristics integrated in the design or inherent to the financial product that can mitigate ML and TF risks.

74. The FATF refers to risk management as developing the appropriate measures to mitigate or reduce assessed level of risk to a lower or acceptable level.[100] Taking an RBA means recognising that residual risks will never be zero. Risk tolerance refers to the accepted level of unmitigated or unmitigable risk taking into consideration the potential impact.[101] Clarity about the country's AML/CFT priorities and risk tolerance is important to inform appropriate and granular risk assessments. With limited resources a focus on more likely and more significant ML/TF risks with more severe consequences may mean that less likely or less significant ML/TF instances or those with more minor consequences may be tolerated in order to focus the AML/CFT system on the priorities set by the country.

2.2.3. Assessing lower risks scenarios to promote financial inclusion

75. Be it on a national, sectoral or institutional level, comprehensive risk assessments should identify not only higher risks, but also scenarios where risks are low or lower. To promote financial inclusion and accurately identify higher risk and lower risk scenarios, risk assessments do not need to be complex but should be sufficiently granular and nuanced.

76. Frequently, different entities within the same sector (e.g. MVTS providers, NPOs, etc.) are exposed to a different level of risk, or a different kind of risk, by virtue of their different activities or different customer groups, as well as the mitigation measures they put in place. This is of particular importance when seeking to identify lower risk scenarios as lower-risk financial inclusion products may be of greatest utility in high-risk jurisdictions. A risk assessment that uniformly assesses such different entities and customer groups may assess the risks incorrectly and resulting in an inappropriate level of risk mitigation measures being applied by competent authorities and regulated entities. Increasing the granularity and level of detail of risk assessments can improve the understanding of risk and risk levels, thereby supporting a more fine-tuned approach to risk management by regulated entities and competent authorities. For example, this can include applying different controls to the highest-risk or lowest-risk entities and customer groups within a particular sector, rather than a single level of control for the entire sector; or it can enable one kind of risk mitigation measure to be substituted for another, less obstructive measure.

77. The FATF Standards give non-prescriptive and non-exhaustive examples of circumstances where ML/TF risks might be determined to be potentially lower in relation to particular types of customers, countries or geographic areas, or products, services, transactions or delivery channels (INR. 10 para. 17). One example of lower risk is "*financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes*". Accordingly, it could be reasonable to apply SDD measures for products fulfilling those conditions provided that lower risk circumstances have been

100 See FATF (2013b).
101 See FATF (2021a).

confirmed, based on a risk assessment, conducted at the national, sectoral or at the FI level (INR.10 para. 16).[102]

78. As mentioned above, a range of contextual factors should be considered in determining the level of risk. With regard to consideration of predicate offences, the nature of the underlying crimes (i.e., petty vs. organised crimes), the use of proceeds of crime (i.e., consumption vs. laundering) and the composition of proceeds of crime (i.e., financial vs. physical assets) of influence the level of ML/TF threats.[103] Risk assessments should also consider issues related to transaction channels, such as the appropriateness of risk control measures imposed on non-face-to-face relationships, geographical reach, methods of funding, access to cash where that may pose a crime risk, and possible segmentation of services between several parties for the execution, etc.. The risk level of a product or service may also be determined by the nature or design of it (e.g. limited functionality, etc.). For the purpose of implementing simplified measures, some industry organisation may identify non-exhaustive examples of lower risk situations (see Box 6).

Box 6. Private Sector, the Netherlands – non-exhaustive examples of lower risk situations identified by national industry organisations

For the purpose of implementing simplified measures, an industry organisation in the Netherlands identified the following non-exhaustive examples of lower risk situations –

- **Retired person with domestic transactions**: a private customer who is retired, earning a modest pension, and engaging solely in predictable, domestic, day-to-day transactions.
- **Employed person with common transactions**: a private customer receiving a salary from regular employment, with periodic fixed expenses and occasional international spending, such as vacations.
- **Subsidised community centre**: a community centre in an adequate AML/CFT jurisdiction funded with municipal or governmental subsidies and expenses limited to rent and activities related to its purpose.
- **Local retail business**: a local grocery store with limited cash transactions in line with its expected transaction profile, mainly operating through wire and card transactions, with predictable expenses such as rent, salaries, and inventory, and no significant international transactions.

79. Apart from the inherent risks of the products, it is important to recognise that un/underserved customer groups can also encompass a wide range of different ML/TF risk profiles. They cannot be classified as lower risk, solely on the basis that

102 INR.10, para 16 states: "There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures".

104 See FATF (2013a), para. 44.

they are about to be or have recently been integrated into the regulated financial system.[104] An RBA must be adopted for each customer.[105]

80. Countries and regulated entities should update their risk understanding/assessments on an ongoing basis. They should consider whether in practice, the risks were actually lower, and the simplified measures were appropriate. This assessment may also analyse whether the simplified serves the objective effectively and improves financial inclusion. Such assessments are particularly important because risks tend to change over time. Risks associated with types of customers evolve, illicit financial flows/typologies also change, and risk levels of products assessed as lower risk may increase over time, especially if criminals start to exploit simplified controls.[106]

81. Countries and regulated entities should also take into account in their risk understandings/assessments the risk mitigation measures adopted by non-profit organizations, including humanitarian and public-funded NPOs, when assessing the risk of terrorist financing and abuse of NPOs.[107]

82. The World Bank, IMF, and Interamerican Development Bank have also developed risk assessment tools and methodologies, and these have been used widely. The World Bank tool contains a specific module for the risk assessment of financial inclusion products.

104 See FATF (2013a), para. 44.

105 For example, the European Banking Authority's Guidelines on policies and controls for the effective management of ML/TF risks when providing access to financial services require credit and FIs to ensure that their controls and procedures specify that specify possible limitations of products and services are applied taking into consideration the personal situation of the individuals, the ML/TF risks associated therewith and their financial basic needs. See European Banking Authority (2023).

106 See De Koker (2009): 334.

107 See also FATF (2023), Para. 124-125.

Box 7. World Bank – Financial Inclusion Product Risk Assessment Module (FIRM)

This box provides a summary of the FIRM detailed at Annex A7.

The World Bank's FIRM tool assesses the ML/TF risks associated with a particular financial product/service intended to support financial inclusion and tests if the product presents a lower level of ML/TF risk that properly justifies SDD. The assessment is based on the net risk level resulted from:

- the product features, which reflect the characteristics and functionality of the product as realistically as possible;
- the product-specific mitigating measures, in place or planned;
- and the overall risk environment, which includes the country's ML/TF threats and the general AML/CFT control measures in the country.

Countries (or regulated entities) using the World Bank tool are invited to provide information on these three parameters in an excel template. Based on the data collected, the module will produce an ML/TF risk assessment of the products.

If the assessment shows a lower level of ML/TF risk, it gives a green light to the country or the regulated entity to simplify AML/CFT measures. If the assessment shows medium or high risk, indicating that applying SDD and other simplified AML/CFT measure is not appropriate, the tool guides the country or regulated entity in trying to reduce that particular financial inclusion product's risk level by modifying its features, functions, and improving the risk mitigation mechanisms. The tool has not only an assessment/diagnostics function, but also a guidance/design component.

2.3. The FATF Standards in the light of Financial Inclusion

83. This section explains how to implement the revised FATF Standards in the light of financial inclusion. It mainly focuses on the 2025 revision of the FATF Standards and other relevant FATF Standards that have been revised since the 2017 Financial Inclusion Guidance. For more details on the implementation of other specific Recommendations in the context of financial inclusion, please refer to Chapter 2 (IV) of the 2017 Financial Inclusion Guidance (extracted in Annex B).

2.3.1. Assessing risks and applying an RBA (R.1)

84. R.1 sets out an overarching, first order principle of the RBA that applies across the FATF Standards, emphasising on the need to understand, identify and assess risks and to apply mitigation and management measures in accordance with the identified risks. The application of RBA is not optional, but a prerequisite for the effective implementation of the FATF Standards.

85. In February 2025, the FATF adopted the revisions to R.1 and its Interpretative Notes (INR.1), along with consequential amendments to other parts of the Standards. These revisions aim to incentivise and provide greater assurance to countries to implement measures proportionate to the risk and in particular simplified measures in identified lower risk situations. The increased focus on proportionality and simplified measures is intended to promote a better

understanding of the RBA and help drive the development of a more inclusive financial system with effective, proportionate AML/CFT measures in place.

2.3.2. Concept of Proportionality

86. One of the key changes in the 2025 revision of the FATF Standards is to formalise the concept "proportionality" as an express objective of the RBA. Prior to the amendment, "commensurate", which has a similar meaning to "proportionate" — corresponding in size, amount, extent, or degree— was used in R.1/INR.1 of the original FATF Standards. The FATF agreed to replace "commensurate" with "proportionate" in R.1/INR.1 and related references, in order to align the FATF's language more closely with that of financial inclusion stakeholders and frameworks and to reinforce the core principle of the RBA .

87. In the context of the RBA in R.1 adopted by the FATF Standards, a proportionate or commensurate measure or action is one that appropriately corresponds to the level of risk and effectively mitigates the risks. The concept of proportionality when implementing RBA is fundamental to AML/CFT decision-making by countries, sectors and regulated entities. Applying a "one size fits all" approach that does not correspond to specific identified ML/TF risk is inconsistent with an RBA, and may place an undue burden on legitimate activities and/or inadvertently discourage them. As a best practice, where there are two or more measures that would both effectively mitigate ML/TF risks, the least burdensome option, having regard to financial inclusion, would typically be the most appropriate option. Requiring the use of enhanced measures by a regulated sector that offers little or no benefit in ML/TF risk mitigation may be considered disproportionate. In contrast, applying SDD measures in providing financial products or services in appropriately defined circumstances (e.g. to certain types of customers), especially for financial inclusion purposes, could be considered proportionate if those circumstances have been identified as lower risk. However, proportionality does not require regulated entities to assess the impact on financial inclusion of each CDD measure and potential additional mitigation action.

2.3.3. Adoption of simplified measures in lower risk situations

88. The original FATF Standards included flexibility for simplified measures, but the wording that countries "may decide to allow" these measures might not have been strong enough to advocate adoption of such measures. To reinforce the FATF's commitment to financial inclusion and create a more enabling environment for implementation of simplified measures, the FATF has changed para. 1 of R.1 from "may decide to allow" to "should allow and encourage". This means that countries are required to not only enable, but also advocate for the adoption of simplified measures in lower risk scenarios. As a baseline, countries should identify[108] areas of lower risk and communicate this information to regulated entities to encourage them to apply simplified measures proportionate to those lower risks. Countries should also provide guidance or information on the possible approaches for the implementation of simplified measures where the risks are lower.

89. In the context of the RBA adopted by the FATF Standards, "simplified measures" refers to AML/CFT measures that countries and regulated entities can take

108 Countries need not designate certain areas as lower risk in every assessment, but rather could highlight those lower risk areas where available, with a view to enabling regulated entities to consider implementing simplified measures.

that are proportionate to assessed lower ML/TF/PF risks. The term includes but is broader than SDD measures. SDD measures refers to CDD measures that regulated entities can take to comply with the requirements implementing R.10 (a) – (d) proportionate to assessed lower risk situations. Beyond SDD, simplified measures may also encompass risk-based simplification of wider AML/CFT measures where appropriate, such as the policies and safeguards applied to specific services and products in the context of a group-wide AML/CFT programme, or simplified nature and intensity of oversight by supervisors, simplified registration and licensing requirements for regulated entities engaged in lower risk activities or operations for or on behalf of customers, etc.

90. Encouragement may take the form of guidance or other communication issued by the government, supervisor or other competent authority to improve understanding of the circumstances when simplified measures may be appropriate and what form they may take, or outreach or other forms of engagement with regulated entities to promote the use of simplified measures in appropriate circumstances, etc. Regardless of the form, 'encouragement' should reiterate the RBA and specifically refer to identified lower ML/TF risks. Policies and practices that create non-risk-based barriers for simplifications (such as persistent and unjustified rejection of financial inclusion product proposals of private sector) would not be in line with this encouragement requirement. There is no implication that encouragement is to be translated directly into legal or regulatory frameworks on the part of the parties involved. Countries have sufficient flexibility to meet the requirement without expectation that the same text should be reflected in their laws or enforceable means. Simplified measures in lower risk scenarios and other examples of proportionate AML/CFT actions are presented in Chapter 3, and additional examples of how encouragement could be translated into actions by countries is further expanded in Chapter 3.

2.3.4. Low risk scenarios and criteria for AML/CFT exemptions

91. Under the FATF Standards (INR.1 para. 2), a country may decide not to apply certain AML/CFT measures to a particular type of regulated entity or activity, in limited circumstances and provided that certain conditions are met. To clarify that making use of exemption is coherent with the RBA, in February 2025, the FATF revised the requirements in INR.1 by removing the word "strictly" when describing limited circumstances and by replacing the word "proven" low risk with "assessed" low risk.

92. The FATF Standards allow countries not to apply some of the FATF Standards requiring regulated entities to take certain actions when there is an assessed low risk of ML and TF; this occurs in limited and justified circumstances; and it relates to a particular type of FI or activity, or DNFBP (INR.1 para. 8a). The main requirement for countries seeking to make use of this assessed low risk exemption will be to demonstrate the limited and justified circumstances pertaining to a specific type of regulated entity or activity, and provide sufficient grounds for the view that there is a low risk of ML and TF. The justification should be based on an appropriate risk assessment and the level of detail will depend on the range and possible impact of the exemption.

93. However, many jurisdictions implement exemptions based on a cursory determination of low risk because of the activity's scale or nature (e.g., leasing, factoring, life insurance) with little or no data to support the risk rating. The World

Bank has developed a tool to assess ML risk of financial inclusion products that may assist countries to undertake the required risk assessments (See Box 7 above and Annex A7). Examples of application of exemptions are further discussed in Chapter 3.

94. The FATF Standards also allow countries not to apply AML/CFT obligations when a financial activity (other than the transferring of money or value) is carried out by an individual or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is low risk of ML or TF (INR.1 para. 8b). To satisfy this exemption criterion, countries must be able to demonstrate a cause-and-effect relationship between the very limited and occasional nature of the financial activity and the assessed low level of ML and TF risk. In implementing this exemption, the duty is on the country to establish that the conditions for the exemption set out in the FATF Standards are met.

2.3.5. Supervision of FIs and DNFBPs

95. On supervisory obligations, under the revised INR.1 para. 9, in ensuring that regulated entities are effectively and proportionately implementing their obligations, supervisors are required to also take into account risk mitigation measures undertaken by regulated entities in addition to their institutional risk profiles and assessments. The changes were made to provide clarity on the supervisory obligations and to align with existing requirements under INR.26 para. 4, which states that AML/CFT supervision of FIs/groups that apply an RBA should encompass, among other things, the adequacy and implementation of its policies, internal controls, and procedures.

2.3.6. Other Recommendations Relevant for Financial Inclusion

96. Apart from R.1, there are a range of other Recommendations that can leverage the flexibility of an RBA to promote financial inclusion, including:

- requirements for CDD (R.10);
- record-keeping (R.11);
- suspicious transactions reporting (R.20);
- reliance on third parties (R.17);
- use of agents of MVTS providers (R.14); and
- internal controls (R.18).

97. In the revised FATF Standards adopted in February 2025, consequential amendments to INR.10 were adopted to reinforce that in lower risk scenarios, countries should allow and encourage FIs to apply simplified measures (including SDD). As the FATF Standards[109] require countries to allow and encourage simplified measures where there is an assessed lower risk of ML/TF (INR.1 para.7. and INR.10. para.16 to 18 and para.21), countries should ensure their AML/CFT regime allows for simplified measures, for specifically defined lower risk customers and products. Countries should encourage regulated entities to decide to apply simplified measures in lower risk situations, based on their own institutional risk analysis. In any case, simplified measures is not permitted if there is any suspicion of ML/TF, or where

specific higher-risk scenarios apply. A detailed description of the other relevant recommendations and associated requirements, as extracted from Chapter 2 Section IV of the 2017 Financial Inclusion Guidance, is at Annex B.

2.3.7. Non-Face-to-Face Business Relationships or Transactions

98. The advancement and increasing use of technological innovations has the potential to improve financial inclusion in circumstances where access to technology and the internet is not impeded). For example, mobile phone banking and mobile payments have increased significantly in recent years (See Figure 3 in Chapter 1) and have the potential to facilitate access to basic services for un/underserved people in remote areas, especially in developing countries. The development of branchless banking channels through non-bank agents (e.g. post offices, petrol stations, lottery kiosks, grocery stores etc.) is similarly promising for enhancing financial inclusion.

99. In this context, it is important to understand the FATF's requirements involving non-face-to-face business relationships and transactions, and to emphasise that the risk posed by such interactions differs greatly between countries' risk profiles. INR.10 para. 15 of the FATF Standards identifies non-face-to-face business relationships or transactions as examples of potentially higher risk scenarios. The FATF Standards also clarify that examples are given for guidance only, and that the risk factors listed may not apply in all situations (INR.10 para. 14). From a financial inclusion perspective, the risks of identity fraud have to be balanced with the ML/TF risks of newly banked people on a case-by-case basis. The application of EDD must be justified based on risk and not applied systematically to non-face-to-face interactions. The FATF Guidance on Digital Identity notes that customer identification/verification measures that rely on reliable, independent digital ID systems, with appropriate risk-mitigation measures in place, may pose a standard level of risk, or may even be lower-risk.[110] On the other hand, technological innovation, particularly the use of artificial intelligence and machine learning, should be coupled with an understanding of and mitigation against algorithmic bias to ensure that marginalised groups are not disproportionately excluded from the formal financial sector as they tend to have a lower digital footprint.

100. Recognising the highly varies risk posed by non-face-to-face interactions and that non-face-to-face interactions have become a standard business practice and advancements in digital identity technologies, the 2025 revision of the FATF standards clarified that non-face-to-face business relationships or transactions are considered as examples of potentially higher risk scenarios under INR.10 para. 15 of the FATF Standards only where appropriate risk mitigation measures have not been implemented. Without appropriate risk mitigation measures, non-face-to-face business relationships and transactions continue to pose challenges and risks, particularly linked to fraud.[111] The use of artificial intelligence and deepfake technologies have posed significant risks to identity verification procedures and these risks may increase as artificial intelligence technologies advances. It is also easier for fraudsters to open and manage multiple accounts, automate transactions, and launder illicit funds remotely, especially with the use of artificial intelligence technologies to mimic real customer behaviours. Regulated entities also face challenges in ensuring

110 See FATF (2020b).

111 A review conducted by The Autorité de contrôle prudentiel et de résolution (ACPR – the French Prudential Supervision and Resolution Authority) in 2024 found that the vast majority of the payment accounts used to launder fraud proceeds had been opened remotely.

the legitimacy of account holders and preventing mule account schemes, where legitimate users unknowingly facilitate fraud.

101. To address these challenges, regulated entities are employing multiple prongs to mitigate these risks. This includes through robust identity verification (e.g. liveness checks, crosschecks of data), transaction monitoring (e.g. biometric authentication, monitoring of device and location changes, profiling system, follow-up communication), and post-transaction checks to detect suspicious activities. See Box 8 below for further details on mitigation measures.

Box 8. Private Sector, Brazil - Multi-layered approach to mitigate the risks associated with non-face-to-face business relationships and transactions

A bank in Brazil employs a robust, multi-layered approach to mitigate the risks associated with non-face-to-face business relationships and transactions in onboarding, transaction and post-transaction stages, addressing issues like identity fraud, scams, and using shell accounts.

Onboarding

- **Facial Biometrics**: The bank validates identity using facial biometrics, including liveness checks, and matching facial data with internal databases. Analytical models are used to enhance fraud detection accuracy. Online account initiation and deposit require biometric validation through the institution's app to prevent fraud.
- **Data Validation**: Digital and registration data captured during account creation are cross-referenced with historical databases and restrictive fraud databases to identify dubious proposals.
- **Documentation Validation**: If facial biometrics are unavailable, documentation is validated using external tools. Machine learning models, like logistic regression and decision trees, are in place to identify suspect cases of fraud based on historic fraud data.
- **Know Your Customer (KYC) Process**: The KYC process verifies customer information, ensuring consistency and resolving discrepancies. The customer's data is validated against the institution's internal systems to ensure authenticity and legitimacy.
- **Continuous Review**: Rules and thresholds are regularly adjusted to align with emerging fraud trends, and proposals are flagged for manual review if necessary.

Transaction Monitoring (Real-Time)

- **User Authentication**: Multiple authentication mechanisms, including passwords, tokens (for two-factor authentication), and biometric verification, are employed for access to banks channel, monetary and non-monetary transactions.
- **Behavioural Profiling**: The bank's system tracks the user's digital habits, including device usage, IP address, Wi-Fi network, geolocation, and behavioural biometrics. This data is used to create a profile and detect anomalies in user

behaviour, which are flagged for review.

- **Artificial Intelligence and Machine Learning Models**: The institution uses artificial intelligence models to assess transaction risk based on factors like transaction value, time, and customer characteristics (e.g., age, segment). The models predict the likelihood of fraudulent behaviour by evaluating over 60 variables.
- **Communication for Confirmation**: If an anomaly is detected, the transaction is delayed, and the customer is notified. Communication with the customer will be conducted via instant messaging tools or phone call. lf the customer recognises the transaction, the operation is released and follows the normal path to conclusion. If the customer doesn't recognise the transaction, the operation is denied, and the account is preventively blocked.

Post-Transaction Monitoring

- **Risk Analysis**: Use of statistical techniques (e.g., outlier identification, clustering methods, logistic regression, machine learning models like Random Forest and Gradient Boosting) to analyse transaction materiality, customer behaviour, and external factors.
- **Specific Controls for Risk Typologies**: Tailored controls target specific risks, including electronic foreign exchange onboarding, payment institution anomalies, influencer monitoring, shell companies, and crypto-asset activities using statistical models and risk-focused methodologies.
- **Identification of Risks associated with Remote Transactions**: The bank put in place several broad rules aimed at identifying risks associated with remote transactions, including contaminated counterparties tracking, incompatibility of transaction flow versus income, AML complaint monitoring, regular KYC updates for ongoing customer profiling.
- **Risk Classification Tool**: Monthly evaluation of customer risk profiles based on variables like reputational, transactional, and personal data. Customers are classified into four risk levels (Very Low, Low, Medium, High).

By combining advanced biometrics, AI-driven transaction monitoring, real-time alerts, communication channels for transaction confirmation, and continuous KYC updates, the institution mitigates risks associated with non-face-to-face transactions and business relationships.

2.3.8. NPOs

102. In addition to these Recommendations, the FATF's amendments to R.8 and INR.8 on NPOs are also relevant to supporting financial inclusion. Risk-based treatment of NPO is also important from a financial inclusion perspective, as disproportionate obligations may result in undermining financial inclusion objectives by driving NPOs to unregulated financial and payment services as a result of their inability to gain access to regulated financial services or increased costs of compliance that acts as a barrier to maintaining activities. In turn, this might unduly hinder the delivery of humanitarian assistance and affect the sustainable development goals and economic and human rights. For detailed discussion and guidance on implementation

of revisions to R.8, please refer to the Best Practice Paper on Combating the Abuse of NPOs.[112]

112 See FATF (2023).

Chapter 3. Risk-based Initiatives to support Financial Inclusion

103. Building on the principles of RBA discussed in Chapter 2, this chapter covers the challenges and potential barriers to effective implementation of the RBA and simplified measures (Section 3.1), describes how policymakers, supervisors and regulated entities can leverage the flexibility embedded in the RBA to promote financial inclusion while maintaining the integrity of the financial system, focusing on application of simplified measures in lower risk situations (Section 3.2). Section 3.3 presents practical guidance on applying proportionate measures to support financial inclusion (including simplified measures for lower risk situations and tailored measures for non-lower risk situations). Examples of best practices from a variety of jurisdictions and sectors in applying the RBA, including simplified measures and exemptions, can be found in Annexes A1-A6. These examples are intended to serve as valuable resources for countries looking to refine their implementation of the RBA and ensure that their AML/CFT measures are both effective and inclusive

3.1. Institutional Challenges to Adopting RBA and Simplified Measures

104. Although the adoption and implementation of simplified measures are often met with various institutional challenges, the 2025 revision of the FATF standards requires countries to allow and encourage the use of simplified measures, providing countries with an opportunity to address such concerns. These challenges can stem from regulatory uncertainties and the risk appetite of regulated entities. Addressing these obstacles requires a nuanced understanding of the concerns faced by policymakers, supervisors, and regulated entities. Institutional barriers to adopting simplified measures may include:[113]

- Legal and regulatory barriers: Legislative and regulatory requirements may restrict the use of certain technologies for CDD. For example, strict regulation on the use of biometric data due to privacy and personal data protection concerns.
- Messaging from regulators/supervisors: Regulators and supervisors may put too much emphasis on EDD for higher risks situation and not enough emphasis on SDD for lower risk situations. The FATF and other standard-setting bodies have moved to an RBA in recent decades, and most national laws and regulations now include such risk-based requirements. However, many authorities still retain elements of a "rule-based approach" to supervision which can deter and discourage regulated entities from applying an RBA, including risk-based measures to encourage financial inclusion, leading to the incorrect expectation that regulated entities should "avoid" rather than "mitigate" risks.
- The perceived lack of benefit: Simplified measures can be viewed as exposing regulated entities and policy-makers to risk that may arise as a result of the simplified controls, e.g. in relation to TF risk where the FATF

113 See De Koker, L. and Symington, J. (2014); De Koker, L. and Casanovas, P. (2024); Alliance for Financial Inclusion (2020).

advises that even lower value transactions may pose a risk.[114] Potential ease of access for criminals may put the regulated entity's reputation at risk.

- Requirements to adjust and update simplified measures: Due to changing risks and circumstances the simplified measures may need to be revisited and adjusted, potentially at significant cost. Industry often observes that fine-tuning CDD is more complex and comes with higher costs while it is cheaper and easier to manage more consistent CDD measures.
- Maintaining access to correspondent banks: Regulated entities may be concerned that international counterparts, such as correspondent banks, will question whether risks have been adequately assessed and mitigated. This is more pronounced when some instances of abuse occurred, even where limited.
- Complexity of technological implementations: Regulated entities, especially small and medium-sized ones, may face difficulties in implementing or integrating new technologies for non-face-to-face onboarding to better enable financial access, such as biometrics or electronically certified copies of documents, which can require significant financial investment and development time.

105. Institutional barriers differ by country and by sector. It is therefore important to engage the regulated entities to understand their concerns and approaches. This collaborative approach will enable policymakers, supervisors and regulated entities to develop measures that balance AML/CFT needs with financial inclusion objectives. Competent authorities should provide positive commentary on financial inclusion efforts by regulated entities, and should likewise be mindful of their own assumptions, approaches and conditions that may create internal disincentives or barriers to providing effective support for simplified measures and exemptions.

3.2. Legal and Operational Framework for Simplified Measures

106. Policymakers, supervisors, and regulated entities each play very important roles in shaping and implementing a legal and operational framework conducive to financial inclusion that addresses potential barriers while also supporting effective risk management. An understanding and appropriate demarcation of each of the key players' distinct roles is an essential building block in creating a coordinated approach that can facilitate efforts to identify and mitigate obstacles to implementing an effective, proportionate and efficient AML/CFT regime.

107. Policymakers develop and issue regulations that allow and support the adoption of simplified measures, while supervisors play a crucial role in guiding and overseeing the application of these measures. Regulated entities, in turn, need to align their internal processes with the RBA, ensuring that simplified measures are effectively implemented. The following sub-sections further elaborates on each of these roles.

114 See FATF (2019a).

3.2.1. Legal Framework and the Role of Policymakers

108. A country's AML/CFT legal framework should expressly allow for regulated entities to implement simplified measures where lower risks are identified, and should avoid making the framework overly prescriptive or stringent. Further, legal/regulatory frameworks should support supervisors in allowing, assessing and supporting entities' use of simplified measures, as derived from the regulated entities' risk assessments. The legal framework should also allow appropriate flexibility for regulated entities to adjust simplified measures to the assessed risk, and facilitate information exchange between competent authorities and regulated entities to support an informed and effective RBA. A legal framework that is too rigid may stifle the efforts of the regulated entities to implement proportionate measures .

109. Policymakers can design financial inclusion strategies with consideration of intersections with AML/CFT measures, and ensure consideration of financial inclusion measures in competent authorities' development of NRA and additional sectoral risk assessments, which regulated entities should take into consideration in developing institutional risk assessments and designing simplified. In the process, countries should conduct early and ongoing consultations with non-governmental stakeholders such as the private sector and civil society to address concerns and avoid unintended consequences.

Box 9. Egypt and India frameworks to support financial inclusion

This box provides an overview of the examples in Boxes 2.2 and 3.3 (Annex A2 and 3).

In 2020, the Central Bank of Egypt, and the Egyptian Money Laundering Combating Unit jointly issued several regulations aimed to enhance financial inclusion while maintaining financial stability and protecting the rights of customers. These measures included SDD for individuals and micro-enterprises, easier account opening for youth and informal workers, use of service providers for customer verification, etc. The Central Bank of Egypt also supported these efforts through training and infrastructure development, encouraging tailored financial products for diverse groups like women, youth, and people with disabilities.

India created a solid institutional framework to coordinate and support its Financial Inclusion strategy. The National Strategy for Financial Inclusion for India 2019-2024 provides (1) an analysis of the status and constraints in financial inclusion in India, (2) specific financial inclusion goals, (3) a strategy to reach the goals and (4) mechanisms to measure progress. It is prepared by the Reserve Bank of India and reflects the outcomes from wide-ranging consultation with relevant stakeholders.

3.2.2. Role of Supervisors

Examples relevant to this section can be found in Annex A3.

110. This sub-section examines the role of supervisors in implementing the RBA pursuant to the FATF Standards.[115] This includes important elements of supervision which can be critical to enabling financial inclusion, and in particular the implementation of simplified measures in lower risk situations. The discussion focuses on obstacles to implementing simplified measures and how supervisory authorities can address them.

111. Supervision provides an essential link between a country's legal framework, its NRA and sectoral risk assessments, and the preventive measures adopted by regulated entities. Supervisors shape the regulated entities' risk understanding and approach to AML/CFT compliance by setting regulatory expectations and incentives; providing clarifying guidance, instructions, best practices guidelines; sharing information on specific ML/TF typologies, alerts, other risk information; and conducting enforcement actions.

Risk-Based Supervision and Guidance as a Facilitator of Financial Inclusion

112. The FATF Standards underscore that countries are required to adopt the RBA to supervision, thereby comprising a critical element of financial inclusion. Risk-based supervision has two basic elements:

a) The RBA to supervision and inspection by which a supervisor, according to its understanding of risks, allocates its resources to AML/CFT supervision by considering the nature, frequency, intensity and focus of supervision and the thematic issues reviewed, based on the degree and type of risks assessed across the sector; and

b) Supervisors assessing how regulated entities implement the RBA which includes the supervisory assessment of the regulated entity's risk-based measures, by which a supervisor reviews the entity's risk understanding/assessment, proportionality and effectiveness of the measures applied on the basis of the entity's risk assessment, clarifies compliance requirements, sets expectations and provides guidance and information on best practices to implement the requirements.

113. A sound approach to risk-based supervision will make both elements risk-based, and a shared understanding of risks between supervisors and regulated entities is fundamental to achieve this. In implementing the first element, supervisors should allocate resources in line with the ML/TF risks in the sector they supervise, where appropriate. Within a risk-based supervision framework, it is expected that there will be areas and segments of regulated entities that are assessed to be of lower ML/TF risk, in which case lesser supervisory actions could be taken (for details on supervisory actions in line with risk, see FATF Guidance on Risk-Based Supervision

115 The FATF has required countries to adopt risk-based supervision since the 2012 Amendments to the Recommendations. See R.26 (risk-based supervision of financial institutions) and R.28 (risk-based supervision of DNFBPs).

published in 2021, in particular Section 3.5 on supervision of lower risk sectors and entities).[116]

114. To support financial inclusion, supervisors should engage with lower risk sectors to ensure measures are proportionate to the assessed risk. Disproportionate legal or regulatory obligations, supervisory expectations and lack of guidance from supervisors may result in the application of unnecessarily prohibitive CDD and other AML/CFT controls in lower risk sectors.

115. Supervisors should ensure that education and outreach extend to lower risk sectors to enable them to implement risk-based, proportionate measures and to help identify and report any ML/TF risks that may arise. With reference to national financial inclusion objectives, supervisors can also play a role in: a) reducing requirements on lower risk entities; b) reassuring other regulated entities that provide financial services to lower risk entities those lower risk entities are adequately supervised. While supervisors may devote less resources to lower risk areas, they should still verify and monitor risk understanding and mitigation measures of those areas.

116. Building up an appropriate and balanced AML/CFT regime based on domestic circumstances requires extensive coordination among competent authorities and effective partnerships between public authorities and the private sector. Effective information exchange and coordination mechanisms are vital for balancing AML/CFT priorities with broader financial inclusion strategies. Multi-stakeholder coordination forum can ensure consistency, reduce duplication of efforts, and foster collaboration among key stakeholders. (See Box 10 and Annex A3 for examples of coordination efforts to support financial inclusion).

116 See FATF (2021a) for detailed guidance on the general process by which a supervisor, according to its understanding of risks, should allocate its resources and adopt risk-appropriate tools to achieve effective AML/CFT supervision.

Box 10. France, Lesotho and The Netherlands' supervisors' guidance and coordination efforts to support financial inclusion

This box provides an overview of the examples in Boxes 3.2, 3.4 and 3.5 (Annex A3).

In France, the Ministry of Europe and Foreign Affairs has set up a multi-stakeholder working group to discuss potential undue restrictions on NPOs and facilitate the mutual understanding of banks' regulatory constraints and compliance requirements set by NPOs' financial backers. The discussions led to the publication of a guide dedicated to the access to financial services of NPOs.

The Central Bank of Lesotho has developed a Risk Management Guidelines for FIs focusing on the RBA and customer due diligence. The Financial Inclusion Steering Committee is the authority responsible for promoting cooperation between different government agencies and the regulator to support financial inclusion. The national Financial Inclusion Forum convenes all financial sector players quarterly on AML/CFT and financial inclusion matters.

In The Netherlands, over the last years, a number of initiatives has been undertaken to engage with, provide guidance and encourage the industry to better implement the RBA in application of the Dutch AML Act. The activities resulted in the publication of an AML/CFT guidance by the Dutch Central Bank and the creation of risk-based industry baselines and sector baselines for sectors most impacted by de-risking (e.g. NPO) by the Dutch Banking Association. Together with other relevant parties, the Dutch Central Bank has also organised multi-stakeholders' forums, events and roundtables.

Shared understanding of the risks

117. Under the RBA, regulated entities are often reluctant to apply simplified measures on the basis of their own institutional risk assessments for fear of inconsistency with the supervisor's risk understanding and possibility of enforcement action. A shared understanding of the ML/TF risks, facilitated by open and collaborative information sharing, can help to ensure that regulated entities institutional risk assessments are sufficient and enable entities to have confidence in their assessments to apply risk-based measures (such as SDD for lower risk situations, or appropriate risk mitigation measures to enable the onboarding of higher-risk customers). Such a shared understanding also deepens supervisors' understanding of the risks faced by regulated entities, enabling more comprehensive and accurate evaluation of the adequacy of the regulated entities' compliance.

118. Competent authorities have a variety of ways to develop and effectively communicate their understanding of relevant risks to regulated entities, as well as to other stakeholders, including financial inclusion officials and advocacy organisations, economic development organisations, technical assistance providers and the general public. In addition to publishing the results of the country's NRA or sectoral risk assessments, regulators can publish illicit finance typologies, issue red flag alerts targeted at particular risks, provide trend analyses involving certain products, services, specific sectors, and/or types of ML/TF and fraud activities. They can also conduct outreach to regulated entities regarding country risk assessment findings,

share information about ML/TF risks obtained from enforcement actions or law enforcement investigations and promote the government's AML/CFT priorities.

119. In addition to providing appropriate risk information, supervisors may provide guidance to regulated entities on how they can conduct an appropriately scoped, data-driven institutional risk assessment. The goal is that regulated entities are able to formulate sufficiently rigorous risk assessments, that can be used as the basis for risk-based CDD measures. Where institutional AML/CFT risk assessments are overly conservative or insufficiently nuanced, it can result in control measures that are not proportionate to identified risks.

120. Supervisors can also initiate public-private partnerships that enable relevant components of the private sector (including regulated entities and their industry organisations) to contribute to the development of the country's NRA or sectoral risk assessments. The public-private partnership approach can gather inputs from a broader range of relevant sources, improving the accuracy of the assessment itself and increasing stakeholder confidence in it. Public-private partnerships can also help ensure that the risk assessment addresses the right questions at the right level of granularity.

121. The supervisory and inspection process is another mechanism that supervisors can leverage to help strengthen regulated entities' understanding of ML/TF risks. Using an RBA to supervision, and taking into account the degree of discretion allowed under it, supervisors should review the regulated entity's ML/TF risk assessments, customer and product risk profiles, and risk mitigation measures. In doing so, supervisors may assess the adequacy of its policies, internal controls, and procedures and the effectiveness of their implementation, and engage with the regulated entity on the results of this review.

Identifying and understanding factors impeding regulated entities' adoption of RBA to CDD

122. When inspecting individual regulated entities for compliance with their AML/CFT obligations, supervisors should take into account the degree of discretion allowed by the RBA, review the risk profiles, risk assessments and risk mitigation measures of the regulated entity, and assess the adequacy and implementation of the policies, internal controls and procedures they have applied on the basis of its risk assessment.

123. In addition to promoting a shared understanding of risk, supervisors should develop a nuanced understanding of the factors that may deter regulated entities from applying proportionate measures to different risk situations and may take effective action to address them. The potential disincentives for regulated entities to adopt an RBA to CDD include inherent risk and liability concerns, and limited expertise in carrying out institutional risk assessment, which can result in overly cautious assessments and the implementation of more stringent controls than necessary.

124. Over-compliance with AML/CFT measures ("*gold-plating*") often leads to financial exclusion and diverts entity's resources from proportionate risk assessment. Regulated entities have limited incentive to onboard marginalised groups due to low profitability or to real or perceived exposure to reputational injury, while the social costs, including higher ML/TF risks, consumer fees, and financial exclusion, are borne by society.

125. Supervisors can play a critical role in helping regulated entities navigate their concerns and encouraging adoption of simplified measures by providing clear guidance, best practices, and other information to ensure that regulated entities understand their obligations regarding the need to apply an RBA. For example, where the supervisors have identified overly conservative approaches,[117] they should consider not only providing the necessary guidance to the individual regulated entity, but also to the relevant sector/sub-sector on how to improve their CDD risk assessment and mitigation methodologies and practices.[118] By fostering a constructive and supportive relationship between competent authorities and regulated entities, supervisors can ensure that compliance measures are proportionate to the risk without discouraging the use of simplified measures. Supervisors may also address decisions by regulated entities to refuse to open or to terminate business relations with entire classes of customers as part of the inspection process. Where necessary, supervisors may follow up on individual inspection by making recommendations to the regulated entities to help them manage their ML/TF customer and product/service risks.

126. Supervisors should also help regulated entities understand the information that can be accepted in situation where customers lack certain documentation. Overly prescriptive requirements may inadvertently exclude customers who cannot provide certain document (e.g. proof of address for persons without fixed residence), and authorities may consider what acceptable information may be appropriate to enhance financial inclusion.

127. Some countries opt to ring-fence (separate out) risk management decisions relating to establishment, termination or limitation of business relationships by recognising a legal right to a payment or basic/limited account (see Box 11).

117 See De Koker and Symington (2014); Ferwerda and Reuter (2022); De Koker and Casanovas (2024).

118 See FATF (2016a), para. 136 for supervisory guidance where overly conservative approaches are identified.

Box 11. El Salvador; European Union, Hong Kong, China; Indonesia and Jordan's examples of right to basic/limited products and services

This box provides an overview of the examples in Boxes 4.2, 4.4, 4.5, 4.6 and 4.7 (Annex A4).

Between 2019 and 2022, El Salvador authorities, the Hong Kong Monetary Authority, the Indonesian Financial Services Authority and the Central Bank of Jordan introduced the requirement for banks to provide simplified bank accounts under specific conditions (narrower service scope, lower transaction volume, specific categories of customers such as legally qualified, financially excluded citizen, etc.). A notable outcome of the measures in El Salvador is that in June 2024, the total number of savings accounts reached 138 924 held by women and 159 294 held by men. As for Hong Kong, China, there were eight banks offering Simple Bank Accounts services, and the cumulative total number of such accounts has increased to over 21 000 as of 2023.

The European Union's revised Payment Services Directive (PSD3) provides third-party payment service providers with access to payment accounts. This is for example recognised in France (see Annex 4.4),[119] Monaco,[120] and Belgium.[121] In these countries, FIs/DNFBPs are not allowed to manage their ML/TF or prudential risks by simply excluding customers. The legal right to a payments account is generally limited because regulated entities are entitled to exclude customers when they can provide sound reasons for such exclusions. Customers may appeal those decisions and, if successful, may be assigned to that institution or another institution.

128. In some countries, in addition to policymakers and regulators, supervisors are also empowered to authorise the implementation of simplified measures in lower-risk situations. In this context, a more concrete specification by the supervisors of the circumstances in which such measures will be applied can provide certainty and better encourage the private sector to implement simplified measures. Such an approach also reduces the need for regulated entities or individual compliance staff to rely solely on their judgement and discretion, and therefore enables more confidence when applying simplified measures. Nevertheless, the FATF does not advocate for a specific approach and while some jurisdictions may benefit from jurisdictions specifying when simplified measures can be implemented, other jurisdictions benefit from providing greater flexibility.

129. At the higher end of the risk spectrum, supervisors should recognise that even sound risk assessments and appropriate mitigation measures cannot prevent all

119 In accordance with article L.312-1 of the Monetary and Financial Code, the right to the bank account is reserved for the following beneficiaries: any natural or legal person domiciled in France; any natural person legally residing in another Member State of the European Union who is not acting for professional purposes; any natural person of French nationality residing outside France.

120 According to Loi n° 1.492 du 8 juillet 2020 relative à l'instauration d'un droit au compte, any person of Monegasque nationality, who is resident or in the process of moving to Monaco, or financial agent appointed by a candidate in an election, may open a bank account in the Principality with a banking establishment of his or her choice

121 According to Article VII. 57 (2) of the Belgian Economic Law Code, any individual legally residing in a European Union Member State is entitled to a basic bank account.

ML/TF activity. The RBA requires regulated entities to assess and understand target systemic ML/TF risks and common typologies, and take proportionate mitigation measures – not to imply a "zero failure" approach.[122] Supervisors must distinguish between isolated breaches of otherwise sound measures and compliance failures due to inadequate risk assessments or mitigation. Without this distinction—and the clear and convincing communication to regulated entities of the policies and supervision/inspection procedures implementing it— the flexibility allowed to regulated entities under the RBA to adopt simplified measures could potentially give rise to a (real or perceived) zero-failure regime, discouraging the adoption of simplified measures and the effective implementation of the RBA. Clear specification of supervisors' roles is crucial to support on the ground adoption of the RBA that supports financial inclusion.

Providing support to enhance institutional capacity

130. A key aspect of this involves ensuring that staff within regulated entities is adequately trained and possess the necessary skills to assess and mitigate ML/TF risks proportionately. Supervisors can encourage or provide targeted training programs that focus on equipping regulated entities' staff with a clear understanding of how to apply an RBA, including the effective implementation of simplified measures in lower-risk situations. Such training should be periodic and tailored to the specific challenges that regulated entities face based on the risks identified in the country's and/or entity's risk assessment.

131. In addition to formal training, supervisors should promote a culture of risk-awareness within regulated entities by continuous sensitisation efforts. This could be achieved through workshops, seminars, and scenario-based exercises that address the evolving nature of ML/TF risks, as well as the latest AML/CFT regulatory expectations. Supervisors can also issue guidance notes, typology reports, and case studies that highlight best practices in applying RBA and simplified measures. These initiatives can be designed to ensure that staff at all levels of the entity—from frontline personnel to senior management—are not only familiar with the concept of an RBA but are also capable of making informed decisions when applying such measures in real-world situations.

132. Capacity building goes beyond training; it requires the creation of institutional structures and resources that support the effective application of an RBA. Supervisors can encourage regulated entities to invest in technology and data analytics tools that can help staff assess risks more accurately. Moreover, supervisors may consider offering advisory services and establish public-private collaboration platforms to facilitate regular interaction between regulatory bodies and the regulated entities. This interaction allows entities to receive tailored feedback on their risk assessments and control measures and fosters an environment where entities can raise concerns about challenges faced. By offering such comprehensive support, supervisors ensure that regulated entities are not only compliant but are also empowered to take a proactive role in risk management and financial inclusion efforts. Supervisors may furthermore support the establishment of public-private electronic KYC utilities and collaborative CDD approaches to improve the effectiveness and efficiency of CDD measures of regulated entities.[123] India's electronic KYC support via Aadhaar (see Box 6.16) and the Asian Development Bank's

122 See FATF (2014a).
123 See Lyman et al. (2019)..

support for electronic KYC systems in the Pacific[124] are good examples of collaborative measures that lower compliance costs for regulated entities while improving the outcomes.

133. Sometimes FIs may feel compelled to impose stricter than necessary measures to their customers where they have correspondent banking relationships and require payments to be made to foreign jurisdictions. Due to differing views in risk assessment and risk tolerance, respondent FIs are sometimes compelled to adhere to the stricter AML/CFT standard expected by foreign correspondent banks. This may impact the respondent FI's ability and willingness to accept or process transactions for those customers deemed to be of lower risk and impact financial inclusion. Strengthening the capacity of local respondent FIs will help demonstrate robust compliance to AML/CFT standards and increase foreign correspondent banks' confidence in their risk mitigation regime and reduce the need for overly strict measures (see for example, the Pacific Island Correspondent Banking Relationship Roadmap project mentioned in Section 1.5 above).

3.2.3. Role of Regulated Entities in applying RBA to CDD

134. Regulated entities are responsible for applying an RBA to develop and operate AML/CFT policies and procedures that are proportionate to the identified risk, and consistent with the national policy framework and supervisory guidance. An appropriate application by regulated entities of the RBA to CDD that enables the use of SDD is critically important to advance financial inclusion objectives in the AML/CFT context. This section focuses on customer identification/verification at onboarding, and ongoing due diligence on the business relationship.

135. Regulated entities should continuously review their SDD measures and modify according to the evolving risk environment. This includes continued dialogue with supervisors on the functioning of SDD measures. They should also provide adequate training to their staff on the proper application of RBA, including simplified measures.

Customer identification and ongoing due diligence

136. Customer identification/verification occurs at the point persons first engage with regulated entities. Complying with customer identification/verification requirements is the main challenge for regulated entities' seeking to onboard previously un/underserved individuals. As noted in previous chapters, un/underserved persons often lack traditional identity documentation. They also lack a transaction or credit history in the regulated financial sector, which might otherwise provide additional or alternative data for customer identification.[125] Given the potential negative impact of customer identification and verification, most AML/CFT-related financial inclusion initiatives focus on enabling simplified customer identification/verification measures.

137. The RBA to CDD involving customer identification and verification is commonly reflected in the following three-step process, which emerges from various case studies and examples of how countries are implementing this approach effectively. These steps are grounded in the practical experiences of jurisdictions

124 See for example Reserve Bank of Fiji (2024).

125 Transaction and credit history is also highly useful for complying with R.10(c) requirements to understanding the purpose and nature of the business relationship at onboarding.

applying SDD and mitigating measures in lower-risk situations. It is intended to help regulated entities apply the RBA to comply with their CDD obligations, and is in no way mandatory. As the case studies and country examples provided in this Guidance illustrate, there are many ways regulated entities can implement SDD measures in lower risk situations.

138. **Step One—Identify and assess all relevant ML/TF risks**: Data driven institutional risk assessment helps ensure that financial inclusion measures are balanced with effective safeguards against ML/TF risks, while promoting safe access to financial services for marginalised groups. Institutional risk assessments may consider factors such as customer risk, including risks related to un/underserved persons, the source of funds, and the availability of reliable identity evidence etc. Additionally, risks pertaining to product, service, transaction, and delivery channels may also be assessed. The factors pertaining to the effectiveness of remote identification, the integrity of agent networks, and the use of innovative technology should also be taken into account. It is important that the risk assessments be sufficiently detailed to enable the effective and proportionate mitigating measures. This is sometimes impeded by overly broad customer risk categorisations (e.g. into broad buckets of high, medium, low risk) and subsequent adoption of a blanket approach in mitigating measures which may be excessive or insufficient. In identifying risk, regulated entities should consult the country's risk assessments, or risk-related information or guidance provided by competent authorities (see Section 3.2.2 on the role of supervisors and the importance of developing a shared understanding of ML/TF and financial exclusion risks).

139. There may be situations where a regulated entity's institutional risk assessment does not align with the findings of the country's NRA and/or sectoral risk assessments, or where new financial products and services are not adequately covered by the past assessments. These differences should be justified and explained by the regulated entity in its institutional risk assessment. In cases these differences persist, the entity should take additional steps to ensure that its approach remains risk-based and compliant. In cases where new products are involved, regulated entities should conduct their own rigorous risk assessments, leveraging available data, relevant sectoral insights, and any updated risk guidance issued by competent authorities. Depending on the nature of the difference, the regulated entity may consider engaging with competent authorities to clarify any discrepancies and seek guidance on addressing the gaps between its institutional assessment and the NRA and/or sectoral risk assessments as appropriate. Dialogue with the authorities could help resolve differing views of risk assessments, which may result in overly conservative approaches and prevent simplified measures.

140. **Step Two—Identify risk mitigating measures**. When deciding on potential mitigating measures, regulated entities should consider differentiating between different types of CDD measures and their levels of intensity and assessing their effectiveness and proportionality to identified risks, depending on the type and level of specific, disaggregated risk factors. When there are several effective measures to fulfil the AML/CFT requirements, regulated entities should consider adopting the least invasive option to avoid placing undue burden on customers—particularly un/underserved populations. For example, regulated entities could consider applying SDD measures for customer acceptance but normal or even enhanced ongoing due diligence and transaction monitoring or vice versa to effectively and proportionately mitigate ML/TF risks, while facilitating financial inclusion (see Box 12 below).

Box 12. Private Sector, Indonesia – SDD for onboarding followed by normal CDD

This box provides an overview of the examples in Box 5.13 (Annex A5).

In Indonesia, a bank offers Basic Saving Account products to its customers, subject to annual maximum thresholds on savings and transactions. When a prospective customer is onboarded, SDD is carried out by requesting verification of a minimum of five pieces of data relating to the customer, made on the government database. However, when the customer wants to collect its debit card, he/she must go in-person to the nearest branch and provide necessary customer data and information to complete regular CDD procedures.

141. Regulated entities should think broadly about potential mitigating measures, including ways to leverage innovative technologies or service delivery platforms to provide additional safeguards as well as financial inclusion.

142. While the application of appropriate CDD is essential for lower-risk customers, it is crucial to also address the challenges faced by un/underserved persons who may be classified as higher risk, particularly those who are under-documented. As explained earlier, regulated entities are only required under FATF Standards to terminate or reject customer relationships, on a case-by-case basis, where the ML/TF risks cannot be mitigated. Regulated entities should include in their policies, procedures, and controls a range of options for mitigating higher ML/TF risks, before resorting to customer rejection on risk grounds. These options could include EDD measures, increasing the level and intensity of transaction monitoring, offering limited or basic services with set prices, and applying targeted restrictions to products or services. Additionally, regulated entities' risk assessments should consider the impact of reduced due diligence on the overall risk levels, particularly when alternative forms of identification are accepted for customers who are unable to provide traditional identity documentation.

143. **Step Three—Apply proportionate CDD measures to the identified** risks. Regulated entities should consider applying customer identification/verification processes and mitigation measures tailored to the type and level of risk. Regulated entities might also reduce the risk associated with financial inclusion products and services by subjecting these products to restrictions of functionalities to limit the attractiveness to criminal abuse. For instance, regulated entities could consider tiered or progressive accounts where customers have access to a range of different account functionalities depending on the risks associated with the functionalities/products/services offered and the level of customer identity verification and other CDD applied, with greater functionality and risk requiring a higher level of identity verification and more intensive CDD processes. Though further detail is provided in section 3.3, SDD measures for lower risk situations could include one or more of the following:

- Alternative and new means of identification methods (e.g. non-documentary identity verification procedures, range of government-issued identity documents, biometrics, voice prints, electronically certified copies, digital identity solutions);

- Specific means of identification for targeted groups of customers (e.g., asylum seekers and refugees, First Nations communities[126]);
- Reducing the extent of information required;
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- Identifying and verifying the beneficial owner based on information from the customer's profile;
- Inferring the purpose and nature from the type of transactions or business relationship established;
- Simplified onboarding procedures with ongoing monitoring of relationships;
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions based on reasonable monetary threshold; or
- Leveraging mobile payments systems safeguards and digital data, including device-based data, as part of customer identification/verification and to support ongoing due diligence.

These measures are for illustrative purposes, and by no means exhaustive nor prescriptive.

3.3. Implementation of Proportionate CDD Measures to Support Financial Inclusion

144. The implementation of CDD measures that are proportionate to the relative risks of a product can significantly increase access and use of financial services. The section describes examples of tiered CDD, and products/services offered with limitations that mitigate risks (Section 3.3.1), SDD measures to facilitate financial inclusion (Section 3.3.2), making use of exemptions in assessed low risk scenarios (Section 3.3.3), tailoring measures to identified risks (Section 3.3.4), and making use of digital tools to promote financial inclusion (Section 3.3.5).

3.3.1. Tiered CDD approach and limitations on products and services

145. When "progressive" or "tiered" CDD measures are applied at the on-boarding stage, the intensity of the monitoring process can be continuously adjusted to mitigate the inherent risks of the financial products and use by the customer, as a proportionate response to the 'relaxed' initial due diligence checks. Many countries have developed entry-level types of financial products with in-built mitigation measures, such as limitations on the product's functionality or availability, or incorporating a tiered CDD approach.

146. The specific features of a tiered CDD approach can vary, but fundamentally provide customers with access to a range of different account functionalities dependent on the extent of identification/verification conducted by the regulated entity. Strict pre-set thresholds are defined for the various account levels. Access to

126 Refer to Box 6.1 in Annex A6 for Australia's approach to specific means of identification for First Nations communities.

the basic, first level set of services is provided upon minimum identification. Access to the subsequent account levels (i.e. tiers) and additional services (e.g. higher transaction limits or account balances, diversified access and delivery channels) is allowed only if/when the customer provides the required additional identification/verification information. In the meantime, the accounts have limited services). The number of tiers in the CDD regime should depend on the characteristics of the financial products and the needs of the un/underserved groups.

147. Countries may prescribe the strict parameters applicable to tiered CDD products, or enact a more flexible framework that enables regulated entities to develop their own parameters, according to the regulated entities' own criteria, account design and evaluation of identified risks. Regardless of the chosen approach, supervisors should work closely with regulated entities to provide feedback on the effectiveness and suitability of the products. This feedback should assess the proportionality of the parameters in line with identified risks, and confirm that they will have the resources and capacities to implement such a scheme.

148. Risks that otherwise may arise from financial inclusion products and services can be proportionately mitigated when they are subject to restrictions or have certain features that address ML/TF risks identified in a risk assessment.[127] Such restrictions limit the attractiveness of the relevant products and services to criminal abuse, as well as the consequences of any abuse that may occur. The type of the restrictions required and whether more than one type of restriction will need to be imposed will depend on the risks identified during the risk assessment (see below for relevant factors to consider and possible variations).[128]

Examples of factors to consider in developing financial inclusion products, including progressive CDD

- the profile of the un/underserved groups;
- the financial needs of the un/underserved groups;
- the ML/TF risks in the country;
- the AML/CFT measures already in place;
- the existence of a national identification register;
- the technology available to monitor transactions, etc.

Possible variations/measures

- restrictions on the way the business relationship is established, or transactions are conducted (e.g. face-to-face only, or non-face-to-face with proper safeguards applied);
- limitations on the holder/beneficiary of the product (e.g. only natural persons who are nationals);
- limitations on the functionalities of the product, such as geographical scope of the transactions (e.g. only domestic transactions or no cross-border transactions with countries with higher ML/TF risks), caps on daily/monthly withdrawals, deposits limits, the number or total value of

127 See Basel Committee on Banking Supervision (2016):29.
128 See Basel Committee on Banking Supervision (2015):41.

transactions per week/month, the amount per transaction, the overall monthly balance, the overall value of the account, etc.

Box 13. Mexico and the United States' tiered CDD approach

This box provides an overview of the examples in Boxes 5.5 and 5.11 (Annex A5).

In Mexico, the Ministry of Finance amended the AML/CFT framework to introduce (1) the classification of bank accounts into four ML/TF risks levels and (2) the simplified KYC/CDD requirements regime, available for specific banking services presenting low ML/TF risks.

In the US, Bank Secrecy Act regulations establish various thresholds for customer identification for different types of money services businesses, including prepaid card providers, money transmitters, check cashers, and money order issuers, which advances financial inclusion and access.

3.3.2. SDD measures to facilitate financial inclusion

Examples relevant to this section can be found in Annex A4.

149. SDD never means an exemption from CDD measures. A simplified set of CDD measures may be basic and minimal but must still respond to each of the four CDD components of R.10 that apply to normal customer relationships and transactions (identification/verification of customer, identification/verification of beneficial owner, understanding the purpose and nature of the relationship, ongoing monitoring of the relationship). In line with the RBA, it is the timing, intensity and the extent of customer information required, and the mechanisms used to meet these minimum standards that will vary depending on the risk level. Simplified measures can be applied to all four CDD components, and not only to the identification/verification of customer part.

150. R.10 requires that regulated entities identify their customers and use "reliable and independent source documents, data or information" (identification data) to verify identity. It is essential to distinguish between identifying the customer and verifying identification. Customer identification will enable the FI to know who the (future) customer is by collecting their information only (e.g. name, contact details, etc.). At this stage, no identification documentation or data is collected. In contrast, the verification of the customer identification requires checking reliable, independent source of documentation, data or information that confirms the veracity of the identifying information that was obtained during the identification process.

151. Except for R.16, the FATF Standards do not establish any specific requirements regarding the identifiers to be collected, nor how identity should be verified. Many countries and regulated entities take a conservative view of what constitutes appropriate identity elements or identifiers (e.g. date of birth, gender and address), but these identifiers are not necessarily evidence-based and may result from historical practices. Verification often relies on the use of official identity documentation (e.g. government-issued ID documentation such as passport). Unless

these are readily available to un/underserved persons who require financial services, these requirements may become access barriers.

152. In a lower risk context, fulfilling the customer identification, verification and monitoring requirements of R.10 could entail less intensive and formal means of information gathering and monitoring and a reliance on appropriate assumptions regarding the intended usage of basic products, or less detailed and frequent information. INR.10 para. 21 provides a number of examples of possible simplified measures with respect to the timing and verification of customer identity and intensity of transaction monitoring. These examples are proposed for guidance only and should not be considered as prescriptive or exhaustive.

Reduction of the extent of identification information required

153. Simplified identification measures can depart from standard due diligence requirements regarding the range of information that the customer has to provide, or the timing of verification. For example, under a SDD approach, the range of information collected from the customer may be reduced, focusing only on key identifiers deemed necessary to assess risk in lower-risk scenarios (such as name).

Alternative and new means of identification applicable to all customers

154. Identification and verification requirements may be set up by enforceable means and/or influenced by guidance defined by banking supervisors and regulators at national and international level.[129] In some countries, national authorities (Central banks, FIUs, supervisors) have taken initiatives to clarify and provide guidance on how to perform identification and verification of a customer's identity when the individual cannot provide "traditional" forms of identification. Such guidelines illustrate what constitutes a "reliable and independent" identification documentation and information in the country's context, in the absence of traditional identification documents. Some countries do not prescribe specific identity verification sources, or instead include a broad list of valid documentation and information for purposes of proving identity and/or alternative or new means of identity verification. They often include a non-exhaustive list of adequate documentation, and provide scenarios that would be considered as meeting the requirements of the law, including for example:

- a voter card
- tax card
- employment card
- non-photo ID
- expired ID
- a reference letter from a "suitable referee", i.e. a person who knows the customer, and can confirm the customer's identity.

155. In a number of countries, the existing legislation provides flexibility to apply different identity verification controls in a reliable and risk-based manner. This flexibility can be applied to target specific groups of vulnerable groups, or in cases of emergencies such as earthquakes. Refugees and asylum seekers are examples of

categories of undocumented customers who need to get access to basic financial services, both to fulfil their immediate payment needs and to sustain livelihoods.[130]

156. Countries and regulated entities should remain mindful that some alternative forms of identification may be more susceptible to fraud and take appropriate mitigation measures, including closer monitoring of the business relationship. In overcoming institutional barriers to implementing simplified measures, competent authorities should work with regulated entities to promote this flexible approach, through an education programme, ongoing outreach, and regular feedback and interactions on lessons learned. Authorities must distinguish between isolated breaches of otherwise sound controls due to inadequate application of the measures from the failure of risk assessment or the mitigating measures not being proportionate to risk.

Box 14. Fiji, Sweden, Türkiye and Private Sector (Malawi and United Kingdom)'s examples of alternative means for identification and verification of customer identity

This box provides an overview of the examples in Boxes 6.2, 6.3, 6.7, 6.9 and 6.11 (Annex A6).

In Fiji, where customers do not have government-issued ID documents, FIs are allowed to rely on a birth certificates accompanied with a confirmation letter from a suitable "referee".

The Swedish Bankers Association, in collaboration with the Swedish Migration Agency, designed a process to enable identification of asylum seekers for the purpose of opening a bank account, through the Swedish Migration Agency.

In Türkiye, following the earthquake in February 2023, authorities put in place a measure for alternative means of identification for customers whose residence were located in cities declared under a state of emergency, and who could not access their personal belongings. The Bank could proceed to customer identification by cross-checking at least four of the information listed in the regulation (including ID number, mother and father's name, date and place of birth, etc.)

In Malawi, a bank established a branch within the Dzaleka refugee camp specifically catering to refugees and asylum seekers with the approval of the regulatory body. The bank permits refugees to use factsheets or ID cards issued by UN High Commissioner for Refugees Malawi in lieu of the National IDs used by the host community. Refugees are not required to provide proof of residence and are instead required to provide a map to their residence within the different zones of the camp. As of December 2024, the bank has 14,800 active bank accounts held by refugees.

In the United Kingdom, a bank worked with NPOs to provide accounts to those fleeing domestic abuse situation and for adult survivors of modern slavery in England and Wales. Flexibility is provided in terms of acceptable identification and verification documents, which may include a letter from the supporting organisations.

130 See Alliance for Financial Inclusion (2017a).

Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship

157. The FATF Standards separate identification and verification (authentication) of the identification, therefore permitting identity verification to take place within a reasonable time after customer identification at the opening of a business relationship (subject to certain conditions). Such a mechanism can be leveraged in developing a tiered CDD approach (see above) that delays verification until a specified threshold is reached(e.g., total account value, transaction value, or transaction velocity), based on and proportionate to the identified risk. Examples of SDD measures in INR.10 include verifying the identity of the customer and the beneficial owner after the establishment of the business relationship.

Identifying and verifying the beneficial owner based on information from the customer's profile

158. When the provision of accounts to legal entities, such as small businesses, are assessed to be lower risk, the beneficial ownership requirements can also be adjusted. In most cases, the beneficial owner will be the individual customer themselves, or a closely related family member, which simplifies the identification and verification process. For such customers, simplified measures may involve collecting only minimal information about the customer's relationship with any closely related individuals and their source of income, rather than undertaking more in-depth investigations.

159. Simplified verification of beneficial ownership can also rely on the information already obtained through the customer's profile, such as official identity documents, transaction histories, or readily available public databases, provided these sources give a reasonable level of assurance. In low-risk cases, regulated entities may opt to infer beneficial ownership from the customer's declared information, without the need for extensive documentation or further verification unless red flags or discrepancies arise. Situations where suspicions arise that the account holder is used as a "straw-man", or "frontman" and is not the real owner, should not be treated as a lower risk and normal, or possibly enhanced, CDD measures should be applied.

Other examples of SDD measures

160. INR.10 mentions other examples such as:

- reducing the frequency of customer identification updates,
- not collecting specific information or, if so, not collecting supporting document, and/or
- inferring the purpose and intended nature of the business relationship from the type of transactions or business relationship established, rather than collecting specific information or carrying out specific measures for this purpose.

Box 15. World Bank's principles for developing RBA for Merchant Due Diligence

The World Bank Electronic Payment Acceptance document outlined principles for developing an RBA to Merchant Due Diligence and proposed a model for simplified Merchant Due Diligence. The model addresses simplified Merchant Due Diligence in four areas: (i) identification and verification of merchants; (ii) identification and verification of beneficial owners; (ii) identification of who retains power and authority; and (iv) collecting of contract particulars.

Ongoing monitoring of the transactions and relationship

161. Countries should also note that having a lower ML/TF risk for identification and verification purposes does not automatically lead to lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions (INR.10 para. 18). Likewise, conducting normal CDD in identifying/verifying a customer does not necessarily require normal CDD for the ongoing monitoring of the relationship. In most cases, the implementation of SDD measures is subject to specific thresholds or restrictions on the type or value of transactions that can be performed. Therefore, regulated entities should conduct ongoing monitoring to verify that the transactions remain within the risk-based thresholds and in line with the customer's risk profile.

162. To manage the ML/TF risks associated with the veracity of customer identification and verification data, regulated entities may choose to apply normal or enhanced monitoring of the transactions or relationships. This may involve a regular and frequent review of the transaction patterns (especially when transactions are inconsistent with the customer's profile) and a focus on potentially suspicious transactions. Customer identification and verification processes should provide regulated entities with sufficient information to engage in such monitoring.

3.3.3. Exemptions in Assessed Low Risk Scenarios

Specific examples relevant for this section can be found in Annex A2.

163. The FATF Standards allow countries not to require regulated entities to apply some of the FATF Recommendations provided that:

- there is an assessed low risk of ML/TF, which occurs in limited and justified circumstances and relates to a particular type of regulated entity or financial activity; or
- An individual or entity carries out a financial activity (other than MVTS) on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is a low risk of ML and TF.

164. The country is responsible for assessing the low risks and deciding what exemptions correspond with the risk. In considering exemptions, countries should evaluate factors such as the nature of products, services, transactions, and customer risk profiles, along with the legal framework and other pertinent characteristics of the activity. Countries should issue clear guidelines to outline the specific conditions under which exemptions can be applied, and the types of financial activities and/or regulated entities eligible for exemptions.

165. As a part of risk assessment, the impact of the exemptions on the overall risk level should be reviewed periodically. Any changes in the risk environment that may increase the ML/TF risk should prompt a re-evaluation of the exemption status. Similarly, ongoing monitoring may identify additional products, services and customers that may benefit from the low-risk exemption regime.

Box 16. Switzerland and the United Kingdom's frameworks enabling risk-based simplified measures and exemptions in assessed low-risk scenarios

This box provides an overview of the examples in Boxes 2.4 and 2.5 (Annex A2).

In Switzerland, the Anti-Money Laundering Act allows a financial intermediary to waive compliance with the duties of due diligence (Art. 3–7) if the business relationship only involves assets of low value and there is no suspicion of ML or TF.

In the United Kingdom, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 allows exemption from certain AML/CFT requirements under specified situations (e.g. engaging in financial activity on an occasional or very limited basis).

3.3.4. Tailoring measures to identified risks

166. There may be circumstances where the ML/TF risk is not lower and simplified measures are therefore not appropriate (e.g. customers in a conflict zone or high-risk jurisdictions), yet financial services still need to be provided in order not to further exclude vulnerable people (e.g. provision of financial channels to support humanitarian assistance in fragile or ungoverned regions). Regulated entities should be encouraged to manage and mitigate the risk through appropriate controls before considering declining or withdrawing services.

167. In this regard, countries should provide guidance to regulated entities on how to apply proportionate measures tailored to the identified risks (for example a combination of the different types of CDD measures identified in INR.10). Such tailored proportionate measures could consist of provision of limited purpose accounts with simplified identification requirements and ongoing controls, tailored monitoring of customer relationships, etc. For higher-risk customers and transactions, EDD involves deeper verification, closer examination of business activities, and intensified transaction monitoring. Effective EDD implementation addresses financial exclusion by enabling business relationships with higher-risk customers through proportionate measures. This approach ensures resources are focused on higher risks, allowing for lighter measures in lower risk scenarios.

168. Additionally, while SDD reduces compliance burdens for lower-risk accounts, ongoing monitoring is necessary to prevent exploitation and to adjust due diligence measures as needed. Countries may also provide specific guidance on sector-specific baselines tailored to the risk context of particular sectors (for example, see Box 1.3 in Annex A1 and Box 10 on The Netherlands's NPO baseline), or guidelines on handling transactions and relationships related to higher risk groups in a risk-based manner (see Box 17 below).

Box 17. The Netherlands – Risk-based industry baseline for transactions and relationships related to high risk third countries identified by the European Commission

This box provides an overview of the example in Boxes 5.9 (Annex A5).

The Dutch Association of Banks has published a Risk-based Industry Baseline on implementing AML/CFT requirements for low, neutral and high-risk scenarios with focus on the specific risks related to high risk third countries identified by the European Commission. The Baselines describes how to perform enhanced customer due diligence measures in a risk relevant manner to transactions, business relationships and correspondent relationships with European Commission high risk third countries as stipulated in the relevant regulations.

169. In summary, financial inclusion products must include appropriate measures to mitigate the identified risks. The degree of scrutiny in AML/CFT measures should be adjusted based on the risk level, with EDD, normal CDD and SDD measures complementing each other under the RBA. Financial products and services can be developed with adequate mitigation measures are embedded in their design, such as limitations on the product's functionality or availability (for example, monetary caps, or limitations in transfer function) or based on a progressive CDD approach (see Box 18 below). When SDD measures are applied at the on-boarding stage, the intensity of the monitoring process can be adjusted to mitigate the inherent risks of the financial products, and compensate for the relaxed initial due diligence checks.

Box 18. Singapore and Türkiye - Accounts subject to enhanced monitoring measures or limited functionality for individuals assessed as posing higher ML/TF risks

This box provides an overview of the examples in Boxes 5.8 and 5.10 (Annex A5).

Monetary Authority Singapore has been working with the key retail banks to enhance financial inclusion by opening Limited Purpose Banking Accounts for individuals whom the banks assess to pose a higher ML/TF risk or reputational risks, such as ex-offenders, in order to meet basic banking needs. To mitigate against abuse, the accounts are subjected to enhanced monitoring measures.

In Türkiye, banks conduct a number of verification activities to identify individuals and entities assessed as posing higher ML/TF risks. Banks seek to achieve financial inclusivity of these high-risk entities and individuals while not overlooking or underestimating the risks involved in their day-to-day transactions. For example, as a measure of appropriate risk mitigation, customers are not allowed to utilise on-line banking services if deemed risky by the parameters (i.e., potential suspicious activities related to illegal gambling, illegal foreign exchange market aimed transactions, etc.).

3.3.5. Digital Financial Inclusion

Specific examples relevant for this section can be found in Annex A6.

170. Digital financial inclusion refers broadly to the use of DFS to advance financial inclusion. It involves the deployment of digital means to reach un/underserved persons with a range of regulated financial services tailored to their needs, delivered responsibly at a cost affordable to customers and sustainable for providers. Some technologies (e.g. identity verification, biometrics and advanced analytics for transaction monitoring) can also enhance the efficiency and reliability of CDD measures, thereby making simplified measures more attainable.

171. DFS is delivered via digital/electronic technology such as e-money (initiated either online or on a mobile phone), payment cards and regular bank accounts.[131] The use and application of digital solutions requires that the necessary infrastructure is in place to enable customers in remote areas to be able to access physical cash.[132] It is not a form of virtual asset (e.g. cryptocurrency).

172. The FATF Guidance on Digital ID[133] emphasises the importance and outlines best practices for using secure and reliable digital identity systems to support customer identification and verification, particularly in the context of financial inclusion. These systems can enhance the integrity and efficiency of CDD measures by providing robust mechanisms to verify customer identities remotely, reducing reliance on traditional identity documents that may not be readily available to underserved populations. When properly implemented, digital identity systems offer a risk-based solution that can facilitate access to financial services for individuals who are otherwise excluded, while maintaining strong safeguards against ML/TF risks. Regulated entities are encouraged to adopt digital identity solutions that comply with the RBA outlined in the FATF guidance, ensuring that they are proportionate to the risk level associated with the product or service.

173. A growing number of countries are adopting innovative, technology-based means to verify customer identity. Some countries have set up country-wide national population registries that regulated entities can use to verify the identity of their customers. Some of these registries store biometric data, such as fingerprints and iris scans. A number of regulators around the world have sought to create enabling environments for DFS, including with regard to AML/CFT requirements. The general principle applies that AML/CFT regimes should be defined according to the nature and level of ML/TF risks and the products/channels used, and be adapted if and when relevant. In a number of countries, the expansion of DFS has supported the implementation of a tiered approach to CDD. Specific legal/regulatory frameworks to promote mobile money or branchless banking schemes involving the use of digital tools and technical support such as point-of-sale terminals for the use of payment cards have been designed. The scope of the applicable measures is limited and SDD applies only when the products or service are accessed in specific circumstances, for example face-to-face via a non-bank agent or through a mobile phone or an e-money issuer. In some countries, this approach is supported by measures to regulate the issuing and operation of cell phones (registration and identification requirements) and mobile money (SDD/CDD requirements).

131 See Global Partnership for Financial Inclusion (2016a)
132 See Hernandez and Martinez (2023).
133 See FATF (2020b).

174. One of the key challenges for these technology-led solutions is building the necessary infrastructure (e.g. adequate readers and sufficient internet connectivity) to allow for real-time or similarly reliable authentication of the captured biometric data with the central database.[134] This is crucial to ensure that the network of agents is technically equipped and capable to conduct identity verification, and to guarantee a satisfactory degree of certainty on whether the risk of identity fraud is adequately managed. The costs of using the real-time verification system can also be challenging for regulated entities. As in the case of traditional systems, stringent data protection and privacy measures must be implemented across the system to ensure the data integrity, prevent data leakages that can facilitate identity fraud, including by money launderers and terrorist financiers, and to protect individuals' privacy and combat abuse.

175. To ensure the success of DFS-focused initiatives, policymakers and other competent authorities must develop complementary legal and regulatory frameworks to support the sustainability of the digital products and meet un/underserved customers' needs.

Box 19. Digital Public Infrastructure

Digital Public Infrastructure (DPI) has emerged as an effective mechanism for delivery of financial services and advancing financial inclusion[135], which has been adapted by several countries in the world to reach un/underserved persons.

DPI is based on systems that are interoperable, open and inclusive in respect of technology and essential public/private services. Key components include building blocks such as digital ID, payment systems and data sharing platforms. DPI allows for reduction in transaction costs for both regulated entities and customers, lowering the overall cost of providing services thereby promoting greater participation from marginalised groups.

DPI has supported innovation across digital financial services - in payment, savings credit insurance and investment products. For example, digital IDs make customer onboarding quicker, and real-time payment systems allow for quicker and cost-efficient methods of money transfer. Regulatory framework adapted by countries should be supportive of DPI while maintaining robust AML/CFT controls. Countries should take measures to address potential risks such as data privacy, cybersecurity, and operational integrity.

176. Additionally, the development of branchless banking channels through non-bank agents (e.g. individual agents, retail shops, petrol stations, lottery kiosks), combined with DFS products (e.g. mobile phone solutions, e-money accounts) have helped reach the un/underserved groups and offer them basic, but regulated financial services. This can be particularly crucial in advancing digital financial inclusion in some countries with significant populations in rural and remote areas where

134 For more details on the Aadhaar experience in India, see Operational innovations in AML/CFT compliance processes and financial inclusion: emerging case studies (2014), slides 56-60.

135 See Alper et al. (2019).

traditional banking infrastructure is lacking. The deployment of digital solutions, such as mobile money and e-wallets, through these agent networks has significantly increased financial access and inclusion. Cash-In Cash-Out services provided by agents play important role for converting digital money to physical cash and vice versa, facilitating transactions in regions with limited banking facilities[136]. However, it is essential that regulatory frameworks are adapted to ensure that agent networks operate effectively and securely. National requirements should:

- establish the unequivocal responsibility of the FI for the sound and safe functioning of the system. This includes effective training and oversight of the network of agents to ensure that all of them are fully aware of their AML/CFT duties;
- make regulated entities accountable for actions of their agents, including in the AML/CFT field, through agent agreements and agent managers, and responsible for the consequences in case of fraud, misconduct or breach of AML/CFT obligations by the agents.

177. In addition, countries may also permit regulated entities to rely on CDD conducted by third parties that are not agents of the FI, under the conditions specified in R.17.[137] By leveraging technologies some countries have operationalised Central Registries which act as central repositories of CDD data. Such mechanisms enable streamlined access of verified CDD data to the regulated entities leading to reduction in duplication of efforts and reduced cost of operation. This mechanism may also allow for utilisation of same CDD data across different segments of the financial sector, thus making the onboarding process easier across different services. These registries can facilitate more efficient onboarding and ongoing monitoring of customers. Under such mechanisms the regulated entities may have to rely on the CDD information collected by third party.

Box 20. Argentina and India's examples of digital ID and biometric data registries

This box provides an overview of the examples in Boxes 6.14 and 6.15 (Annex A6).

In Argentina, the implementation of digital identity systems has allowed people to open accounts online and to get remote access to the financial system, thus boosting financial inclusion. As a result, the number of natural persons holding registered a net increase of 8.1 million (28%) between December 2019 and December 2023.

In India, a multi-pronged approach to promote financial inclusion and promote transactions through financial channels, called JAM Trinity, was developed based on three pillars: (1) access to financial services to the unbanked population, (2) biometric-based identification for every citizen, and (3) the development of a digital payment ecosystem. As per the Global Findex, access to financial services increased from 35% of total population in 2011 to 53% in 2014 to 80% in 2017.

136 See Hernandez and Martinez (2023).

137 See Operational innovations in AML/CFT compliance processes and financial inclusion: emerging case studies (2014).

Annex A. Examples of risk-based initiatives implemented by countries and the private sector to support financial inclusion

Annex A features examples of risk-based initiatives implemented by countries and the private sector which may, depending on the circumstances, help to support financial inclusion. In practice, the unique circumstances and context of each case will determine whether a particular measure is a good practice that support financial inclusion. Examples from the private sector have been de-identified.

The examples are provided under the following elements:

1. Countries' efforts in addressing de-risking issues
2. Frameworks enabling risk-based simplified measures and exemptions in assessed low-risk scenarios
3. Supervisor's guidance and engagement with supervised entities to support financial inclusion
4. Access to basic/limited financial products and services under specific circumstances
5. Risk-based customer due diligence
6. Simplified identification sources, documents and information requirements
7. World bank's financial inclusion product risk assessment module

Annex A1 Countries' efforts in addressing de-risking

Box .1.1. Australia – Statements and guidance on de-banking

Australia's AML and CTF laws requires FIs to develop tailored risk-based systems and controls that are proportionate to the level of ML/TF and serious crime risk they face in providing services to particular businesses. ML/TF risks associated with individual businesses in a given industry sector can vary significantly, even if the sector itself presents higher inherent risks. The appropriate implementation of an RBA does not require disengagement from risk or prevent FIs from establishing business relationships with higher-risk customers.

As highlighted in its statement on de-banking released in 2021[138] and guidance on de-banking released in June 2023,[139] the Australian Transaction Reports and Analysis Centre continues to discourage FIs from de-banking classes of customers, and instead encourages these institutions to assess and respond to customer risk on a case-by-case basis as ML/TF risks associated with individual customers in a given industry sector can vary significantly.

Australian Transaction Reports and Analysis Centre expects FIs to assess and understand risks presented by each customer, and this guidance outlines the Centre's regulatory expectations for FIs' engagement with customers they assess as being higher-risk. Although the decision to close an account may remain a necessary risk control, Australian Transaction Reports and Analysis Centre considers with appropriate systems and processes in place, FIs should be able to manage high risk customers, including those operating remittance services, digital currency exchanges, NPO and financial technology businesses.

For businesses in sectors identified as high-risk, the guidance encourages open communication with FIs about the nature of their work to demonstrate the steps they are taking to address risks within their business. For Australian Transaction Reports and Analysis Centre regulated businesses, this includes providing information on how they are managing the ML/TF risks within their business.

Australian Transaction Reports and Analysis Centre has also provided guidance for regulated entities to use a flexible and compassionate approach to customer identification processes,[140] to further encourage financial inclusion considerations in implementing an RBA.

138 https://www.austrac.gov.au/news-and-media/media-release/austrac-statement-2021-de-banking

139 https://www.austrac.gov.au/business/core-guidance/financial-services-customers-financial-institutions-assess-be-higher-risk

140 Australian Transaction Reports and Analysis Centre on Assisting customers who don't have standard forms of identification (2022) at https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/assisting-customers-who-dont-have-standard-forms-identification.

Box 1.2. Norway – Legal provisions against refusal to provide payment services without valid reason

The Norwegian Financial Contracts Act has provisions on financial inclusion, including that an entity cannot, without a valid reason, refuse to provide payment services on common terms.

Several cases where the consumer has been refused payment services citing the AML/CFT legal framework were brought before the Anti-Discrimination Tribunal and the Norwegian Financial Services Complaints Board. The cases have helped in raising awareness about malpractices, and addressing obstacles in financial inclusion.

Examples of cases before the Anti-Discrimination Tribunal include:

- Customers with disabilities that require assistance to log in to their bank accounts, were denied financial services as a general rule, and not based on an individual assessment of the risk.
- Customers who have a residence permit as their only identification got rejected.
- The tribunal concludes that this is contrary to the prohibition of discrimination on grounds of ethnicity, on the basis of the ML regulations and the guidance from the Norwegian Financial Supervisory Authority (stating that there must be made an individual assessment of each customer, and that the termination or refusal must rely on not being able to conduct appropriate CDD measures according to the AML act and regulations).

Cases before the Norwegian Financial Services Complaints Board include:

- Customers who have passports without radio-frequency identification, which were denied access to payment services as a general rule.
- The Board stated that the entity had internal routines stricter than the national requirements for identification, and this cannot be a valid reason for routinely refusing payment services on common terms.

Box 1.3. The Netherlands – Establishing risk-based industry baselines and sector baselines for sectors most impacted by de-risking (e.g. NPO baseline)

In 2022, The Dutch Central Bank published the report "From Recovery to Balance", [141] which underscored the importance of a correct application of the RBA for the effective execution of the gatekeeper role and reduce the undesirable side effects such as de-risking.

After the publication, the Dutch Central Bank set up a series of roundtables with representatives of the financial sector, the Dutch Ministry of Finance and the Dutch Banking Association. The results were twofold:

- Risk-Based Industry Baselines published in May 2023 for banks and customers, to provide banks with clear principles for risk-based CDD.
- Sector Baselines, with more detailed sector baselines for those sectors most impacted by de-risking, such as NPOs.[142]

The NPO baseline includes both risk enhancing and risk mitigating factors for NPO transactions. Banks are instructed to approach NPOs as neutral (as opposed to previously, when the entire NPO sector was seen as high-risk for TF) and then to apply a risk lens to do 'more if necessary, less if possible' in terms of CDD.

Initial feedback has been encouraging, with one large international bank reporting that, as of June 2024, the number of NPOs immediately designated as high-risk reduced from 34 000 to 14 000 following application of the NPO baseline and risk-based standard.

141 See https://www.dnb.nl/en/general-news/press-release-2022/fight-against-money-laundering-must-be-more-focused/?trk=organization_guest_main-feed-card_feed-article-content.

142 See https://www.nvb.nl/media/5836/nvb-sector-standard-not-for-profit-organisations-npo-_eng.pdf.

Box 1.4. United States – Department of Treasury's 2023 de-risking strategy

In April 2023, the Department of the Treasury published a De-risking Strategy, which examines the causes of de-risking for certain customer categories, including non-profit organizations (NPOs), foreign FIs with low correspondent banking transaction volumes, and money service businesses, which are often used by immigrant communities in the United States to send remittances abroad. As defined by the De-Risking Strategy,[143] de-risking is the practice of FIs acting indiscriminately "to terminate, fail to initiate, or restrict a business relationship with a customer, or a category of customers, rather than manage risk associated with that relationship consistent with risk-based supervisory or regulatory requirements."[144]

This strategy is the latest demonstration of Treasury's longstanding commitment to combatting de-risking and highlights the importance of FIs assessing and managing risk. The De-Risking Strategy focuses on de-risking in the context of correspondent banks, money services businesses (MSBs), and charities, not individual customers. The report found that profitability is the primary factor in FIs' de-risking decisions, which is influenced by a range of factors, such as a FI's available resources and the cost of implementing anti-money laundering and countering the financing of terrorism (AML/CFT) compliance measures and systems commensurate with the risk posed by customers. The strategy identifies other contributing factors, including reputational risk, FI risk appetite, a perceived lack of clarity regarding regulatory expectations, and regulatory burdens.

The strategy proposed a dozen concrete actions designed to reduce de-risking and its adverse consequences. Proposed actions include revising FI AML/CFT programs, reviewing bank inspection (referred to as examination in the US) practices, modernizing U.S. sanctions programs, and reducing burdensome requirements for processing humanitarian assistance. These actions would promote consistent regulatory expectations, provide better incentives to U.S. banks to avoid de-risking, and advance public and private engagement and cooperation at home and abroad.

Treasury's commitment to addressing the problem of de-risking through the implementation of the 2023 De-risking Strategy is additionally enshrined with measurable targets in the Department's 2024 National Strategy for Combatting Terrorist and Other Illicit Financing. The strategy provides a blueprint of the U.S. government's goals, objectives, and priorities to disrupt and prevent illicit financial activities.

143 AMLA The Department of the Treasury's De-Risking Strategy (April 2023), https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf.

144 Id. At pp. 2-3.

Box .1.5. Private Sector - Engagement with respondent banks to address challenges faced by a foreign correspondent bank in the Caribbean

A foreign correspondent bank engages with respondent banks and representatives from countries in the Caribbean that are underbanked. De-risking in these jurisdictions is driven by several overlapping factors:

- Most of the jurisdictions typically have less mature AML regimes and some have been "grey listed" by the FATF.
- The jurisdictions often do not meet the revenue thresholds required by foreign correspondent banks' risk acceptance criteria.
- Even when a foreign correspondent bank conducts an appropriate, individualised risk assessment of a particular correspondent relationship, there is a strong tendency for foreign correspondent banks to prefer not to be the sole clearer in a jurisdiction – especially in a country that is high-risk.

In one jurisdiction, to overcome this concern, the foreign correspondent bank undertook the following steps:

- Outside of country-based financial sanctions, it does not engage in wholesale exits from correspondent relationships in particular jurisdictions and instead seeks to work with each respondent bank to mitigate ML/TF risks, exiting only as a last resort.
- It encourages smaller and un/underbanked jurisdictions to seek out select respondent banks with whose programs it is comfortable and whose downstream nesting arrangements are monitored.
- It maintains close contact and ongoing communication on AML/CFT regulatory development with certain regulators of its Caribbean respondent bank customers.

Annex A2 - Examples of frameworks enabling risk-based simplified measures in lower risk scenarios and exemptions in assessed low risk scenarios

Box 2.1. Brazil – Exemptions from CDD to assist lower income population in debt renegotiation

The Central Bank of Brazil´s AML/CFT regulation was amended[145] in 2023 to assist the lower income population with debt renegotiation to allow exemptions under a federal government program called "*Desenrola Brasil*" aimed at renegotiating debts of individuals listed in default registries.

Under this programme, regulated institutions contracting credit operations with individuals listed in default registries are exempt from carrying out qualification and customer classification procedures, provided that, cumulatively:

1. The renegotiated operations are in default on the date of establishing the respective program.
2. The funds released in the operation are transferred directly to the creditor of the renegotiated debt, without any interference from the debtor.
3. The debts relate to defaults with non-financial legal entities or institutions authorised to operate by the Central Bank of Brazil, which are responsible for the debtor's registration in default registries.
4. The provisions of the main text do not apply to the contracting of other products and services by the beneficiary of the renegotiation.

145 The amendment was introduced by Central Bank of Brazil´s Circular 3,978/2020.

Box 2.2. Egypt – Legal framework for Financial Inclusion

The Central Bank of Egypt actively supports financial inclusion efforts by regulated entities across the country through regular workshops and training programmes covering the national financial inclusion strategy, the implementation of a risk-based AML/CFT approach, and leverage technology for secure customer identification/verification and other CDD measures at on-boarding.

In 2020, the Central Bank of Egypt, in cooperation with Egyptian Money Laundering Combating Unit, issued several regulations aimed to enhance financial inclusion while maintaining financial stability and protecting the rights of customers:

- SDD procedures for individuals and micro-enterprises, for accessing financial services.
- Allowing application of SDD, without obtaining approval of Central Bank of Egypt and with Egyptian Money Laundering Combating Unit to new customers when opening traditional bank accounts, whether current or saving, provided that banks neither provide new products nor such accounts imply use of new financial technology.
- Banks applying simplified customer identification and verification procedures may rely solely on the given information and documents in the simplified KYC application, without requesting additional documents (e.g. allowing the bank to infer the purpose and intended nature).
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship.
- Allowing the reliance on service providers on behalf of the banks for identifying and verifying customers, to have access to financial inclusion products and service (i.e. mobile wallets and prepaid cards) subject to certain conditions.
- Allowing low ML/TF risk craftsmen, free lancers, companies and micro-enterprises that do not have official documents to prove their commercial activities, to open an account using simplified measures.
- Allowing youth from 15 years old to open bank accounts without the need for their guardians' approval.
- Opening branches of small banks, especially in urban and rural areas, with the aim of availing banking services to citizens.
- Working on developing the financial infrastructure.[146]

In compliance with the regulation, almost all banks in Egypt developed several products for different segments, such as women, youth, persons with disabilities.

146 This is achieved through the establishment of the credit information company "I-Score", in addition to supporting the access of medium and small enterprises to the necessary financing, by strengthening the role of the Credit Risk Guarantee Company. Also, the Central Bank of Egypt issued regulations for the licensing and registering of Digital Banks, allowing entities to provide banking services and products through digital platforms and channels to enhance financial inclusion.

Box 2.3. Luxembourg –Tiered-approach to identity, customer and beneficial ownership verification requirements for low value transactions executed by payment service providers

Under Grand-ducal Regulation of 5 August 2015, the obligated entities may reduce the identification measures and not verify the identity of their customer and, where applicable, the beneficial owner of the business relationship , when providing online payment services fulfilling a set of cumulative conditions, including:

1. The transaction being executed via accounts held with payment service providers located in the European Union or in a third country which imposes equivalent requirements relating to the fight against money laundering and terrorist financing;
2. The transaction does not exceed a unit amount of EUR 250;
3. The total amount of the transactions executed for the customer during the 12 months preceding the transaction does not exceed EUR 2 500.

The simplified customer due diligence regime is excluded when:

- there is a suspicion of money laundering or terrorist financing,
- there are doubts about the veracity or adequacy of previously obtained data or
- in specific circumstances which carry a higher risk.

In case of a justified low risk, the obligated entities may exceptionally accept other types of ID documents that meet the criteria of reliable and independent sources. This includes for example a letter addressed to the customer by a governmental body or other reliable public body, where the customer cannot provide the usual identification documents and, insofar as there are no grounds for suspicion.

Box 2.4. Switzerland – Due diligence requirements' exemptions for long-term business relations

In Switzerland, to support the implementation of the RBA to combating ML/TF, the Anti-Money Laundering Act allows financial intermediaries to be exempted from complying with the due diligence obligations[147], under these conditions:

- long-term business relationships,
- the amounts involved are of low value,
- the legality of the business relationship is established.

Such a "de minimis clause" helps to ensure that newly emerging markets or financial products with a very low risk of money laundering and terrorist financing can be introduced and developed in Switzerland.

The Swiss Financial Market Supervisory Authority , may, at the request of financial intermediaries (art.3, Swiss Financial Market Supervisory Authority AML Ordinance) authorise further exemptions from compliance with due diligence obligations under the Anti-Money Laundering Act for long-term business relationships, provided it is demonstrated that the money laundering risk is low, within the meaning of art.7a Anti-Money Laundering Act.

147 Under articles 3 to 7.

Box 2.5. United Kingdom – Definition of engagement in financial activity on an occasional or very limited basis for exemptions

In the United Kingdom, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017[148] allows exemption from certain AML/CFT requirements under specified situations, including:

- a person whose main activity is that of a high value dealer engaging in financial activity on an occasional or very limited basis, or
- a person who engaging in financial activity on an occasional or very limited basis[149].

For the purpose of the said exemption, the regulation set the following conditions for an occasional or very limited basis financial activity:

- the person's total annual turnover in respect of the financial activity does not exceed £100 000;
- the financial activity is limited in relation to any customer to no more than one transaction exceeding EUR 1 000 euros, whether the transaction is carried out in a single operation, or a series of operations which appear to be linked;
- the financial activity does not exceed 5% of the person's total annual turnover;
- the financial activity is ancillary and directly related to the person's main activity;
- the financial activity is not the transmission or remittance of money (or any representation of monetary value) by any means;
- the person's main activity is not that of a person falling within regulation 8(2)(a) to (f) or (h) to (k);
- the financial activity is provided only to customers of the main activity of the person and is not offered to the public.

148 Including the ML/TF, amendment number 2, Regulations 2022.
149 Falling within regulation 8.

Annex A3 - Supervisor's guidance and engagement with supervised entities to support financial inclusion

Box 3.1. Cooperation with provincial governments, universities and agencies to promote financial education

The *Banco Central de la República Argentina* has developed financial education and training actions and signed agreements with nine provincial governments to implement them with the provincial education ministries and/or commercial banks. The Banco Central de la República Argentina has also signed agreements with national universities and agencies that seek to promote financial education in the country and the joint production of educational content and materials. The programs implemented are:

- "Financial Education in the Classroom": for secondary level teachers to develop financial education content in the classroom. This program reached more than 14 000 teachers and 92 648 high school students between 2020 and 2024.
- "Local Finance" targets the most vulnerable sectors in society, through the training of leaders from different provinces, including volunteers from provincial public banks and from different departments of the provincial governments to reach the final recipients. Between 2021 and 2024, the programme reached 2 940 references and 6 421 final beneficiaries (microentrepreneurs, technical school students, older adults, among others).

The *Banco Central de la República Argentina* invited financial entities, non-financial entities, banking and fintech association to voluntary join the formation of the Working Group for Financial Education Initiatives to implement financial education training in the different districts of the country. To date the following committees have been formed: "Contents in Financial Education" and "Analysis and Approach to Target Audiences".

Box 3.2. France – Joint working group to promote NPO's access to financial services

The French Ministry of Europe and Foreign Affairs found that the NPOs with which it works in the context of its humanitarian action reported recurring difficulties with their banks in carrying out certain operations. In particular, NPOs often need to send money to high-risk third countries as part of their activity. Sometimes, this need is accompanied by an emergency. Under AML/CFT/CPF regulations, banks implement EDD measures to mitigate these risks.

The Ministry of Europe and Foreign Affairs has therefore set up a working group, bringing together its teams, the main French NPOs, the French banking federation and some of the main banks, the banking supervisor and the competent authority for the implementation of restrictive measures (French Treasury). Increasing mutual understanding between customers that are NPOs and banks should therefore facilitate NPOs' access to financial services and the carrying out of the transactions they need to achieve their missions.

The discussions within the working group led to the publication of a guide (in French) dedicated to the access to financial services of NPOs, partners of the Ministry of Europe and Foreign Affairs, that carry out international solidarity activities. The aim of this guide is to:

- facilitate the understanding of banks' regulatory constraints by leading internationally active NPOs.
- enable banks to better understand the compliance requirements set by NPOs' financial backers or by themselves.

Box 3.3. India - National strategy and domestic cooperation to promote financial inclusion

India created a solid institutional framework to coordinate and support its Financial Inclusion strategy. The National Strategy for Financial Inclusion for India 2019-2024 provides an analysis of the status and constraints in financial inclusion in India, specific financial inclusion goals, strategy to reach the goals and the mechanism to measure progress. It is prepared by the Reserve Bank of India and reflects the outcomes from wide-ranging consultation with relevant stakeholders.

Created in 2010, the Financial Stability and Development Council, chaired by the Union Finance Minister and supported by a technical group, is responsible for financial stability, financial sector development, inter–regulatory coordination, and financial inclusion.

Other engagement activities include:

- The FIU-India and all the financial sector regulators hold meetings on a quarterly basis,
- The Lead Bank, a periodical forum for cooperation between state government, banks and Reserve Bank of India in charge of establishing and implementing a financial inclusion plan,
- Centre for Financial Literacy project, launched in 2017 by the Reserve Bank of India, is a NPO community-led innovative initiative to financial literacy, across the country.
- The Reserve Bank of India Financial Literacy Week 2016 to propagate financial education messages on various themes among members of public across the country.
- The Reserve Bank of India mass media campaign disseminate financial inclusion awareness key messages to the public.

Box 3.4. Lesotho – Institutional structures and Guidance to support financial inclusion

In Lesotho, FIs are required to apply RBA when establishing business relationships with customers[150]. It is expressly provided in the regulation that regulated entities may apply simplified measures where the risks are lower. Several initiatives support its effective implementation:

- The Central Bank of Lesotho has also developed Risk Management Guidelines for FIs on the RBA, covering key issues such as customers and sectors risk assessment and the risk-based customer due diligence (SDD where the risk is low, standard CDD where the risk is moderate and EDD when the risk is high).
- The Financial Inclusion Steering Committee is an institutional structure dedicated to promoting cooperation between different government agencies and the regulator to support financial inclusion. It has several thematic sub-committees working on implementation of the financial inclusion strategy of which AML/CFT issues are embedded into. The national Financial Inclusion Forum which consists of all financial sector players also convene quarterly on general financial inclusion matters of which AML/CFT forms part of.
- The regulator engages with the financial sector regularly through established structures (the banking association, insurance association, microfinance association, national payments council) and sub-committees. For instance, the fintech working group promotes awareness of AML/CFT and other compliance matters.

150 Regulation 5 of the Money Laundering and Proceeds of Crime Regulations, 2019.

Box 3.5. The Netherlands – Engagement and guidance to the industry to support an RBA to the AML Act

Over the last years, the Dutch Central Bank undertook a number of initiatives to engage with, provide guidance and encourage the industry to implement an RBA in application of the Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft), including:

- Publication of the report "From Recovery to Balance"[151] in 2022, recommending banks to improve their customer risk classification processes, apply more limited scrutiny to low-risk customers, and allocate greater capacity to higher-risk customers.
- Publication of the Dutch Central Bank AML/CFT guidance ("*DNB Wwft Q&As and Good Practices*") to implement risk-based AML/CFT requirements. It identifies low, neutral and high-risk scenarios on issues including: ultimate beneficial ownership identification and verification, PEPs and source of funds, determining origin of funds and assets for low-risk customers, policy on remote identification and verification, periodic and event-driven review, etc.[152]
- The organisation, jointly with the Ministry of Finance, of discussions with representatives of the financial sector in 2022 and 2023 focusing on enhancing the RBA in preventing ML/TF.
- The discussion of this issue in the multistakeholder National Forum on the Payment System, aiming to enhance the accessibility, reliability, and efficiency of payment transactions in the Netherlands.[153]
- The Dutch Banking Association has also published various Industry Baselines to support payment service providers in making accurate risk assessments, for example, for non-profit organisations and VASPs (referred to as Crypto-asset Service Providers in the Netherlands).[154]

151 See https://www.dnb.nl/en/general-news/press-release-2022/fight-against-money-laundering-must-be-more-focused/?trk=organization_guest_main-feed-card_feed-article-content.

152 See for more information the website of the Dutch Banking Association (NVB): Results of public consultation of DNB Wwft Q&As and Good Practices | De Nederlandsche Bank and DNB Wwft Q&As and Good Practices.

153 The NFPS brings together representatives from different ministries and public bodies, consumer organisations, businesses, and other stakeholders. The NFPS discusses various topics, including the accessibility of banking services, innovations in payment systems, payment security, and the impact of regulations. The recommendations made by the NFPS can lead to policy changes and measures that improve financial inclusion.

154 See the website of the NVB for examples of the Industry Baselines.

Box 3.6. United States – Joint statement and factsheet to encourage and provide clarity on RBA

The United States Federal Banking Agencies and Financial Crimes Enforcement Network have consistently **engaged with the financial sector by direct outreach to the banks** they supervise through:

- presentations at industry conferences,
- bilateral meetings,
- participation in financial inclusion-focused discussion roundtables and working groups,
- the issuance of guidance on the application of the RBA, and
- the issuance of joint statements.

For example, in 2022, the Federal Banking Agencies and Financial Crimes Enforcement Network participated in the issuance of the *Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence*[155]. The Statement reinforced a longstanding position that:

- no customer type presents a single level of uniform risk a particular risk profile related to ML, TF or other illicit financial activity,
- banks must adopt appropriate risk-based procedures for conducting ongoing CDD that enable them to understand the nature and purpose of customer relationships for developing a customer risk profile, conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information.
- banks are encouraged to manage customer relationships and mitigate risks based on customer relationships, rather than decline to provide banking services to entire categories of customers.

In 2020, the Federal Banking Agencies and Financial Crimes Enforcement Network also participated in the issuance of the *Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations*[156] :

- It provides clarity to banks on how to apply an RBA to charities and other NPOs, consistent with the CDD provisions of the Bank Secrecy Act.
- The Statement was issued in response to difficulty reported by some charities in obtaining and maintaining access to financial services, jeopardising the important contributions charities make to the most vulnerable.
- The Federal Banking Agencies reminded banks that charities vary in their risk profiles and should be treated according to such profiles.

The United States Treasury and the federal functional regulators encourage FIs to apply an RBA to Customer Identification Programme Rule requirements (e.g., customer identity verification, ongoing CDD) and have clarified the flexibility that the regulatory provisions allow. Examples include:

- Interagency Interpretive Guidance on Customer Identification Program Requirements.[157]

- Under the Customer Identification Program Rule, banks could accept a New York City Municipal ID containing name, photo, date of birth, address, and signature as "a primary source of identification in opening a new account for either U.S. or non-U.S. persons.

155 https://www.fincen.gov/sites/default/files/2022-07/Joint%20Statement%20on%20the%20Risk%20Based%20Approach%20to%20Assessing%20Customer%20Relationships%20and%20Conducting%20CDD%20FINAL.pdf.

156 https://www.fincen.gov/news/news-releases/fincen-and-federal-banking-agencies-clarify-bsa-due-diligence-expectation.

157 under Section 326 of the USA PATRIOT Act, 2005 FAQs, Staff of the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), Final CIP Rule, April 28, 2005.

Annex A4 - Examples of access to basic/limited financial products and services under specific circumstances

Box 4.1. Chile – Account associated to the tax-identification number allocated to all nationals and residents

CuentaRUT (RUT Account) is a demand deposit account that targets low-income individuals who do not have access to traditional financial products due to their low resources and/or informal working conditions. The RUT Account is linked to a tax-identification number allocated by law to each Chilean national and foreign resident. The account allows deposits, transfers or withdrawals and can be linked to a debit card (*RedCompra*) to make payments in different stores, with no monthly maintenance fee. To mitigate risks, the account has certain transaction conditions and limits related to maximum amounts (e.g. max. balance amount USD 4 576; daily transfers limitations, depending on transfer channels).

Box 4.2. El Salvador – Legal requirement to support financial inclusion: verify supervised entities RBA and simplified opening of savings accounts

El Salvador has adopted several measures to support financial inclusion:

1. El Salvador has implemented an RBA to AML/CFT[158]:
   - Regulated entities must identify, evaluate and understand their ML/TF/PF risks, adopt proportionate mitigating measures and apply relevant resources to them.
   - The supervisory authorities may (i) verify the effectiveness of the supervised entities' prevention and detection programmes[159] and may (ii)review the ML/TF/PF risk profiles and the risk assessments prepared by the regulated entities to evaluate whether simplified measures or exemptions (in case of a proven low risk) have been applied in compliance with the law.
2. El Salvador has also incorporated in its legal framework a simplified regime for opening of "simplified savings accounts" that allows for customer onboarding through various channels[160]:
   - They can be opened through (i) electronic channels or media, (ii) financial correspondents, or (iii) banking agents, and the agents of savings and credit societies.
   - The following information must be collected when opening the account: name of the holder, unique identity document number, residence address,

158 FIU Instructions for the Prevention, Detection and Control of ML/TF/PF.
159 Article 4, Regulation of the Law against Money and Asset Laundering.
160 Law to Facilitate Financial Inclusion.

economic activity, origin of monthly income, name and residence address of the beneficiaries.

- The accounts are subject to several restrictions: (i) The holder can only be a natural person, (ii) there may not be more than one holder per account, (iii) each holder can only hold one account in each financial service provider; and (iv Balance and transactional limits are determined every two year by the Central Reserve Bank based on economic factors.
- A notable outcome of this measure is that in June 2024, the total number of savings accounts reached 138 924 held by women and 159 294 held by men in El Salvador.

Box 4.3. European Union – Limited products and services for asylum seekers from high-risk third countries or territories

(See also Box 6.2 on the use of asylum seeker's official documentation as an identification method for bank account opening).

In the European Union, the European Banking Authority issued an Opinion in April 2016 which clarifies how CDD measures can be adapted to facilitate financial inclusion of asylum seekers from higher risk countries or territories, while maintaining robust AML/CFT controls.

The Opinion takes the view that the ML/TF risks associated with asylum seekers from third (non-European Union) countries are unlikely to be lower, due to a combination of factors, including the robustness or trustworthiness of the applicants' identity documentation and the higher risk third (non-European Union) countries or territories of origin. As a result, a SDD regime has not been set out at European Union level. However, the European Banking Authority has clarified how CDD measures can be adapted to facilitate financial inclusion, while maintaining proportionate and solid AML/CFT controls.

The European Banking Authority mentions examples of limits FIs might impose on a risk-sensitive basis:

- no provision of credit or overdraft facilities,
- monthly turnover limits (unless the rationale for larger or unlimited turnover can be explained and justified),
- limits on the amount of person-to-person transfers (additional or larger transfers are possible on a case-by-case basis),
- limits on the amount of transactions to and from third (non-European Union) countries (while considering the cumulative effect of frequent smaller value transactions within a set period of time), in particular where these third (non- European Union) countries involved are associated with higher ML/TF risk,
- limits on the size of deposits and transfers from unidentified third parties, in particular where this is unexpected, and

- prohibiting cash withdrawals from third (non-European Union) countries.

Box 4.4. France – The Banque de France to nominate a credit institution to open an account with basic banking services and caps for eligible individuals denied of banking service

France has put in place a regulatory framework and a guidance to support financial inclusion through the right to a bank account. This measure ensures that:

1. any natural or legal person domiciled in France,
2. any natural person of French nationality residing outside France, and
3. any natural person of foreign nationality legally resident in the territory of another European Union Member State and not acting for business purposes,

can benefit from the opening of a bank account. In case of refusal, the Banque de France designates a credit institution, that is under the obligation to open an account for this person featuring basic banking services and caps.

The AML/CFT obligations apply to these business relationships in the same way as to other business relationships. Furthermore, the limitation of the services offered is a factor in reducing the potential ML/TF risk. A guidance helps credit institutions understand the specific risks associated with these business relationships.

Box 4.5. Hong Kong, China – Simple Bank Accounts with narrower service scope and lower transaction volume

In April 2019, the Hong Kong Monetary Authority announced the introduction of Simple Bank Accounts by banks as a measure to promote financial inclusion and to provide corporate customers with more choices.

Simple Bank Accounts are a tier of accounts derived from traditional bank accounts, focusing on provision of basic banking services such as deposits, withdrawals, local and cross-border remittances, etc.

Compared to traditional bank accounts, Simple Bank Accounts have a narrower service scope and lower transaction volume, so the risks involved in Simple Bank Accounts would be relatively lower and hence less extensive CDD measures are required. For instance, banks may require less detailed information and supporting documents from applicants.

Individual banks have the flexibility to design their own Simple Bank Accounts based on their business strategies and risk assessments, so the scope of services of Simple Bank Accounts offered and the extent of CDD measures may vary across different banks. Simple Bank Accounts customers who require more comprehensive banking services in the future may upgrade their accounts to traditional bank accounts by completing the standard CDD process.

As of 2023, there were eight banks offering Simple Bank Accounts services, and the cumulative total number of such accounts has increased to over 21 000.

Box 4.6. Indonesia – Regulation for mandatory provision of basic saving account at no charge in specified circumstances

In 2022, the Indonesian Financial Services Authority issued regulations[161] requiring FIs to provide a basic savings account, at no charge, under certain specified circumstances. Under this regulation, a basic saving account is systematically classified as a low-risk product and, as such, is subject to the application of simplified measures. It is further exempt from charges for monthly administration, account opening, cash deposit transactions, incoming transfer transactions, transfer transactions, and account closing. Its characteristics include:

1. any Indonesian citizens,
2. Indonesian rupiah (IDR) currency only,
3. maximum account balance of IDR 20 million (about USD 1 224), and
4. maximum cumulative limit for account debit transactions (cash withdrawals, overbooking, and/or outgoing transfers) within one month cumulatively on each account of IDR 5 million (about USD 500).

Box 4.7. Jordan - Basic bank accounts for all legally qualified citizens

In line with the National Financial Inclusion Strategy (2018-2020), the Central Bank of Jordan issued in 2019 the basic bank account instructions requiring all banks operating in the Kingdom to open a basic bank account for all legally qualified and financially excluded citizens. The basic bank account is a low-cost account available to individuals that do not have a bank account and are willing to deal with banks within limits and costs that suit their income and abilities. These instructions provide that:

1. the opening of a basic bank account is subject to SDD procedures,
2. the only required document for opening a basic bank account is a national ID (no need to provide proof of residence or work),
3. there is no minimum balance,
4. the customer is exempted from certain types of commissions and fees, and
5. the customer has access to basic banking services such as withdrawals, deposits, wire transfers and electronic banking services.

The Central Bank of Jordan has also issued specific SDD procedures for different sectors which are applied only when the assessed ML/TF risk is low.

161 POJK No. 1/POJK.03/2022 and POJK No. 8 of 2023.

Box 4.8. Türkiye – Special products with limitations for international students from countries assessed as posing a higher ML/TF risk

Special products such as prepaid cards that can be used within certain limits and carries out activities such as internet banking and remote customer acquisition for financially underserved groups. International students from countries assessed as posing a higher ML/TF risk who are enrolled in full-time universities in Türkiye can also open deposit accounts if they are to receive grants and scholarships from official agencies. These groups can have limited transaction amounts so that the account has restricted functionality in terms of any AML/CFT abuse.

Box 4.9. Private sector, Indonesia – Simple saving product with minimal transaction fees

A bank's majority owned subsidiary in Indonesia offers a product of financial inclusion called "Tabungan Danaku," a simple saving product that can be reached directly by the customer segments that would not normally be able to be banked through traditional products. This is a local-agent-based banking product supported by SMS banking and with a limit on the maximum balance being IDR20 million (USD 1330). In 2023 onwards, this was shifted to be focused on digital banking, using a mobile app. The main benefits of the product are that there is no minimum deposit to open an account, no minimum balance and minimal transaction fees. Customers do not need to come to a bank branch to use the product, and every transaction can be done through the local agent, or through text.

Box 4.10. Private Sector, Mexico – Basic current account without showing ID documentation

See also Box 5.5 "Mexico - Low risk bank accounts to serve the underserved groups"

In Mexico, an international bank provides a digital channel for opening "Level 2" accounts, under the Government's tiered due diligence program. This initiative permits customers with access to a basic current account without showing ID documentation – instead, identification is checked against a government database. In parallel, identity fraud controls implemented as part of the bank's on-going monitoring programme aim to reduce the risk associated with onboarding without an identification document. In line with the "Level 2" requirements, the account also has limited functionality (e.g. caps on the overall balance month-to-month, no cross-border activity, etc.).

When this initiative was reviewed during examination by the international bank's home country regulator, where ID documentation is required for account opening, the international bank was able to demonstrate that an exception to the bank's group-wide policy was acceptable given the importance of the Mexican Government's tiered due diligence program to reducing overall ML/TF risk in the country. The home country supervisor assessed that the exception to policy was sufficiently documented and subject to appropriate governance, and did not raise any objections to the bank's support for the initiative.

Annex A5 - Examples of risk-based tiered customer due diligence

Box 5.1. Argentina – Requirement to comply with the minimum SDD in the cases of low-risk customers with no suspicion of ML/TF

In February 2023, Argentina published Resolution 14/2023[162] to introduce amendments to its legislative framework for AML/CFT to, amend other objectives, establish that in situation where customers are identified as exposed to low risk and if there is no suspicion of ML/TF, a FI can/must comply with the minimum SDD when identifying and verifying the identity of its customers.[163] In particular, for low-risk customers who are covered by the measures provided within the framework of public policies that aim to promote and/or expand financial inclusion, the FI are obliged to require the pertinent information and documentation and evaluate whether it is appropriate to adjust the profile, only when the monthly accreditations exceed the equivalent of four minimum wages (minimum wages in April 2024 was equivalent to USD250).

Information provided by employers and the competent national, provincial or municipal organisations are considered sufficient for identification of the customers whose legitimate monthly income does not exceed 24 minimum wages and correspond to the accreditation of remunerations, or to the unemployment fund for workers in the construction industry; or whose monthly income does not exceed 3 minimum wages in accounts linked to the payment of social plans. The SDD does not apply when there is suspicion of ML/FT.

162 Through resolution 14/2023 , the Financial Information Unit (UIF) adopted measures regarding SDD that FIs apply to low-risk clients at https://servicios.infoleg.gob.ar/infolegInternet/anexos/375000-379999/379085/texact.htm.

163 Art. 21-25, 28.

Box 5.2. China – Bank account management based on risks

In China, bank accounts for individuals have been classified into 3 categories since 2015[164], to help banks mitigate their AML/CFT risks.

- Type 1 account has full functions including cash deposit and withdrawal, transfer, purchasing financial products, making payments for goods and services, etc.
- Type 2 account can be used to purchase financial products, but limits transfers or payments to below certain thresholds.
- Type 3 account is limited to payments, subject to a specific volume cap.

Both Type 2 and Type 3 accounts cannot be used to make cash deposits and withdrawals, and do not have physical cards associated to these accounts. They can be opened through remote video teller machines, smart teller machines, online or through smart-phones. However, when these remote onboarding opening channels are used, banks are required to apply additional CDD measures with the aim of effectively mitigating risks: customer's identity has to be verified by bank staff on site.

Box 5.3. Ghana – CDD tiered approach for mobile money services

In Ghana, the Central Bank published guidelines in 2015 to regulate the issuing and operations of electronic money. Non-bank e-money issuers have been allowed to enter the market. Customer accounts opened are categorised in three levels, with different CDD requirements for each, as part of an RBA. Level 1 is a minimum CDD account with very low transaction and balance limits and documentation requirements.

Box 5.4. India – Flexibility in CDD to ensure financial inclusion

India's Prevention of ML Rules (2005) provides CDD obligations for FIs and aim to ensure financial inclusion while addressing ML/TF risks through an RBA. The Prevention of ML Rules requires (Rule 14(1)):

1. The regulators to issue guidelines incorporating the CDD requirements outlined in the Prevention of ML Rules, including enhanced and simplified measures, based on the type of customer, nature of business relationships, transaction values, and identified risks.
2. Every reporting institution to formulate and implement a CDD Program:
    - Simplified measures are permissible for low-risk scenarios, provided they align with India's National Risk Assessment.
    - are not allowed when there is suspicion of money laundering or terrorist financing, in higher-risk situations, or when risk identified is

164 2015 Chinese Central Bank Circular.

not consistent with the national risk assessment.

- Alternate identification methods are permitted for customers unable to undergo biometric or Aadhaar authentication due to age, injury, or other limitations.
- Clients lacking a Permanent Account Number may continue account operations under specified conditions.

Box 5.5. Mexico – Low risk bank accounts to serve the underserved groups

In 2011, the Ministry of Finance amended the AML/CFT framework to include a simplified KYC and CDD requirements regime, for specific banking services, presenting low ML/TF risks. In application of the amended legislation, bank accounts are classified according to four ML/TF risk levels.

For example, level 1 are low ML/TF risk account that may allow non-face-to-face opening process, but subject to monitoring from financial entities and to enhanced supervision of the financial authorities. Its main characteristics are as follow:

Amount/threshold limitation

- Limited to a maximum deposit amount of 750 UDIS165 per month (around USD 250) per month. Low-value transactions; Limited to a non-cumulative maximum balance of 1 000 UDIS (around USD 350).
- Customer identification and ID verification can be exempted – Banks can decide whether or not to apply the procedure, according to their policies, measures and internal processes.

Restricted use for payment of services and/or products

- Maximum amount per transaction established by FIs.
- Only one account per person.
- Cannot be linked to a mobile phone account (for funds transfers).
- Valid only in Mexico.
- Contracted at banking branches, banking agents, by phone or at the banking institution website.
- No transfer funds to other accounts or products.
- Able to receive international funds transfers, but not from high-risk and non-cooperative jurisdictions and countries sanctioned by the UN.

Strategic monitoring

- If suspicious acts are detected (e.g., when there are several transactions in a short period of time, with the same ATM) FIs must send a report to the Financial Intelligence Unit. Also, FIs will be able to cancel accounts or block transactions resulting from suspicious acts.

165 The Mexican Investment Unit is a unit of value calculated by the Central Bank of Mexico, which is adjusted on a daily basis to maintain purchasing power of money taking into consideration the changes on the inflationary indicator INPC (Mexican Consumer Price Index). Therefore, any financial and commercial transaction referenced to Mexican Investment Unit is updated automatically.

- Electronic transaction records are retained and made accessible to Law Enforcement Agency upon request.

Box 5.6. Pakistan - Basic/entry level branchless banking accounts

In 2011, the State Bank of Pakistan revised the branchless banking regulations introduced in 2008 and applicable to all FIs (commercial, Islamic and microfinance banks). With a view to expanding the outreach of branchless banking operations in the country, State Bank of Pakistan introduced level "0" branchless bank accounts to bring the low-income earning segment of society into the formal financial sector. The Branchless Banking Regulation of the State Bank of Pakistan was revised in 2019.[166]

Branchless banking agents are allowed to send the digital account opening form, the customers' digital photo and an image of the customer's Computerised National Identity Card to the FI-electronically, instead of sending the physical account opening forms and copies of customers' Computerised National Identity Cards to the FI for further processing.

The category of level "0" branchless banking accounts aims at providing provide flexibility to agents and FIs for opening basic branchless banking accounts, while rationalising the KYC requirements in line with the account transaction limits. Account opening requirements include:

- FIVerification of customer identity from the National Database & Registration Authority
- Pre-screening the name and Computerised National Identity Cards against proscribed/designated persons and entities as per the Statutory Notifications issued by Federal Government from time to time.
- Call Back Confirmation or generation of One-Time Password for verification in remote account opening.

Process Flow:

- Authorised Financial Institutions shall develop Account opening process flow and any additional requirement as per their internal risk assessment.
- Authorised Financial Institutions shall invariably conduct Biometric Verification of customers of other AFIs for fund transfers from their agent network.
- Level-0 account holders cannot perform Account-to-Person transfers, Cash in, and cash out till their Biometric Verification.
- Level-0 can be upgraded to Level-1 account after biometric verification of customer from the National Database & Registration Authority upon customer's request.

Thresholds:

- PKR 25 000 per day (USD 89)
- PKR 50 000 per month (USD 177)

166 See Branchless Banking Regulations for Financial Institutions at https://www.sbp.org.pk/bprd/2019/C10.htm.

- PKR 200 000 per year (USD 710)

Box 5.7. Peru – SDD measures based on a specific authorisation of the supervisor

Since 2015, FIs can apply SDD measures, based on an authorisation granted by the financial supervisor of Peru (Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones) for a specific product or service. When the financial supervisor's authorisation is granted, FIs only have to collect the full name, type and number of identity document of the customer, and the verification is done though the national identity or international ID (for foreigners). Under the standard regime, customers would also be requested to provide information on their nationality and residence, phone number and/or e-mail address, occupation and name of employer.

Box 5.8. Singapore – Limited Purpose Bank Accounts subject to enhanced monitoring measures for individuals assessed as posing higher ML/TF risks

Monetary Authority Singapore has been working with the key retail banks to enhance financial inclusion by opening Limited Purpose Banking Accounts for individuals whom the banks assess to pose a higher ML/TF risk or reputational risks, including ex-offenders involved in serious financial crimes (e.g., cheating, corruption, ML offences, etc).

The functionalities and safeguards for Limited Purpose Banking Accounts are designed to enable individuals to meet their basic banking needs, such as receiving salaries and paying bills, receiving government disbursements and insurance payouts. To mitigate against abuse, the accounts are subjected to enhanced monitoring measures. For example, banks will check that individuals are only receiving funds from specified sources which had been agreed upon at account-opening, including for the above-mentioned purposes/sources.

The banks are expected to conduct and document appropriate risk assessments and be able to substantiate why the Limited Purpose Banking Accounts are unable to address residual risks posed by individuals for whom the bank has assessed Limited Purpose Banking Accounts to be unsuitable. In situations where the account is closed or the individual is rejected from opening an account with the bank, the banks would also have to communicate clearly with the accountholder/individual and, as far as possible, explain the reason for account closure/rejection. In their communication with the accountholder/individual, the banks should also provide a clear process for appeal against the initial decision and set out the relevant contact details clearly.

Box 5.9. The Netherlands – Risk-based industry baseline for transactions and relationships related to high risk third countries identified by the European Commission

The Dutch Association of Banks Risk-based Industry Baseline outlines the framework for applying AML and CFT requirements, specifically focused on transactions, business relationships, and correspondent relationships with high-risk third countries identified by the European Commission. The baseline emphasises the importance of adopting an RBA to EDD measures as prescribed under the "General Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act" (Wwft), with reference to the 4th Anti-Money Laundering Directive (4AMLD) and the European Banking Authority Risk Factor Guidelines.

The baseline clearly defines low, neutral, and high-risk scenarios and specifies how FIs should approach each scenario. In general, for low and neutral risk scenarios, information that is already available from the CDD processes will generally satisfy the requirement to collect 'additional' information. Banks will assess the available information to determine that it satisfies the purpose and intent of the individual EDD measures in a proportionate manner. In high-risk scenarios, additional information should be obtained via desk research or customer outreach.

The baseline also includes specific use cases to illustrate a practical application of the baseline, covering both examples of scenarios considered as low, neutral or high risks, as well as practical measures implemented under each scenario.

Box 5.10. Türkiye – Enhanced measures for individuals and entities assessed as posing higher ML/TF risks

In Türkiye, Banks conduct a number of verification to identify individuals and entities assessed as posing higher ML/TF risks, including:

- For a foreign entities, the country-risk is the first element to be considered by the FI. "High-risk countries" are identified by the Ministry based on the weak legal and regulatory framework to combat money laundering and financing of terrorism, which are not cooperative on combating these offences or are considered high-risk countries by competent international organisations.
- KYC-based documentation and information shall be verified through notarised Turkish translations of copies of such documents.
- For foreign nationals, banks conduct name screenings by using the global database platforms such as, but not limited to Dow Jones, Google open search and so on.
- In terms of industries and legal persons, the banks in Türkiye utilise software that identify unusual transaction and raise red flags according to the parameters decided by the compliance department.
- High-risk deemed markets and industries that deal with precious metals, cryptocurrency service providers, money services businesses and similar

others are evaluated within what would be expected to be normal of them in the current overall economic environment.

- By doing so banks achieve financial inclusivity of these high-risk entities and individuals while not overlooking or underestimating the risks involved in their day-to-day transactions. In addition, as a measure of appropriate risk mitigation, customers are not allowed to utilise online banking services if deemed risky by the parameters (i.e., potential suspicious activities related to illegal gambling, illegal foreign exchange market aimed transactions, etc.).

Box 5.11. United States – Different thresholds for customer identification for different types of money services businesses

Bank Secrecy Act regulations establish different thresholds for customer identification for different types of money services businesses, including prepaid card providers, money transmitters, check cashers, and money order issuers, which advances financial inclusion and access.

For example, money transmitters are not required to retain records of the transmitter's identity information for a transmittal below a USD3000 threshold and for transmittals above that threshold are only required to collect the transmitter's name and address (and account number, if payment ordered from an account). The recordkeeping threshold for check cashers is also USD3000. The customer identification threshold for open-loop prepaid access cards that do not enable international or person-to-person transfers or non-depository reloading is for each customer USD1000 per device per day.

Box 5.12. Private Sector, Brazil – Customer behavioural activities as the driver to calibrating customer AML/CFT risks

A Brazilian bank has conducted a pilot of a customer risk-rating methodology that places significant weight, after on-boarding, on the "behavioural activity" of the customer as the most significant driver of risk.

"Behavioural activity" includes a range of factors but is primarily focused on cash and cross-border activity. When those two factors play a larger role in the customer risk profile, there is a general trend of customer risk shifting from "high/medium" risk ratings to "medium/low" risk ratings, which in turn reduces the frequency of customer identification updates. This is then paired with increasingly robust triggers, which over time should permit the bank to move to a trigger-based only refresh process for lower risk customer segments.

Box 5.13. Private Sector, Indonesia – SDD for onboarding followed by normal CDD

In Indonesia, a bank offers Basic Saving Account products available for certain customer segments and can be opened and operated by Branchless Banking Agents through the Agent Banking System. A Branchless Banking Agent can provide services for opening Basic Saving Accounts and carrying out domestic transfer transactions and cash withdrawals. The characteristics of this Basic Saving Account product are that there are limitations on savings and transactions carried out by customers annually. When a prospective customer is onboarded, Branchless Banking Agent will carry out SDD by requesting a minimum of five data of prospective customer to be verified on the government database. However, customers are still required to visit the nearest branch to collect their debit card, and at the same time, the branch is required to complete customer data and/or information referring to normal CDD procedures.

Box 5.14. Private Sector, Nigeria – Tailored tiered KYC system to promote financial inclusion of women

In 2011, In Nigeria, barriers such as physical distance to bank branches, lack of trust, financial literacy, affordability, and stringent eligibility criteria has hindered women's access to financial services in the country. The Central Bank of Nigeria established a tiered KYC requirement, which made it possible to open a simple savings account without ID. Based on the tiered requirements, a bank introduced a tailored tiered KYC system, allowing for varying levels of account access based on the documentation provided. This approach enabled customers to open basic accounts with minimal identification and gradually providing more information as their relationship with the bank grew. The key components of the tailored tiered KYC implementation included:

- **Minimal documentation for initial account opening**: Customers could open accounts with basic identification documents, such as name, number and address.
- **Provision of information over time**: As customers used their accounts and built a relationship with the bank, they were required to provide additional information and documentation.
- **Use of mobile technology**: Customers could access services through their mobile phones, making it convenient for them to manage their accounts and complete KYC requirements.
- **Bank agents**: Bank agents played a crucial role in educating customers about the importance of KYC compliance and assisting them in providing the necessary documentation.

The implementation of tiered KYC was successful in increasing the number of accounts opened and improving customer engagement. The impact is evident: over 620,000 accounts have been opened and 72% of women customers are still using their accounts, further increasing their financial inclusion.[167]

167 See Women's World Banking (2016) "New Tools Increase Women's Financial Inclusion in Nigeria" at https://www.womensworldbanking.org/insights/cfr-new-tools-increase-womens-financial-inclusion-nigeria/

Box 5.15. Private Sector, Senegal – Tiered Know Your Customer (KYC) approach

Tiered KYC approach implemented by wallet providers in Senegal has contributed to the deepening of financial inclusion in the country by increasing formal individual account ownership from 42% in 2017 to 56% in 2021.[168]

For example, a provider has taken a customer-centric RBA to CDD as follow:

- Once the user registers on the mobile app (for smartphone users) or gets a designated QR code card (physical card for non-smartphone users) from an agent they can immediately make domestic transactions up to 200 000 XOF/month (about USD 336).
- The provider refers to this entry account provided for in the instruction by The Central Bank of West African States[169], as the KYC 1 limit (KYC1).
- KYC 1 documentation only requires the entry of the customer's legal name and their phone number (the least barrier to entry into the formal financial system).
- Users can increase their wallet limit to XOF 2 000 000 (about USD 3 386) and graduate to KYC 2 by presenting their government issued ID to an agent who then uploads it on to the company system using their agent app.
- Accepted IDs can range from the foundational ID issued by the *Agence Nationale de la Statistique et de la Démographie* or specific government issued IDs like passport, resident card or consular card. These are then approved based on a combination of Optical Character Recognition software and human verification of the customer ID against the individual presenting the ID to an agent.
- Every customer begins at a lower tier KYC1 and then most of them very quickly graduate to a fully identified KYC2 level. At the end of September 2024, 44.8% of registered wallets were at KYC1, while 55.1% were at KYC2.

This tiered approach has allowed the provider to include customers who have never had a formal bank or financial services account. Customers get the opportunity to 'test' the product and how it operates, 'trust' the system, evaluate its affordability and relevance in the context of their daily lives and then graduate to a higher tier wallet where they can conduct even more transactions monthly.

At the end of June 2024, 68% of active customers that were classified as KYC2 were conducting transactions monthly. In contrast, only 32% of KYC1 customers were active on a 30-day basis.

The provider's user surveys reveal that one of the biggest customer constraints for not graduating to KYC2 is the lack of an ID (52% of active customers at KYC 1 level did not have a government issued ID). While providers are encouraging customers to submit official IDs to increase their limits, KYC 1 provides thousands of financially excluded individuals an entry level opportunity to participate in the formal financial system.

168 See Financial Inclusion in Senegal of FinDev Gateway at https://www.findevgateway.org/country/financial-inclusion-in-senegal

169 Number 008_05_2015, Article 31.

Annex A6 - Measures for simplifying identification sources, documents and information requirements

Alternative identity verification sources

Box 6.1. Australia – Referee statements, government correspondence and community ID as alternative identification

To support financial inclusion, in December 2022 the Australian Transaction Reports and Analysis Centre released updated guidance[170] to help banks and other regulated businesses implement flexible procedures to identify vulnerable customers while appropriately managing associated ML/TF risks.[189] This guidance is the result of a close consultation with industry associations, FIs and advocates for financially excluded groups.

It provides innovative approaches to identify customers from a range of backgrounds, including:

- Aboriginal and Torres Strait Islander peoples,
- people impacted by family and domestic violence and individuals who are or have recently been in prison.

If a customer cannot produce standard identification documents, banks and other regulated businesses can use alternative identification options to verify their customer's identity, subject to its risk-based system and controls. Alternative options include:

- referee statements[171],
- government correspondence,
- Indigenous community identity or organisation membership cards and
- customer's self-attestation (as a last resort in instances of low ML/TF risk).

Following publication of the guidance, the Australian Banking Association undertook a project working with its member banks and First Nations community groups to support wider acceptance of First Nations community ID cards by banks.

The project was driven in large part through a community-led forum which helped to highlight the lack of traditional identification in many remote communities and the impact this can have on accessing banking and other services.

To support wider acceptance of First Nations community ID cards, the Australian Banking Association also developed factsheets for banks which includes information

170 Australian Transaction Reports and Analysis Centre on Assisting customers who don't have standard forms of identification (2022) at https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/assisting-customers-who-dont-have-standard-forms-identification.

171 In relation to referee statement as an option to establish a customer's identity, the Australian Transaction Reports and Analysis Centre guidance includes an example form that reporting entities can tailor to meet their specific requirements for a referee statement. It includes information entities can collect from the customer and information for verification by their referee.

about First Nations community ID cards and how they can be used for Know-Your-Customer purposes, and for First Nations community groups to assist current and prospective issuers of First Nations community ID cards by setting out the type and nature of information to display to ensure such cards can be relied upon by banks.

Box 6.2. European Union – Use of asylum seeker's official documentation as an identification method for bank account opening

See also Box 4.3 on "Limited products and services for asylum seekers from high-risk third countries or territories".

In 2016, the European Banking Authority issued an Opinion that clarifies how CDD measures can be adapted to facilitate financial inclusion of asylum seekers from higher risk countries or territories, while maintaining robust AML/CFT controls.[172]

The Opinion suggests that official identity documents issued by a European Union Member State to confirm an asylum seeker's status and his/her right to European Union Member State are likely to be sufficient to meet the identification and verification requirements to access banking services.

Importantly, the European Banking Authority advises that FIs should be mindful how the type of evidence of identity they choose to accept affects the ML/TF risk associated with the business relationship, and determine the most appropriate way to mitigate that risk effectively, for example through enhanced monitoring or providing access only to certain lower risk products or services.

The European Banking Authority guidelines[173] foster a common understanding by institutions and AML/CFT supervisors within the European Union/ European Economic Area of effective ML/TF risk management practices in situations where access by customers to financial products and services should be ensured. More specifically, they include details on how to handle applications from individuals that may have credible and legitimate reasons to be unable to provide traditional forms of identity documentation and on targeted and proportionate limitation of access to products or services on an individual and risk-sensitive basis.

172 European Banking Authority Opinion on the application of CDD to customers who are asylum seekers from higher risk countries or territories at https://www.eba.europa.eu/documents/10180/1359456/EBA-Op-2016-07+(Opinion+on+Customer+Due+Diligence+on+Asylum+Seekers).pdf.

173 European Banking Authority Opinion on the scale and impact of de-risking in the EU (2022) at https://www.eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20(EBA-Op-2022-01)/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-risking.pdf; Guidelines on "policies and controls for the effective management of ML/TF risks when providing access to financial services" (2023) at https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2023/1054144/Guidelines%20on%20MLTF%20risk%20management%20and%20access%20to%20financial%20services.pdf; Guidelines on ML/TF risk factors at https://www.eba.europa.eu/legacy/regulation-and-policy/regulatory-activities/anti-money-laundering-and-countering-financing-1.

Member States including Belgium, France, Germany, Luxembourg, and Sweden have taken measures to ensure access to basic financial services to asylum seekers.

In **Belgium**, a July 2016 Circular of the Central Bank clarifies that the documents issued to persons applying for a residence permit or refugee status by a Belgian authority can be used to verify the identity of the customer.

In **France**, the financial supervisor (French Prudential Supervision and Resolution Authority) issued guidelines in December 2016 to specify that the official identity document called "certificate of asylum seeker" with photograph and an expiration date can be used as a valid identification document by banks.

In **Germany**, a special regulation issued by the Ministry for Internal Affairs provides rules for the customer identification of refugees. For refugees who have to be registered without identity papers a preliminary document ("proof of arrival") can be used.

In **Norway**, the Financial Supervisory Authority had made it possible for vulnerable groups (refugees, asylum seekers) to establish customer relationships with Norwegian banks in case they are not in possession of a passport or other ID documentation. The services are limited to low-risk products., banks may conduct the identification process using alternative documentation[174].

In **Sweden**, the Swedish Bankers Association, in collaboration with the Swedish Migration Agency, designed a process to enable identification of such persons for the purpose of opening a bank account, through Swedish Migration Agency:

The individual presents to the bank:

- The LMA card (Asylum Seeker card), proving that the person has entered the asylum application process and has permission to work
- Copies of their identity-documents, which are made and authenticated by the Swedish Migration Agency upon application for the LMA card.

The Swedish Migration Agency confirms to the bank through an online process:

- At on-boarding: That a person of that name is an asylum seeker and that an authenticated copy if the identity document has been issued
- During ongoing due-diligence: that the person is still part of the asylum-process.

This process is not set in law or regulation, but rather is an agreement between the Swedish Bankers´ Association and the Swedish Migration Agency. It is not mandatory, and not all banks have chosen to use it. However, it has been successfully operated since 2015 and has enabled many refugees to open bank accounts, despite being unable to present formal identity documents.

174 Examples of alternative documentation for customer identification include asylum seeker certificate, copy of a foreign identity card, employment contract for asylum seekers with a work permit issued by the Directorate of Immigration (UDI), confirmation of the customer's identity from a close relative with valid identification, employment contract, housing rental contract.

Throughout the **European Union**, rules on providing basic banking services will also apply in the asylum seeker context[175]: asylum seekers have a right to access and use a payment account with basic features with credit institutions located in the EU Member State where they are established.

175 Directive 2014/92/EU of 3 July 2014 at http://ec.europa.eu/consumers/financial_services/bank_accounts/index_en.htm.

Box 6.3. Fiji – Letter from a suitable "referee" and special monitoring

In Fiji, in a situation where national customers do not have government-issued ID documents, FIs are allowed to rely on a birth certificates (available to all citizens) accompanied with a confirmation letter from a suitable "referee". An FIU guidance provides that:

- A "referee" is defined as a person who knows the customer and whom the FI can rely on to confirm that the customer is who he or she claims to be and can verify other personal details (occupation, residential address) of the customer.
    i. For minors or students, this includes school head teacher, school principal, landlords, parent or guardian.
    ii. For other customers, such as those who reside in the rural areas or villages, suitable "referees" can be a village headman, a chief administration officer, a Provincial Administrator at the Provincial Office, a religious leader, current or former employer, an Official from the Fiji Sugar Corporation sector office (for sugar cane farmers, labourers), an Official from a district government agency such as the Social Welfare Office, Police Station, Health Centers, etc.
- The confirmation letter from a suitable referee should include:
    i. customer's name, address, occupation,
    ii. referee's name, address, occupation and contact details (such as phone number)
    iii. statement stating how long (period) the referee has known the customer
    iv. statement stating that the referee knows the customer by the stated name
    v. statement stating that the referee confirms the customer's stated address and occupation or nature of self-employment to be true and
    vi. signature of the customer and referee with the date the document was signed.

Fiji considered the risk that use of referee certificates could be abused by members of the public due to the ease with which these could be obtained. To mitigate this risk, FIs were advised by the FIU to specifically monitor customers' accounts and transactions for any unusual transaction or pattern of transactions when account opening relied on a "referee" certificate.

Box 6.4. Guatemala – Creation of the Simplified Electronic Information Form for individuals

The Financial Intelligence Unit of Guatemala promotes the implementation of simplified measures through the "*Simplified Electronic Information Form*" to identify and know customers who are individuals in low-risk commercial relationships. The Simplified Electronic Information Form is applicable to accounts, electronic wallets, remittances with an annual accumulated value of up to 60 minimum wages (the minimum wage is approximately USD 505), and credits (up to USD 10,373 accumulated in one or more credit products, during the business relationship). The use of Simplified Electronic Information Form is optional and complementary to other measures such as transactional monitoring and due diligence.

The entities that can make use of the Simplified Electronic Information Form were determined based on the results of the National ML/TF Risk Assessment, particularly the financial inclusion module. Products and services that were previously identified as low risk for the access and use of financial services for the population were examined in order to promote the National Financial Inclusion Strategy. A study was also conducted to analyse the amounts of deposits and credit products to help the thresholds.

Box 6.5. South Africa – Relaxed legal requirements for customer identification and verification

In 2017, the Financial Intelligence Centre Act 2001 and the Money Laundering and Terrorist Financing Control Regulations have been amended to remove the documents required for customer identification and verification before concluding a transaction or a series of transactions with a new customer. In addition, the exemptions which previously applied have been withdrawn. The principle of customer identification and verification is now expanded significantly.

In line with the RBA, regulated FIs:

- can choose the nature and extent, as well as the type of information and the means of establishment and verification of customers' identities[176],
- must describe its customer identification and verification measures in its Risk Management and Compliance Program, including how its standard CDD measures are simplified or intensified, based on the assessed ML/TF risks,
- are not required anymore to carry out the full scope of CDD measures for occasional transactions[177],
- are prohibited from conducting occasional transactions below the threshold for an anonymous person or a person the accountable institution suspects is using a false or fictitious name.

As a result, in such cases, the accountable institution should obtain and record at least some information describing the identity of the customer even if that information does not have to be verified.

Examples of information to be obtained could include the full name and identity number of the customer and other information such as a contact number. An added step of requesting to view an identification document of the customer is advisable. The manner in which the accountable institution complies with section 20A of the Financial Intelligence Centre Act in respect of business relationships and single transactions, both below and above the threshold, must be recorded in the institution's Risk Management and Compliance Program.

176 It can be for example government-issued or other identity documents (physical or digital), or non-documentary means.

177 For example, transactions conducted by persons who have not established a business relationship with the accountable institutions below the threshold set by the Minister of Finance in the Money Laundering and Terrorist Financing Control Regulations (currently = R5000, around USD 275).

Box 6.6. Switzerland – RBA to verifying customer's identity in specific situations

As a rule, for opening of bank accounts banks must prove the identity of their customers using government issued identification documents[178].

In very exceptional cases where the identity of the customer cannot be verified in the prescribed manner, for instance because an individual has no identification documents, the bank may verify the identity by inspecting other credentials or by obtaining corresponding attestations from public authorities. Attestations and copies of substitute documents must be kept on file, and a file memorandum must be created explaining the reasons for the exceptional situation.

Box 6.7. Türkiye – Exhaustive list of acceptable identification documents for targeted groups and acceptance of alternative means of identifications in case of emergencies

In accordance with the national regulators' guidelines, exhaustive list of acceptable identification documents is utilised for customer onboarding procedures. Asylum seekers, refugees and members of other underserved minority groups in Türkiye are granted specific documents for identification.

In this respect, the confirmation of the identity information of people who have International Protection Application Registration Document, International Protection Applicant Identity Document, International Protection Status Holder Identity Document, Stateless Person Identity Document and Temporary Protection Identification Document (Foreign Identification Document) is required in accordance with the relevant provision of the Regulation on Measures document.

On the other hand, if there is no seal (approval) on the temporary protection identity document; the identification number on the document can be used for identification, provided that it is checked from the Identity Sharing System of the General Directorate of Population and Citizenship Affairs and the necessary measures stipulated by the legislation on the prevention of laundering proceeds of crime and the financing of terrorism are taken into consideration.

Following the earthquake in February 2023, for customers whose residence are located in cities declared under a state of emergency, and who could not access their personal belongings (ID cards, etc.), the transactions of earthquake-affected customers were carried out for a duration of one month. [179] This was done by cross-checking at least four of the information listed in the 1st Paragraph of Article 6 of the Regulation, through the identity sharing system database of the Ministry of Internal Affairs, General Directorate of Population and Citizenship Affairs, of the identity information they declared:

- ID number,

178 Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB 16). The decision as to which documents to accept remains within the discretion of the individual banks, leaving banks free to deal with specific situations as appropriate in keeping with an RBA.

179 Communiqué (Sequence No: 23) on the Amendment of the Financial Crimes Investigation Board General Communiqué which was published by the Ministry of Treasury and Finance.

- Mother's and father's name,
- date and place of birth,
- province, district, neighbourhood,
- type and number of identification document,
- mobile phone number,
- e-mail address,
- home and work address information,
- if there are family members included in the relationship information, their birth dates and ages,
- account information and amounts.

As a result of the risk analysis conducted after the earthquake, this practice was allowed for earthquake victims who were identified as low risk, not for everyone living in the region, but for those with low risk.

Box 6.8. United States – Acceptance of alternative identity verifications and addresses

United States AML/CFT regulations require FIs covered by the Bank Secrecy Act Customer Identification Program Rule,[180] such as banks and broker dealers, to have a written Customer Identification Program appropriate for its size and type of business that includes risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. These procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer, based on the bank's assessment of relevant risks.[181] The Customer Identification Program Rule requires FIs to obtain specified identifying information (for individuals, name, date of birth, address, and identification number)[182] but allows risk-based procedures for verifying the identity of the customer. This means that in proven low-risk situations, the bank does not need to verify all four elements of identifying information.

The Customer Identification Program Rule permits covered FIs using documentary or non-documentary identity verification procedures or both at account opening. FIs are permitted to accept government-issued digital credentials (including, e.g., mobile driver's licenses, and a wide range of government-issued identity documents, including municipal identity cards.

Non-documentary identity verification procedures may include:

- contacting a customer;
- independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
- checking references with other FIs; and
- obtaining a financial statement.

180 See, e.g., Customer identification program requirements for banks, 31 CFR 1020.220.
181 See, e.g., Customer Identification Program Rule for Banks, 31 CFR 1020.220(a).
182 31 CFR 1020.220(a)(2)(i).

The Customer Identification Program Rule also permits FIs to accept alternative forms of address for individuals who do not have a residential or business street address, including:

- Army Post Office or Fleet Post Office box number, or
- the residential or business street address of next of kin or of another contact individual.

Under the Customer Identification Program Rule, covered FIs may permit a customer to use an account while the bank attempts to verify the customer's identity, provided the FI's written Customer Identification Program sets out the terms under which this will be allowed and how illicit finance risk will be mitigated. In connection with a customer who opens a credit card account, under the Customer Identification Program Rule, a bank may obtain some of the required customer identity information from a third-party source before extending credit to the customer, which may enable the use of innovative digital identity verification procedures and identity attribute verification services.

Box 6.9. Private Sector, Malawi – Alternative identity verification source and proof of residence for refugee community

In Malawi, a Bank has significantly advanced financial inclusion for refugees by establishing a branch within the Dzaleka refugee camp, specifically catering to refugees and asylum seekers. This initiative was launched in April 2018 with the approval of the regulatory body. To facilitate the KYC process, the bank permits refugees to use factsheets or ID cards issued by UN High Commissioner for Refugees Malawi in lieu of the National IDs used by the host community. Refugees are not required to provide proof of residence, such as utility bills; instead, they must provide a map to their residence within the different zones of the camp. The bank provides a comprehensive suite of services tailored to the unique needs of the refugee community, including savings and transactional accounts, fixed deposits, access to ATMs, agency banking, money transfers, financial literacy programs, and foreign exchange transactions. These services empower refugees to manage their finances effectively, fostering economic independence and stability.

As of December 2024, the bank has 14,800 active bank accounts held by refugees.

Box 6.10. Private sector, Sierra Leone – Usage of Employee Identification Card in Sierra Leone

A significant portion of Sierra Leone citizens do not have government-issued identification documents. As such, it is difficult for FIs to obtain government-issued ID documents for individuals (customers and related parties).

As part of financial inclusion, a bank permits the usage of employee identification card supported with a letter from the employer to serve as an appropriate identification document that can be collected to verify the identity of prospect.

This exemption only applies to those national customers or related parties whose employers are existing customers of the banking group where there is an established ongoing relationship. The bank must also confirm that all other ways to obtain and verify the information have been attempted and there is a valid reason for not being able to provide the other preferred forms of identification documents. In all instances, a certificate of birth and a letter from the employer on the employer's letterhead, subject to verification of authenticity, is required.

This is in line with the guidance in the Joint Money Laundering Steering Group Guidance for individuals who are not able to provide standard identification evidence.

Box 6.11. Private Sector, United Kingdom – Special measures to provide flexibility in acceptable identification and verification documents for dedicated groups

A bank partners with different charities to provide special supports to specified disadvantaged groups (e.g. domestic abuse victims, adult survivors of modern slavery, prisoners, etc.)

- Domestic abuse charity: this project seeks to assist customers fleeing domestic abuse, arising from an incident or a pattern of behaviour that is used by someone to control or obtain power over their partner or ex-partner. This includes controlling ID, salary and bank accounts. The bank works with the charity to provide accounts to those fleeing such situations, providing flexibility in terms of acceptable identification and verification documents, which may include a letter from the supporting charity.
- National referral mechanism for adult survivors of modern slavery: the bank works with a charity which provides specialist support to protect and care for adult survivors of modern slavery in England and Wales since 2011 under the National Referral Mechanism. The National Referral Mechanism is a framework for identifying and referring potential victims of modern slavery and ensuring they receive the appropriate support. The charity works with local charities to support victims in rebuilding their lives. The bank works with the charity to provide accounts and is flexible on what it considers acceptable identification and verification documents, which may include a letter from the supporting charity.
- Prisoner banking programme: established in 2010 following a pilot project run by national charity, the programme operates in England and Wales and enables prisoners who are about to be released to apply for and open a Basic Bank Account, ahead of their release without providing identification and verification documents. Instead, a witnessed identification document is supplied along with the application form, signed by a member of the Ministry of Justice to attest that the applicant's details are correct. The programme only relates to basic bank accounts and does not extend to any other products that a bank may wish to offer a prisoner. The bank works with 25 partner prisons helping offenders rehabilitate back into society through the provision of access to banking.

Box 6.12. Private Sector, United States – Accepting different types of documents to verify identity

A United States bank created a dedicated internal group to promote and coordinate financial inclusion efforts and AML compliance objectives to provide banking services to historically marginalised communities. The bank allows several different types of identity documentation for verification, including municipal IDs, which themselves are backed by a range of options for evidence of core identity factors or varying reliability. The bank requires additional types of identity documents to verify identity if the primary document is a municipal ID.[183] It also provides alterative evidence and means to verify identity, including the address requirement, for people without permanent addresses.

On the other hand, several large United States banks that do not accept municipal IDs do accept other alternative identity documents to facilitate financial inclusion as part of a "tailored approach"[184] to balancing AML/CFT requirements and financial inclusion, focusing on effectiveness. To promote financial inclusion and meet the requirements of the Bank Secrecy Act Customer Identification Program Rule, the banks tailor the type of customer information collected, and the evidence used to verify it to individual cases. For example, Afghan refugees may have letters from the United States government and unhoused people may have letters from charities or shelters, which the banks may use on a case-by-case basis to verify their identity. Two of these banks also noted that in some cities, they participated in a programme to facilitate financial inclusion for victims of domestic violence by concealing all or part of the individual's address or enabling the customer to use a temporary shelter as the address.

Delayed verification of identification information

Box 6.13. Egypt – Utilisation of mobile payment and prepaid card services with limitations prior to verification

According to the CDD measures issued by the Egyptian Money Laundering Combating Unit, for mobile payment service and prepaid card service customers and financial inclusion product and service customers, a customer may utilise the business

183 Other United States banks reported that they do not accept municipal IDs as a primary form of identification due to fraud concerns and aligning their programme controls with the National Anti-Money Laundering and Countering the Financing of Terrorism National Priorities, which identifies combating fraud as a national priority. See Financial Crimes Enforcement Network, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (June 30, 2021)

184 It is important to note that the substance of simplified or alternative AML/CFT compliance measures, not what they are called by regulators, supervisors, or regulated entities. The large banks in this example use the term, "tailored approach," to refer to their use of proportionate, risk-based CDD actions to facilitate financial inclusion and consider it distinct from SDD because in their experience, customers belonging to underserved or excluded communities, such as refugees or survivors of human trafficking, often do not present the lower illicit finance risks required to apply SDD. These banks generally reserve the term, SDD, for regulated entities, government agencies/bodies, or companies whose securities are listed on a recognised exchange—customers of a very different nature than those targeted for financial inclusion.

relationship prior to verification, provided that limitations are set to the number, amounts and type of the transactions which can be conducted, until the said documents, information or data are completed. Setting threshold to the values and type of transactions that can be conducted falls under the risk management procedures.[185]

Box 6.14. India – Delayed submission of Officially Valid Document

The requirement to submit an Officially Valid document with the current address for the purpose of CDD is cumbersome for the migrant population. The customer who does not have an Officially Valid document with current address on it is permitted to submit a deemed Officially Valid document as current address proof. However, such a customer should submit an Officially Valid document with current address within 3 months of submission of the deemed Officially Valid document.

Minimum-detail Prepaid Payment Instruments, which have transaction and loading limitations, have been permitted to be issued to customers with simplified KYC requirements wherein mobile-One-Time Password authentication and Officially Valid document number would suffice.

185 See Simplified CDD Procedures for Mobile Payments at https://www.cbe.org.eg/-/media/project/cbe/page-content/rich-text/aml-and-cft/regulations/simplified-cdd-procedures-for-mobile-payments_ar.pdf and Simplified CDD Procedures for Prepaid Cards at https://www.cbe.org.eg/-/media/project/cbe/page-content/rich-text/aml-and-cft/regulations/simplified-cdd-procedures-for-prepaid-cards_ar.pdf.

Examples of digital ID and biometric data registries

Box 6.15. Argentina – Policies for digital identification and remote onboarding / information sharing

The Registro Nacional de las Personas (the national registry of individuals) has developed the Digital Identity System (*Sistema de Identidad Digital*) that links the IDs with biometric information. The purpose of this system is to create a digital ID that citizens can use to access services or carry out procedures using any electronic device with a mobile connection.

The identification, verification and acceptance of customers may be carried out remotely[186], using electronic means substitutes for physical presence, with the use of rigorous, storable, auditable biometric techniques that are not manipulable. These electronic means must have protection against fraud due to physical and digital attacks and be used for the purpose of verifying the authenticity of the information provided, and the documents or biometric data collected. FIs must have controls in place for identity verification, which generally comprise:

- scan of the national identity document,
- selfie or video of the person's face,
- validation of image integrity: detection of invalid, altered or forged documents,
- controls to determine that the person using the app is physically present ("proof of life"),
- verification of the submitted document with the Registro Nacional de las Personas database and of the link between the document, the data and the scanned photo.

To facilitate remote onboarding, the Banco Central de la República Argentina allows financial entities[187] to share information about their customers that allows other financial entities to open an account for those customers remotely[188].

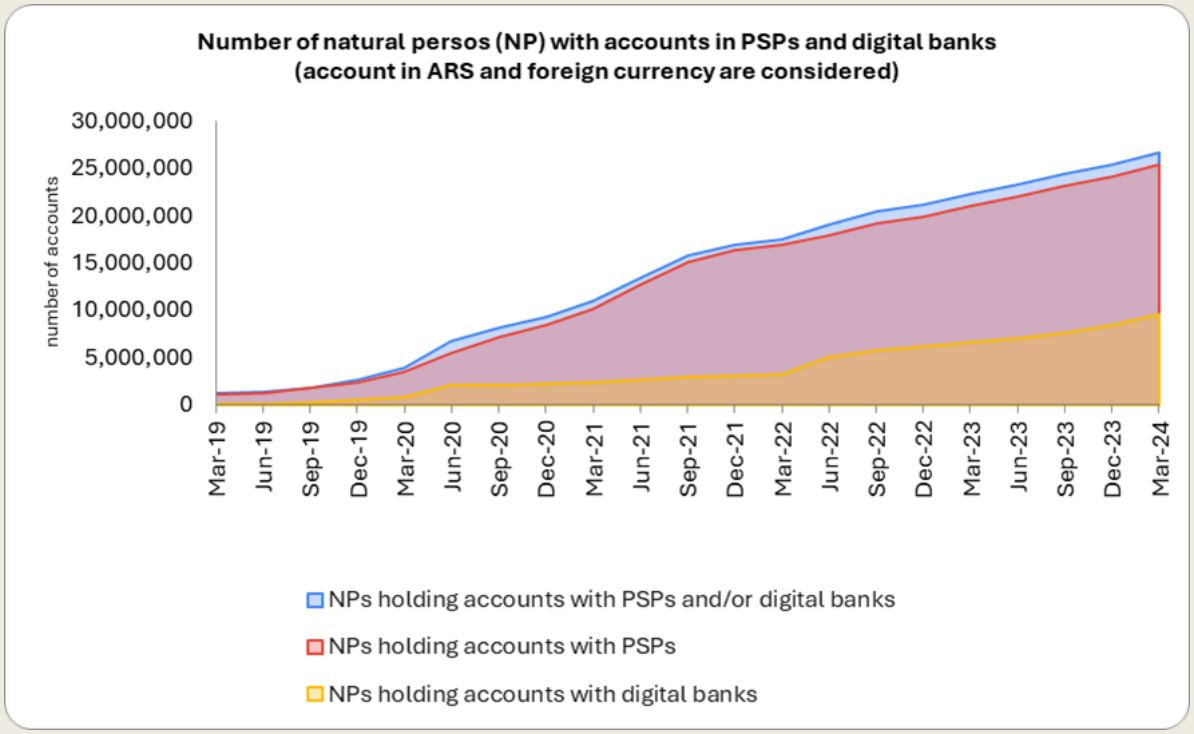
The implementation of digital identity systems has allowed people to open accounts online and to get remote access to the financial system, thus boosting financial inclusion. As shown in the charts below, the number of natural persons holding accounts reached 36.3 million (nearly the entire adult population) in December 2023 (a net increase of 8.1 million (28%) compared to December 2019). The growth in the number of adults holding both bank and payment accounts stands out. The number of people holding both

186 Article 25 of the Resolution 14/2023 of the Financial Information Unit at https://servicios.infoleg.gob.ar/infolegInternet/anexos/375000-379999/379085/texact.htm. Remote customer onboarding is conducted pursuant to the provisions set out by the Banco Central de la República Argentina in paragraph 3.3—titled "Digital Identification"—of the Consolidated Text on Minimum Requirements for the Management and Control of Information Technology and Security Risks related to Digital Financial Services at https://www.bcra.gob.ar/Pdfs/Texord/t-rmrtsd.pdf

187 In accordance with the provisions of article 39, paragraph d) of Law 21,526.

188 Communication "A" 6059 to financial institutions (8 September 2016) at https://www.bcra.gob.ar/Pdfs/comytexord/A6059.pdf.

types of accounts climbed from 1.9 million in 2019 to 22.1 million in 2023, reaching 63% of such segment.[189]



189 See Informe de Inclusión Financiera by Banco Central de la República Argentina (April 2024) at https://www.bcra.gob.ar/Pdfs/PublicacionesEstadisticas/IIF-segundo-semestre-2023.pdf; As for account activity, there is a narrower gap between holders of accounts and those having activity in their accounts. 25.5 million natural persons made at least one credit or debit transaction in any of their accounts in the fourth quarter of 2023, that is, 70% of natural persons holding accounts as of December 2023. This set of natural persons recorded a net increase of 7.6 million compared to the same month a year earlier, which means a 42% rise.

Box 6.16. India – JAM Trinity strategy: Financial Inclusion through a multi-pronged approach

In India a multi-pronged approach to promote financial inclusion and promote transactions through financial channels was developed called JAM Trinity[190], based on three pillars:

The first pillar of this strategy was launched in 2024 aimed at providing universal, affordable, and formal access to financial services to the unbanked population. As per the Global Findex, access to financial services increased from 35% of total population in 2011 to 53% in 2014 to 80% in 2017.

The second pillar is a biometric-based identification for every citizen called "Aadhaar", integral to India's digital governance framework:

- a 12-digit unique identification number issued by the Government of India, designed to ensure data security,
- links biometric data with demographic details,
- used for government subsidies, taxation, banking, welfare programs, and supports direct benefit transfers,
- used as an electronic identity authentication process[191] in banks.

The Central KYC Record Registry is a centralised repository of KYC records of customers in the financial sector with uniform KYC norms and inter-usability of the KYC records across the sector. Launched in 2016, it caters to reporting entities of all four major regulators of financials sector.[192] As of 2024 Central KYC Record Registry hosted more than 940 million KYC records.

The third pillar is the development of a digital payment ecosystem which has been accorded the highest priority by the Government of India, including:

- establishment of platforms to enhance digital payment capabilities, [193]
- launch of the digital payment solution e-RUPI, a cashless and contactless instrument for digital payment.

190 JAM stands for "Jan Dhan", "Aadhaar", and "Mobile": "Jan Dhan" refers to a financial inclusion program that aims to expand affordable access to financial services such as bank accounts, remittances, credit, insurance and pensions; "Aadhaar" is a biometric identification number given to each resident; "Mobile" refers to mobile phones.

191 A customer can present his/her "Aadhaar" number at any banking location that is equipped with a biometric fingerprint reader. The customer has to provide the bank with permission to obtain e-KYC details from the Unique Identification Authority of India database and get his/her fingerprint captured. The bank then sends the customer's "Aadhaar" number and fingerprint to the Unique Identification Authority of India server. If the information matches, a bank can instantly open an account for the customer.

192 Under the arrangements, clients need to submit their KYC details only once with any of the reporting entities of Reserve Bank of India, Securities and Exchange Board of India, Insurance Development and Regulatory Authority of India and Pension Fund Regulatory and Development Authority at the time of account opening. Thereafter, they are assigned a unique Central KYC Identifier which can

Box 6.17. Private Sector, Luxembourg – Centralised KYC repository

An operator established in Luxembourg in December 2019 under a "Support Professional of Financial Sector" license also acts as a centralised KYC repository for customer due diligence purposes for customer onboarding and when updates are required in the course of the business relationship of the customer with the professional of the financial sector subject to AML/CFT laws. The platform allows the exchange of customer information, which ultimately also facilitates the change by the customer from one professional of the financial sector to another.

Box 6.18. Private Sector, South Africa – National biometric ID database for AML/CFT scanning

A bank uses South Africa's universal biometric ID coverage and digital ID database, managed by the Department of Home Affairs, to automatically identify customers for AML/CFT requirements. An applicant first enters his or her ID card number. The bank uses the number to connect to the national ID database and pulls customer data. The customer scans his or her fingerprints, which then are compared with the biometrics from the national database. The fingerprint reader uses a thermos-scanner to determine whether a real person is using the kiosk. Once the individual is identified as a real person, his or her information is scanned for AML and sanction concerns, the customer account is created, and a personalised card is printed and disbursed by the kiosk.

Box 6.19. Private Sector, The Netherlands – List of possible SDD measures

The Dutch Banking Association provided a list of possible SDD measures that should be proportionate to the bank's risk profile and the specific lower risk elements (e.g., customer, product, geography, transaction and delivery channel) identified, with sufficient monitoring systems to ensure detection of unusual or suspicious transactions.

Simplified and automated risk assessment

- Conduct a basic risk assessment instead of a comprehensive analysis, focusing on key risk factors.
- Encourage the use of automated tools for the risk assessment.
- Simplify onboarding and reviews by access to trusted national databases to minimise manual verification and reduce the administrative burden for customers.

Exemption from detailed source of funds or source of wealth check

be used by the client when they are establishing an account-based engagement with any other reporting entity.

193 Bharat Interface for Money-Unified Payments Interface, Immediate Payment Service, and pre-paid payment instruments.

- No analysis of the origin of funds or wealth where the transaction volume, customer profile, and business operations indicate lower risk.
- Use of publicly available information or existing customer records, reducing the need for additional customer outreach.
- Permit banks to forego customer inquiries when dealing with lower risk transactions.

Simplified verification of beneficial ownership

- For entities with simple, transparent ownership structures allow reliance on publicly available records or confirmation by the customer of ultimate beneficial ownership-information obtained from the central registry.

Exemption from periodic reviews

- Exempt periodic reviews of lower risk customers, particularly those with predictable financial behaviour, and allow sole reliance on event-driven reviews.

Reduction of required datapoints

- Offer flexibility in data collection requirements for lower risk customers to minimise unnecessary burden while maintaining compliance.
- Clear guidance from authorities would reduce inconsistencies across banks and increase predictability of KYC processes for customers.
- Examples of reduced measures for lower risk customers:
    - For natural persons only information will be collected that is essential to verify the identity and ensure adequate ongoing monitoring, such as names, date of birth, nationality and address including country of residence. Obtaining information on place of birth may be excluded as the date of birth is sufficient for identity verification. Similarly, secondary nationalities may add little value if the primary nationality is adequate to assess risks.
    - For business customers, focus will be on key identifiers, such as business name, address, names of ultimate beneficial owner(s) and representative(s), and may exclude exhaustive structure, nominee shareholder and director (limiting senior managing officials to board level) details. Also, the tax identification number may be excluded as this is not directly relevant to the risk assessment.

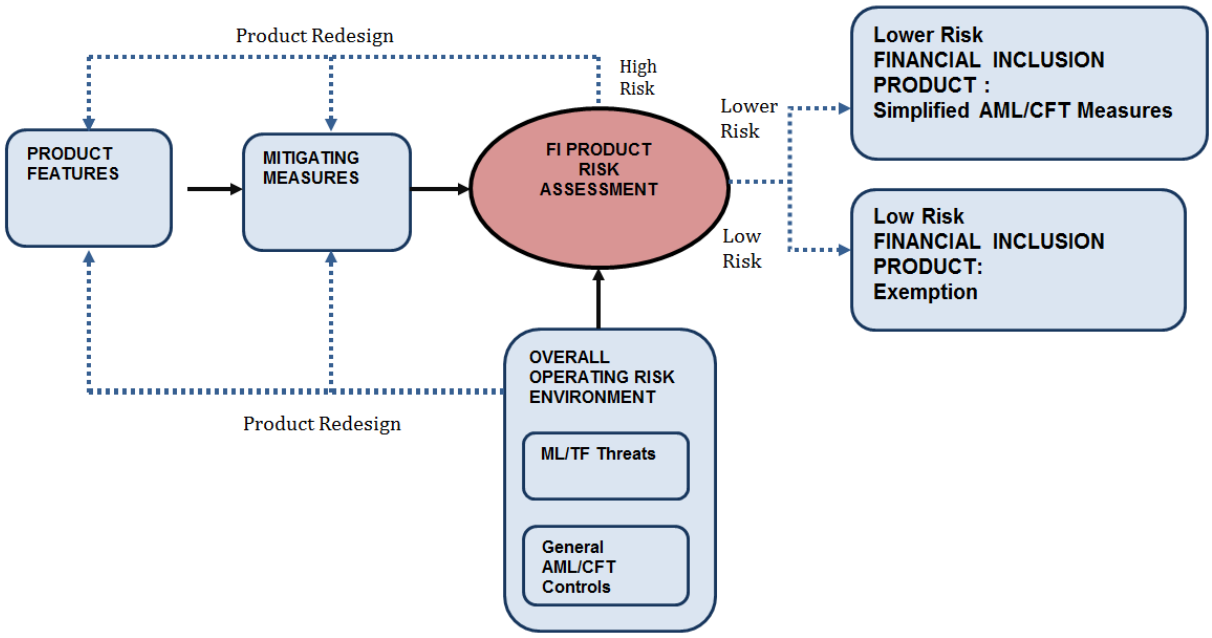
Annex A7 World Bank's financial inclusion product risk assessment module

The World Bank has developed a standalone ML/TF risk assessment module[194] specifically to facilitate the assessment of the ML/TF risks associated with "*financial inclusion products*" in a systematic and evidence-based way. The module is based on following four steps:

Step 1 –Analysing the product features and their risk implications At the first step of the assessment, the assessor identifies the features of the product and their possible implications on the ML/TF risks. For example, having features such as "availability of international transactions", "non-face-to-face account opening", "anonymity", "delivery through agents", "availability to non-resident/non-citizens", or "availability to legal persons" increases inherent risk of the products and therefore, the need for stronger mitigating measures. In contrast, introducing a cap on transaction size and/or number or limiting some of the functions of the product reduces the risk level.
Step 2 – Assessment of Risk Mitigation Measures The second step of the assessment focuses on the adequacy and quality of risk mitigation measures that are linked with each product feature. For example, if the product has a cap for amount or number of transactions, the module asks questions about the existence and quality of the analytical work that informed the decision for this cap. If the product allows international transactions, the module asks questions about the quality of relevant monitoring mechanisms of the institution. Moreover, if the product is offered through agents the procedures for onboarding, training, and monitoring of the agents need to be assessed.
Step 3 – Assessing the impact of country risk context on the product The risk context of the country is important, because a financial inclusion product that may have low risk in a certain country context may not be necessarily low risk in another country. Step 3 of the assessment allows users to reassess the mitigation measures, considering the country's ML /TF threat and vulnerability context. The quality of the supervision and institution's capacity to detect and mitigate the risks are also assessed in this step. Inputs from country's national ML/TF risk assessment are crucial for this step.
Step 4 – Overall assessment This final step facilitates the assessment of the ultimate net risk level which is a function of the product features, risk mitigation measures, and country's risk context. The country or institution may consider (or justify) a SDD regime only if the assessment results in "lower" or "low" risk. If the assessment results are "medium" or "high" the country may use the module as a basis for the redesign of the product, then reassess the risk level. Limiting the functions of the product, lowering the caps, or improving the control and mitigation measures may reduce the risk level of the product.

194 Formerly named as FIRAT.

Figure A7.1. The structure of the Financial Inclusion Product Risk Assessment Module



The diagnosis of the impediments to financial inclusion is essential to determine the most appropriate policy for SDD:

The Financial Inclusion Risk Assessment Module is being introduced to countries in a workshop. Typically, this workshop brings together experts from the financial intelligence unit, the financial sector supervision department, the financial inclusion department or group (usually part of the central bank), telecom authorities (with regulatory responsibilities for mobile money), and representatives from the private sector. The main objective of this workshop is assessing the impact of a country's current AML/CFT regime on financial inclusion and analysing how and to what extent possible simplifications of CDD requirements can help reduce financial exclusion.

This workshop usually provides a clear idea about the interplay between the current CDD requirements and financial inclusion in the country.

In some countries (such as Zambia, Tanzania, Bangladesh) this analysis showed that some parts of the CDD requirements were too stringent for the country conditions and were impeding access of certain low risk categories of customers to finance. On the other hand, in some other countries like India, the analysis concluded that the country's CDD regime was flexible enough to accommodate financial inclusion and that the developments in e-KYC further reduced the need for relying on SDD practices.

The workshops start with a stocktaking discussion that attempts to analyse the country's CDD regulatory framework in force, as well as the state and reasons of financial exclusion. Next, the financial inclusion risk assessment module is being introduced to the country's in-house assessors. Following the four-step methodology, explained in the previous page the assessors use the module for assessing the risk level of current or planned financial inclusion products/services in the country.

Some examples of financial inclusion products with a lower or low ML/TF risk:

The table below shows a sample of the financial inclusion products that have been assessed and found to be "lower" or "low risk" by some of the countries which used the module. As seen in the sample, most of the countries concluded that their regulatory framework requires revisions to better recognise the SDD and accommodate financial inclusion.

Table 1. Examples of financial inclusion products assessed and found to be "lower" or "low risk"

Country	Financial Inclusion Product with Low or Lower ML/TF Risk*	Assessment's Conclusion on CDD Regulatory Framework
Bangladesh	Farmer Accounts. School Banking Accounts. Accounts for Street Children.	Country's regulatory framework required revision to facilitate SDD.
India	Basic Bank Accounts	Country's regulatory framework facilitated SDD.
Malawi	Basic Saving Accounts. Basic Credit Accounts. Ordinary Farmer Bank Accounts. Micro-Credit.	Country's regulatory framework required revision to facilitate SDD.
Nigeria	Low Amount Saving Accounts. Micro-Insurance Products. Micro-Credit Products. Some Mobile Money Products.	Country's regulatory framework facilitated SDD.
Sri Lanka	Micro-Credit Products. Community Lending Products. Micro-Insurance Products.	Country's regulatory framework required revision to facilitate SDD.
Tanzania	Basic Saving Accounts (Chap-Chap Accounts and Similar). Group Micro-Lending Products. Certain Mobile Money Products (by Some Operators).	Country's regulatory framework required revision to facilitate SDD.
Zambia	Zampost Salary Payment Service Zampost Money Transfer Certain Mobile Money Products Certain E-Wallet Products. Zanaco Xapid Account	Country's regulatory framework required revision to facilitate SDD.

*The countries assessed a broader range of products. The products that were not found to be low risk did not qualify for SDD- and have therefore not been included in this table.

Annex B. Detailed description of the other recommendations relevant for financial inclusion

Annex B provides an extract of detailed description of the other recommendations relevant for financial inclusion as laid out in Chapter 2 Section IV of the 2017 Financial Inclusion Guidance.

IV. The FATF Recommendations in the light of financial inclusion objectives

4.1. CUSTOMER DUE DILIGENCE (RECOMMENDATION 10)

61. Under the FATF Recommendations, FIs must perform customer due diligence (CDD) in order to identify their clients and ascertain information pertinent to doing financial business with them. CDD requirements are intended to ensure that FIs can effectively identify,[195] verify and monitor their customers and the financial transactions in which they engage, in relation to the money laundering and terrorism financing risks that they pose.

62. The three core elements of "identification", "verification" and "monitoring" are interrelated and closely associated in the FATF Recommendations. They are intended to reinforce each other so that the FI builds knowledge of the customer that is crucial from an AML/CFT perspective.

63. The revised FATF Recommendations have not modified the basic CDD requirements. They do, however, clarify how the broad RBA principle relates to the implementation of CDD measures. In particular, and of specific relevance to financial inclusion, the revised FATF Recommendations provide indicators to identify potential lower risks factors (INR.10. par.16 to 18), and examples of simplified due diligence measures that the RBA allows (INR.10. par.21.). These examples are intended as illustrations only, and should not be read as either exhaustive or mandatory.

Circumstances in which CDD must apply

64. Under the FATF Recommendations, all FIs that are subject to AML/CFT obligations are required to implement CDD measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;[196]
- carrying out occasional transactions above USD/EUR 15 000 or that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;
- there is a suspicion of money laundering or terrorist financing; or
- the FI has doubts about the veracity or adequacy of previously obtained customer identification data.

195 FATF Recommendation 10 does not allow financial institutions to keep anonymous accounts or accounts in obviously fictitious names.

196 The FATF Recommendations do not define this notion. It is left to countries to decide whether business relations are established.

CDD measures - general

65. Pursuant to these transaction thresholds and other criteria, the institutions, professions and businesses subject to AML/CFT obligations must:

a) Identify the customer and verify that customer's identity, using reliable, independent source documents, data or information.

b) Identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner, such that the FI is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include FIs taking reasonable measures to understand the ownership and control structure of the customer.

c) Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

d) Conduct ongoing due diligence on the business relationship and scrutinize transactions throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer and its business and risk profile, including, where necessary, the source of funds.

66. Applying these CDD measures is challenging for financial service providers, particularly FIs dealing with "small" clients and those in Low Capacity Countries. It is essential to distinguish between identifying the customer and verifying identification. Customer identification entails the gathering of information on the (future) customer to identify him/her. At this stage, no identification documentation is collected. In contrast, the verification of the customer identification requires checking reliable, independent source documentation, data or information that confirms the veracity of the identifying information that was obtained during the identification process.

67. Industry feedback highlights a number of practical difficulties regarding identification and verification requirements, most of which arise pursuant to national legislative or regulatory requirements, and not the FATF Recommendations. For instance, in a normal CDD scenario, the FATF Recommendations do not require information to be gathered on matters such as occupation, income or address, which some national AML/CFT regimes mandate, although it may be reasonable in many circumstances to seek some of this information so that effective monitoring for unusual transactions can occur. Similarly, although a majority of countries specify the use of a passport or government-issued identification card as one of the methods that can be used to verify the identity of customers, the FATF Recommendations do allow countries to use other reliable, independent source documents, data or information. This flexibility is particularly relevant for financial inclusion, since low income migrant workers, for example, often lack standard identification documents. Rigid CDD requirements that insist on government-issued identification documents, adopted by some countries or FIs, have acted as barriers to these disadvantaged populations obtaining access to the formal financial system.

CDD measures - lower risk scenarios

68. The revised FATF Recommendations allow for simplified CDD measures where there is a lower risk of money laundering and terrorist financing (INR. 1 par.5. and INR 10. par.16 to 18 and par.21). This is an option that is open to all countries. Jurisdictions may consider establishing a simplified CDD regime, for specifically defined lower risk customers and products. Countries may also allow FIs to decide to apply simplified CDD measures in lower risk situations, based on their own institutional risk analysis. In any case, simplified CDD measures is not permitted if there is any suspicion of money laundering, or terrorist financing, or where specific higher-risk scenarios apply.

69. *Examples of lower risk situations*. The FATF gives examples of circumstances where the risk of money laundering or terrorist financing might be considered as potentially lower, in relation to particular types of customers, countries or geographic areas, or products, services, transactions or delivery channels (INR. 10 par. 17). The examples are not prescriptive and do not amount to an exhaustive list. The FATF explicitly includes as one lower risk example "*financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes*". This means that it could be reasonable to apply simplified CDD measures for customers of products fulfilling those conditions. For instance, so-called "small bank accounts"[197] for unbanked individuals who lack acceptable identification documents, where the account has caps on overall value, frequency of use, and size of transactions to mitigate the risk of potential for misuse while still providing adequate functionality. This would be particularly relevant for individuals who rely on remittances from family members living and working away from home. FIs still need to monitor lower-risk accounts, but it may be appropriate to do so less frequently and less intensely than with standard-risk accounts, which allows a more efficient allocation of resources, permitting FIs to focus their compliance resources on higher risk threats. In all situations of simplified CDD, the lower risk circumstances will have to be confirmed based on a thorough and documented risk assessment, conducted at the national, sectoral or at the FI level (INR. 10 par. 16).[198]

70. As the above example makes clear, the FATF Recommendations support the development of entry-level banking or other financial products that will facilitate the integration of financially excluded people into the formal financial sector and mitigate ML/TF risks relating to financial exclusion. Countries will have to specify the different criteria required to benefit from a simplified CDD regime or require FIs to do so within their own risk management framework. In general, targeted products may include several specific conditions such as the customer being a natural person, limited transactions in amount (*e.g.,* withdrawals not exceeding X EUR/USD per day or X per month), limited account balance at any time etc.

71. *Application of simplified measures.* Simplified CDD never means a complete exemption or absence of CDD measures. A simplified set of CDD measures may be basic and minimal but must still respond to each of the four CDD components that apply to "standard" customer relationships and transactions. [199] In line with the RBA approach[200], it is the intensity and the extent of customer and

197 Such accounts lay also be referred to as low-value, simple or no-frills accounts
198 See par. 40 and s.
199 See par. 65.
200 See par. 37 and s.

transaction information required, and the mechanisms used to meet these minimum standards that will vary depending on the risk level. In a lower risk context, fulfilling CDD customer identification, verification and monitoring requirements of Recommendation 10 could for example entail less intensive and formal means of information gathering and monitoring and a reliance on appropriate assumptions regarding the intended usage of basic products, or less detailed and frequent information.

72. INR. 10 par.21 provides a number of examples of possible simplified measures with respect to the timing and verification of customer identity and intensity of transaction monitoring. Again, these examples are proposed for guidance only and should not be considered as prescriptive or exhaustive. They include the possibility of verifying the identity of the customer and the beneficial owner after the establishment of the business relationship, reducing the frequency of customer identification updates or reducing the degree of ongoing monitoring and scrutinising transactions, based on a reasonable monetary threshold. [201]

73. Regarding beneficial ownership requirements, in a financial inclusion context the beneficial owner will in most instances be the customer him/herself, or a closely related family member. Situations where suspicions arise that the account holder is used as a strawman, or frontman and is not the real owner,-should not be treated as a lower risk and normal or enhanced measures should be applied (INR. 10 par. 15 a).

74. Countries may consider applying a so called "progressive" or "tiered" KYC/CDD approach whereby low transaction/payment/balance limits could reduce money laundering and terrorism financing vulnerabilities. The stricter the limits that are set for particular types of products, the more likely it would be that the overall ML/TF risk would be reduced and that those products/services could be considered as lower risks. Simplified CDD measures might therefore be appropriate. This approach may provide undocumented (financially excluded) individuals access to accounts or other financial services with very limited functionalities. Access to additional services (*e.g.,* higher transaction limits or account balances, access through diversified delivery channels) should be allowed only if/when the customer provides proof of identity and address. For example, in India, the government amended the AML/CFT regulations to authorize banks to open a "small" or "no frill" savings account for low income customers lacking acceptable forms of identification, using simplified CDD norms. The account is subject to strict limitations on the yearly aggregate of all credits, the monthly aggregate of all withdrawals and transfers, and the balance at any point. It can only be opened at an institution with core banking facilities that can monitor the account and ensure that the transaction and balance limits are observed. The account is operational for 12 months and can only be renewed for another 12 months if the account holder provides evidence that he/she has applied for valid identity documents within a year of account opening. [202]

201 Specific examples of simplified measures which could be envisaged by countries for each step of the CDD process to accommodate the specificities of lower risk financial inclusion products or situations are detailed in the following paragraphs.

202 See also experiences from Mexico, Malawi, Brazil, Pakistan as part of Annex 7.

CDD measures – customer identification

75. The FATF Recommendations do not specify the exact customer information (referred to by certain countries as "identifiers") that businesses subject to AML/CFT obligations should collect to carry out the identification process properly, for standard business relationships and for occasional transactions above USD/EUR 15 000. Domestic legislation varies, although common customer information tends to consist of name, date of birth, address and an identification number. Other types of information (such as the customer's occupation, income, telephone and e-mail address, etc.) are generally more business and/or anti-fraud driven and do not constitute core CDD information that must be collected as part of standard CDD—although such information could appropriately be part of enhanced CDD for higher risk situations.

76. The FATF Recommendations allow countries' laws or regulations to apply an RBA to the types of customer information that must be collected to start a business relationship. A carefully balanced approach has to be taken, because if identification processes are too lean, monitoring may make a limited contribution to risk mitigation, and manual or electronic scanning of transactions may not be able to identify individual suspicious activity effectively[203]. In some countries, differentiated CDD requirements have been introduced, in relation to certain types of financial products. For instance, in Colombia, a 2009 modification of the Finance Superintendence of Colombia (SFC) Basic Banking Circular simplified AML/CFT procedures for low-value electronic accounts and mobile accounts that are opened via agents (who receive and forward the application materials).

CDD measures – verification of customer identification

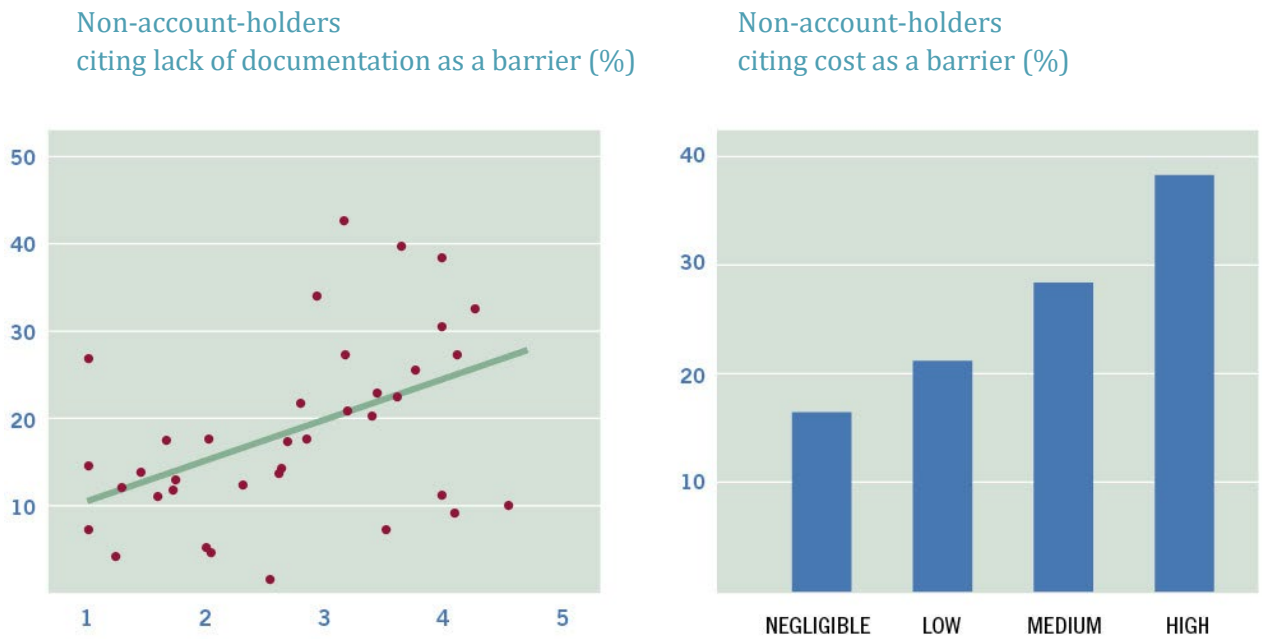
77. The FATF Recommendations require FIs to verify the customer's identity using reliable, independent source documents, data or information. When determining the degree of reliability and independence of such documentation, countries should take into account the potential risks of fraud and counterfeiting in a particular country. It is the responsibility of each country to determine what can constitute "reliable, independent source documents, data or information" under its AML/CFT regime. The general application of the RBA can introduce a degree of flexibility as to the identity verification methods and timing.

78. According to the industry, the customer identity verification stage is, in all instances, the most difficult and burdensome part of the process. Rigorous verification requirements can act as a disincentive for financial inclusion.

79. The World Bank has pointed out that respondents to its recent survey often quoted lack of documentation as one of the central reasons for not having an account, especially in countries that require extensive or formal, government-issued documentation: [204]

203 See also par 102.
204 World Bank (n.d.).

Figure B1. Objective data support perceptions of documentation requirements and cost as barriers to use of formal accounts



Note: Data on number of documents required are for 2005. Data on annual fees are for 2010 and reflect scoring by the national central bank. The sample for the left-hand panel includes 38 economies, and the sample for the right-hand panel 100 economies.
Source: Demirguc-Kunt, A. and Klapper, L. (2012); World Bank, Bank Regulation and Supervision Database; World Bank Payment Systems Database

80. *Relying on a broader range of acceptable identification means*. To address such challenges[205], countries have expanded the range of acceptable IDs for the verification process to include such documentation as expired foreign IDs, consular documents or other records that undocumented people can typically acquire in the host country (bills, tax certificate, healthcare document, etc.). Using an RBA, local authorities have often allowed a broader range of documentation in pre-defined types of business relationships and for specific (financial inclusion) products and accounts, with low balance limits. [206] Countries should take advantage of the RBA to facilitate proportionate requirements with regard to acceptable IDs that will support the provision of relevant services to unserved groups. [207]

81. Groups such as community-based financial cooperatives that provide defined financial services to their members only, can have a CDD regime that takes note of their nature. The financial service provider can leverage off the membership process for persons to become members of the

205 This may address the issue of the identification of children since children generally lack IDs and at times do not have guardians.
206 See experiences from various countries in Annex 5.
207 However, the ability to identify individuals reliably is fundamental not only to financial services, but also to distribution of social welfare support and safeguarding national security, so that where it is lacking authorities should prioritise the development of a national system to identify citizens.

cooperative to also meet CDD requirements. This may be considered an alternative form of CDD which reaches the same objective as the normal identification and verification process in retail FIs.

82. *Fraud risk relating to alternative acceptable IDs*. Countries should remain mindful that alternative forms of acceptable identification may be more susceptible to fraud and abuse. For instance, whether reliance can appropriately be placed on a letter from a village chief to verify a customer's identity depends on the village chief's integrity and knowledge of the customer. In some reported cases, village chiefs began to demand money for their "verification services". Although such abuse may not be widespread, it is important to remember that like every method of verifying customer identification, alternative identification processes require some basic due diligence and monitoring to ensure integrity and reliability. A proper risk analysis is crucial to support the adoption of verification processes that are proportionate to the level of ML/TF risk.

83. In South Africa, in May 2010, the Financial Intelligence Centre issued an advisory to banks instructing them not to accept documents issued by the South African government to asylum-seekers evidencing their asylum applications as identification documents for the purpose of opening bank accounts. However, following litigation challenging that position, a compromise was reached allowing banks to accept the asylum documentation to verify identity but only after confirming the authenticity of the document with the Department of Home Affairs.

84. *Postponing ID verification*–Amongst the examples of simplified CDD measures in INR. 10 par. 21, the verification of the customer's (and beneficial owner) identity after establishment of the business relationship is envisaged, *i.e.* if account transactions rise above a defined monetary threshold. As part of a tiered CDD approach, [208] customers can be provided with limited and basic services, and access to a full or expanded range of services or higher transactions ceilings would only be granted once full identity verification has been conducted.

85. This flexible approach for limited purpose accounts, where verification is postponed but not eliminated, allows clients to get access to basic products with limited functionalities and for low-value transactions. It is very useful in a financial inclusion context since it enables unbanked individuals to get access to the basic formal services they need, and at the same time reduces the costs of small value accounts and increases financial inclusion outreach for FIs. Countries' experiences in dealing with identification and/or identity verification challenges are outlined in Annex 8.

CDD measures - Identification in non-face-to-face scenarios[209]

86. The increasing use of technological innovations is a promising channel to expand the provision of financial services to unserved and remote population[210]. In this regard, mobile phone banking and mobile payments have developed significantly over the last years, and have major potential to facilitate access to basic services for unbanked people, especially in developing countries. According to the World Bank, around three quarters of the world's inhabitants now have access to a mobile phone, and the vast majority of mobile subscriptions (five billion) are in

208 See par. 74.
209 See also FATF (2013b).
210 See G20 Financial Inclusion Experts Group (2010), Annex 3 and FATF (2013b),

developing countries[211]. In Sub-Saharan Africa, the Gallup World Survey poll indicated that 16% of adults reported having used a mobile phone in the prior 12 months to pay bills or send or receive money[212]. Although mobile banking shows potential for financial inclusion purposes, at this stage, it primarily gives access to payment and transfer services. This functionality offers a useful first step to formal financial services but does not in itself provide the benefits of full banking or other financial services.

87. The development of branchless banking channels through non-bank agents (*e.g.,* petrol stations, lottery kiosks, grocery stores etc.), combined or not with mobile phone solutions, also offers significant potential by which financial services can reach the still unbanked or unserved groups. [213]

88. In this context, it is important to understand FATF's requirements involving a non-face-to-face relationship. INR. 10 par. 15 of the new FATF Recommendations identifies non-face-to-face business relationships or transactions as examples of potentially higher risk scenarios. The new Recommendations also clarify that examples are given for guidance only, and that the risk factors listed may not apply in all situations (INR. 10 par. 14). In a financial inclusion perspective, the risks of identity fraud have to be balanced with the ML/FT risks of newly banked people on a case-by-case basis to decide if it is appropriate to apply enhanced due diligence measures.

89. As far as identification of lower risk customers at the account opening stage is concerned, FIs are requested to apply equally effective procedures as for clients with whom they meet. In a number of cases, although there is no direct face-to-face communication with the FI, a third party or an agent is involved in the account opening process. In this case, the principles relevant to agent or third-party relationships will apply[214]. In most other cases, FIs require customers to send digital copies of their identification documentation, and the whole range of the account facilities are activated once the verification is completed. [215]

90. *New products and technologies.* New FATF Recommendation 15 requires that countries and FIs identify and assess the specific risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for existing and new products. In the case of FIs, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies, and they should take appropriate measures to manage and mitigate those risks. The initial, pre-launch risk assessment will be refined and adjusted in light of the experience, as part of the requirement that FIs regularly review and adapt their RBA measures (INR. 1.8.).

91. Recommendation 15 is part of the section of the new Recommendations requiring additional CDD measures for specific customers and activities. This does not mean, however, that the use of new technologies to develop innovative distribution channels or products automatically calls for additional CDD measures in all cases. While an additional, particularized risk assessment of the new products business practices is required, the specific type of business relationships and transactions involved, the client target groups, the involvement of intermediaries, the sophistication of the

211 World Bank (2012c)
212 World Bank (n.d.)
213 See par. 116 and s.
214 See par. 93 for third party relationships and par. 116 and s. for agents.
215 See countries' experiences in Annex 7.

technology used are all factors that must be taken into account in evaluating the risks, and determining the appropriate level of CDD that should be applied. [216]

92. In the new technology/business practices/financial inclusion context, it is worth noting that the FATF Recommendations (INR. 10 par.11) allow FIs in non-face- to-face scenarios to verify the identity of the customer following the establishment of the business relationship (and not before or during the course of establishing a business relationship) when essential to not interrupt the normal conduct of business and provided that the money laundering risks are effectively managed. [217]

93. *Reliance on third parties* - Reliance on CDD undertaken by third parties who are not agents of the FIs and are not covered by outsourcing agreements is permitted under the FATF Recommendations, provided that certain requirements are met (Recommendation 17). Third party CDD is not permitted in some countries, but when allowed, the ultimate responsibility for customer identification and verification must remain with the delegating FI. In a reliance scenario, a FI that is accepting a customer relies on a third party to perform some or all of the following elements of the CDD process (a) identifying the customer (and any beneficial owner), (b) verifying the customer's identity, and (c) gathering information on the purpose and intended nature of the business relationship. This information has to be provided immediately to the FI. FIs must satisfy themselves that the third party is adequately subject to AML/CFT regulation and supervision by a competent authority and has measures in place to comply with the CDD requirements. New Recommendation 17 clearly limits such reliance on third parties to only other FIs (INR 17 par. 3). When they belong to the same financial group, the FI and the third party may be considered as meeting some of the required conditions as a result of their group-wide AML/CFT programme. In practice, firms develop measures to check the reliability of the third party (especially in a cross-border context) such as the degree of domestic AML/CFT regulation and supervision.

CDD measures - obtaining information on the purpose and intended nature of the business relationship

94. The RBA would allow FIs in appropriate circumstances (i.e., with respect to particular types of customers or services/products) to infer the purpose and nature of the business relationship from the type of account established and transactions conducted, instead of collecting specific information and carrying out specific measures intended to satisfy this obligation (INR 10, par. 21 4th bullet point). This means that if an account is obviously opened to enable a poor migrant to send/receive small value transfers to and from his/her country of origin through a safe, affordable and formal channel, this element of the CDD requirements could be considered fulfilled.

CDD measures – enhanced regime if money laundering or terrorist financing is suspected

95. Under INR. 10.21, simplified CDD measures will not be applicable if there is any suspicion of money laundering, or terrorist financing. Neither are they applicable where specific higher-risk scenarios apply. Institutions designing CDD measures for lower risk products should therefore ensure that their institutional measures and systems require employees and agents to implement

216 See countries' experiences in Annex 7.
217 See FATF (2013b).

normal or enhanced CDD measures where such suspicions may be harboured or where higher-risk scenarios are encountered.

CDD measures - conducting ongoing due diligence and monitoring the business relationship

96. Monitoring refers to manual or electronic scanning of transactions. Scanning uses parameters such as the country of origin or destination of the transaction, the value of the transaction and its nature. Client names and beneficiary names are also scanned against national and international sanctions lists. The scanning process may flag a number of transactions for internal investigation, such as transactions with values that exceed the normal value for that type of transaction. Monitoring and internal investigations require capacity and, depending on the method of monitoring, may be time-consuming and expensive. If an outlier transaction is identified, it must be investigated internally. Additional facts must be gathered and considered. The investigator will typically require more information about the client and the transaction before a reasonable conclusion can be drawn that the transaction is above suspicion or that there are reasonable grounds to suspect that the transaction involves ML/FT.

97. The degree and nature of monitoring by a FI will depend on the ML/T risks that the institution faces. In applying an RBA to monitoring, FIs and their regulatory supervisors must recognize that not all transactions, accounts or customers will be monitored in the same way. The degree of monitoring will be based on the identified risks associated with the customer, the products or services being used by the customer and the location of the customer and the transactions. The risks a FI is willing to accept, either with respect to the customers it serves or the services it offers, need to be consistent with the resources of the FI and its ability to monitor and manage its risks effectively. Technology-based service models often offer greater ease of monitoring, and this should be particularly considered by countries in a financial inclusion context.

98. The principal aim of monitoring in a risk-based system is to respond to enterprise-wide issues based on each FI's analysis of its major risks. Regulatory authorities should, therefore, be mindful of and give due weight to the determinations made by FIs, provided that these determinations are consistent with any legislative or regulatory requirements, and informed by a credible risk assessment and the mitigating measures are reasonable and adequately documented.

99. Monitoring under an RBA allows a FI to create monetary or other thresholds below which an activity will receive reduced or limited monitoring. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. FIs should also assess the adequacy of any systems and processes on a periodic basis. The results of the monitoring should always be documented. [218]

100. Some form of monitoring, whether automated or manual, a review of exception reports or a combination of screening criteria, is required in order to detect unusual and hence possibly suspicious transactions. Even in the case of lower risk customers, monitoring is needed to verify that transactions match the initial low risk profile and if not, to trigger a process for appropriately revising the customer's risk rating. Risks for some customers may only become evident once the customer has begun transacting either through an account or otherwise in the relationship with the

218 Wolfsberg (2009)

FI. This makes appropriate and reasonable monitoring of customer transactions an essential component of a properly designed RBA. Moreover, where there is an actual suspicion of money laundering or terrorist financing, this should be regarded as a higher risk scenario, and enhanced due diligence should be applied regardless of any threshold or exemption.

101. It is also important to note that lower risk circumstances can be limited to specific aspects of a given relationship (INR. 10 par.18). In this situation, the simplified regime may not be applied uniformly to all CDD steps, and the extent of the CDD measures can be differentiated, depending on the risk factors identified for each of the relationship's stages. For example, in the case of a newly banked client benefiting from simplified identification measures, normal levels of ongoing transaction monitoring may be applied in order to make sure that the account facilities are used appropriately and within the agreed limits.

102. As noted above, in some countries, the choice has been made to mitigate the risk introduced by simplified CDD by closely monitoring transactions linked to the relevant products and accounts. However, if little CDD is undertaken, so that the FI lacks a sufficient range of available information, manual or electronic scanning of transactions may not be able to deliver significant benefit.

CDD measures – the specific case of Politically Exposed Persons (PEPs)

103. Products and services targeted at financial inclusion are not expected to normally involve PEPs as customers or beneficial owners, although in a number of cases, FIs have to deal with family members of PEPs. Nevertheless, FIs must have appropriate risk-management systems to determine whether a customer or the beneficial owner is a foreign PEP, and reasonable measures to make that determination are required in relation to domestic and international PEPs (Recommendation 12). What constitutes an appropriate risk-management system or reasonable measures to identify foreign PEPs could vary, depending on the risk presented by the customer base.

104. When a foreign PEP is identified as a (potential) customer or beneficial owner, FIs must apply enhanced CDD, including obtaining senior management approval for establishing (or continuing, for existing customers) such business relationships; taking reasonable measures to establish the source of wealth and source of funds; and conducting enhanced ongoing monitoring of the business relationship.

105. In addition, FIs should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization, and to apply the enhanced due diligence measures described above on a risk-sensitive basis *i.e.,* in cases of a higher risk business relationship with such persons. [219]

CDD measures – the specific case of wire transfers

106. Wire transfers are often used for remittances sent for reasons that are linked to financial inclusion issues. In addition to CDD requirements, they are subject to specific rules relating to the customer/originator and beneficiary to ensure full transparency throughout the payment chain

219 See Wolfsberg (2008) and FATF (2013a)

(Recommendation 16). Countries may adopt a *de minimis* threshold (no more than USD/EUR 1 000), below which reduced information requirements can be applied (INR 16).

107. CDD requirements apply to occasional wire transfers in the circumstances covered by INR16 (R10 (ii)). This means that, in countries which have adopted the *de minimis* threshold:

- for occasional cross-border wire transfers below USD/EUR 1 000, the reduced requirements of INR16 apply and the name of the originator and of the beneficiary will be requested, as well as an account number for each or a unique transaction reference number. Such information will not have to be verified (INR. 16 5.a).
- for occasional cross-border wire transfers above USD/EUR 1 000, the information accompanying the transfer should include the elements listed in INR 16.6. : the name of the originator; the originator account number; the originator's address or national identification number of customer identification number or date and place of birth; the name of the beneficiary; and the beneficiary account number. This information needs to be verified.

4.2. RECORD-KEEPING REQUIREMENTS (RECOMMENDATION 11)

108. Under Recommendation 11, FIs should maintain records of all domestic and cross-border transactions (including occasional transactions) for at least five years, to enable them to comply swiftly with information requests from the competent authorities. The rationale is to facilitate the reconstruction of individual transactions and provide, if necessary, evidence for the prosecution of criminal activity.

109. Recommendation 11 also states that FIs should keep all records of the identification data obtained through the customer due diligence process (*e.g.,* copies or records of official identification documents such as passports, identity cards, driver's licenses and similar documents, account files and business correspondence, including the results of any analysis undertaken such as inquiries to establish the background and purpose of complex and unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction. The record keeping requirement is not dependent on risk levels and it is fully applicable to the CDD, transaction and other information collected, whatever the range of this information (INR. 1 6.).

110. Under the FATF Recommendations, the record keeping requirement does not require retention of a photocopy of the identification document(s) presented for verification purposes; it merely requires that the information on that document be stored and kept for five years. A number of countries, such as the United States, Australia and Canada, have considered, but rejected, imposing photocopying obligations on their regulated institutions for a number of reasons: for example, the photocopies could be used to commit identity fraud; their retention may breach privacy laws and they may reveal information about the client that could form the basis of discriminatory practices, such as the refusal of credit facilities. [220]

111. Recommendation 11 therefore allows different forms of document retention, including electronic storage. For example, the following record retention techniques are acceptable:

220 See other countries' experiences in Annex 8.

- Scanning the verification material and maintaining the information electronically;
- Keeping electronic copies of the results of any electronic verification checks;
- Merely recording (hand-writing) reference details on identity or transaction documents. This may be particularly useful in the context of mobile banking, since mobile money agents are often basic corner shops. The types of details it is advisable to record include:
- Reference numbers on documents or letters,
- Relevant dates, such as issue, expiry or writing,
- Details of the issuer or writer,
- All identity details recorded on the document.

4.3. SUSPICIOUS TRANSACTIONS REPORTING (RECOMMENDATION 20)

112. The reporting of suspicious transactions or activity is critical to a country's ability to utilize financial information to combat money laundering, terrorist financing and other financial crimes. All countries should have legal or regulatory requirements that mandate the reporting of suspicious activities. Once a suspicion has been formed, a report must be made and, therefore, an RBA for the reporting of suspicious activity is not applicable.

113. The RBA is, however, appropriate for the purpose of identifying potentially suspicious activity, for example, by directing additional resources at those areas (customers, services, products, locations etc.) that a FI has identified as higher risk. As part of an RBA, it is also likely that a FI will utilize information (typologies, alerts, guidance) provided by competent authorities to inform its approach for identifying suspicious activity. A FI should also periodically assess the adequacy of its system for identifying and reporting suspicious transactions.

114. FATF Recommendation 20 stipulates that if a FI suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing, it should be required to report the incident promptly to the country's Financial Intelligence Unit (FIU). This obligation applies to all FIs that are subject to AML/CFT obligations, including those that serve disadvantaged and low-income people. The implementation of such a requirement requires FIs to put in place appropriate internal monitoring systems to identify any unusual behaviour.

115. In most countries, transactions with vulnerable categories of clients are not deemed to be subject to separate or specific monitoring systems to identify suspicious transactions. However, some businesses may have developed indicators. For example, money transfer businesses[221] would focus on the following, in addition to other criteria, such as systematic monitoring:

- A lack of cooperation at the counter when further questions are asked, or suspicious behaviour is detected.
- An identified transaction pattern that is not consistent with the status of a financially excluded individual: e.g., consumers who are sending or receiving large amounts of money are typically less likely to have limited access to ID documents (from the country

221 Based on the experience of Western Union.

of residency or from the country of origin). This disconnect is a source of potential ML/TF risks.
- Any signal that a consumer is engaged in a TF initiative, whatever the amount of money sent.
- Any signal that a consumer tries to bribe / influence the agent or staff at counter or is producing wrong information and recognizes it.

4.4. THE USE OF AGENTS TO CARRY OUT AML/CFT FUNCTIONS

116. *General.* The use of non-bank agents to distribute financial services is part of an increasingly popular model for financial inclusion in many countries. Most of the countries that contributed to this Guidance paper have developed some forms of agent banking options, some of which are referred to as branchless banking, or banking beyond branches. In these countries, banking and payment services are provided through channels such as post offices, mobile phones and small retail outlets, like airtime sellers, groceries, bakeries, etc., with the goal of providing a broader and cheaper access to financial services than the bank branch-based model. The development of these networks of non-bank agents also offers considerable potential to fill the physical distance gap that appears to be one of the major obstacles to financial inclusion. [222] Brazil has developed such a network so that all 5 564 municipalities in the country now have a banking access point, with 25% of the municipalities served only by such mechanisms. [223]

Definitions and scope

117. *General.* Customer identification and verification obligations are normally predicated on the basis that these functions are carried out by the officers or employees of the FI. However, depending on the jurisdiction, and having regard to the diversity of the financial sectors, there may be occasions when these functions are permitted or are in practice performed by agents. [224]

118. *Notion of agent[225].* Although the business models and the terminology may vary significantly from country to country, it is understood that the agent, in any kind of branchless banking model and most mobile money businesses models, works on behalf of a FI (INR 17.1.).[226] The latter has the business relationship with the customer and is accountable for it. The FI grants authority for another party, the agent, to act on behalf of and under its control to deal with a client/potential client. For instance, in the mobile money business, the agent can be working on behalf of a mobile network operator who has the license to issue e-money. So the customers tend to view the retailer/agent as a point of access and as a representative of the operator. An agreement creating this relationship may be express or implied, and both the agent and the FI may be either an individual or an entity, such as a corporation or partnership.

222 See par. 22.
223 www.ifmr.co.in/blog/2010/07/28/correspondent-banking-in-brazil/
224 See par. 93 for the specific case of the CDD process being undertaken by a third party.
225 The specific case of Money and Value Transfer Services agents covered by Recommendation 14 is dealt with as part of par. 134 and s.
226 This can include other account providers such as mobile network operators or payment services providers, see World Bank (2011).

119. In these branchless banking and mobile money business models, agents are viewed by the FATF as simply an extension of the financial services provider, and consequently, the conduct of CDD by these agents is treated as if conducted by the principal FI. The customers themselves generally view the retailer as a point of access and as a representative of the principal FI.

120. *Who can be an agent?* Many countries permit a wide range of individuals and legal persons or other entities to be agents for FIs. Other countries restrict the list of legally eligible agents. [227] For example, India permits a wide variety of eligible agents, such as certain non-profits, post offices, retired teachers, and most recently, for-profit companies, including mobile network operators. Kenya requires agents to be for-profit actors and disallows non-profit entities. Brazil permits any legal entity to act as an agent, but prevents individuals from doing so. This range of approaches reflects that countries have different regulatory concerns that balance agent eligibility requirements from an AML/CFT perspective with financial inclusion objectives. In some countries the list of eligible agents may be very extensive but under-used by the FIs, in which case, countries may wish to explore the reasons underlying the reluctance to engage agents. [228]

121. The principle that the FI is ultimately liable for compliance with the AML/CFT requirements is required by the FATF Recommendations, and is almost universal amongst jurisdictions, although the extent of liability may differ from one country to another.

122. Finally, countries have adopted different practices regarding licensing or registration of agents and service providers. In Kenya, mobile phone operators are licensed by the communications sector regulator with respect to their provision of traditional communications services, but they operate under the oversight of the Central Bank in relation to the provision of any mobile financial services.

AML/CFT functions of the agent and related challenges

123. The fact that agents act as an extension of the principal FI means that the processes and documentation, for AML/CFT purposes, are those of the principal FI. The main role and duties and how agents have to perform those duties will be determined by the principal FI. In this regard, it is essential that these duties are clearly specified in the agency agreement that sets the terms by which the retailer is appointed as an agent of the principal FI. In practice, the contracts between the principal FI and their agents vary considerably across countries and markets but common clauses generally include the duty to perform specified AML/CFT checks, record-keeping and reporting obligations.

124. In determining the AML/CFT role and duties of the agents, it is crucial that FIs and regulators take into account the potential practical limitations faced by retailers acting as agents (often small shops). Retailers generally have only partial knowledge of the transactions conducted by the

227 See CGAP (2011).

228 CGAP reports that some countries may also restrict the location of agents. For instance, Indian regulators initially required agents to be located within 15 kilometres of a "base branch" of the appointing bank in rural areas, and within 5 kilometres in urban areas. This policy, intended to ensure adequate bank supervision of its agents, limited the use of agents by banks with only a few branches. Consequently, regulators have since expanded the distance to 30 kilometres, and banks can seek exemption from this requirement in areas with underserved populations where a branch would not be viable.

customer (i.e. the transaction conducted in their particular shops). AML/CFT functions of the principal FI and its agents should be seen as complementary and inclusive, keeping in mind that the principal FI bears ultimate responsibility for compliance with all applicable AML/CFT requirements.

125. Although the precise role of a retailer agent may differ from business model to model, it generally involves providing cash-in and cash-out services. It may also extend to other customer interface functions such as account opening and customer care. Most regulations permit agents to process cash-in and cash-out transactions.

126. Many countries permit agents to conduct CDD, and agents routinely verify customer identity. In other countries, agents' ability to conduct CDD measures is limited to certain lower risk financial products. The challenges related to the identification of the customer and verification of the identity (as described in section 4.1) will therefore greatly vary from country to country.

127. As indicated above, the FATF requires FIs to have appropriate systems and controls to monitor transactions, and report to the FIU any transaction or activity that could be suspected to be related to money laundering or terrorism financing. This monitoring requirement may require some adjustments in principal-agent duties although the models developed across FATF jurisdictions seem very similar.

128. Under Mexico's AML/CFT legal framework for instance, FIs are required to establish systems and mechanisms that allow them to receive online all transactions made through an agent, in the same way as those carried out in banking offices. FIs must monitor the operations carried out by the agent and report to the FIU all cases where there is a suspicion of money laundering or terrorism financing. In addition, FIs must have automated systems that allow them to monitor client transactions and detect possible unjustified deviations in the client transactional profile to enable the institution's Communication and Control Committee (consisting of high-ranking employees) to analyse them and if appropriate, report them to the FIU. Similar arrangements exist in Malaysia and South Africa. In the Philippines, both principal and agents are covered institutions and are thus required to adhere to AML/CFT laws and regulations on monitoring and reporting suspicious transactions. Principals and agents submit reports (including suspicious transactions reports) to the FIU, separately and independently from each other.

Internal controls applicable to agents

129. As part of the AML/CFT obligations, FIs are required to develop internal control programmes against money laundering and terrorist financing (Recommendation 18). The type and extent of measures to be taken for each of the requirements under Recommendation 18 should be appropriate in light of the risk of money laundering and terrorist financing and the size of the business.

130. These programmes generally should include: (1) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees; (2) an ongoing employee training programme; (3) an audit function to test the system. Such internal controls are

applicable to agents. They may also be adapted to branchless banking scenarios, in which case agent screening and agent training would be crucial. [229]

Oversight of agents

131. Since agents are viewed by FATF as an extension of-the principal FI[230], it is appropriate for regulatory supervision and oversight to focus primarily on the principal FI. Monitoring and supervising thousands of agents would be extremely challenging for most, if not all, countries[231]. The oversight of agents is mainly performed by the principal FI, in a similar manner as it monitors employees (see Recommendation 18). It is nevertheless also essential that the regulatory supervisor reviews FIs' oversight functions, including by examining the policies, procedures, training and monitoring of agents put in place by the principal FIs.

132. Agent monitoring is a very important element in an effective AML/CFT program. While all FIs should conduct baseline monitoring of agents to assess and address systemic risks such as inadequate training, new or changing services or products, and poor individual judgment or performance, the application of a risk-based approach will require a higher level of monitoring where there are indications that some agents knowingly or through wilful blindness act in a way that may conceal their customers conduct from the institution's routine transaction monitoring. The degree and nature of agent monitoring will depend on factors such as the transaction volume and values handled by the agent, the monitoring method being utilised (manual, automated or some combination), and the type of activity under scrutiny. In applying a risk-based approach to agent monitoring, the degree of monitoring will be based on the identified risks, both external and internal, associated with the agent, such as the products or services provided by the agent, and the agent's location.

133. In some countries, agents can act on behalf of multiple principal FIs. A particular business such as a convenience store can be an agent for more than one FI such as one or more money remitter(s) and one or more retail banks(s), micro lender(s), or micro insurer(s). If the different principal FIs do not exercise the same level of monitoring of the agent (or they are not subjected to the same level of oversight in so far as their agent monitoring is concerned), it could lead to arbitrage between the products and services of the different principal FIs that can be accessed through the agent. It is therefore important that homogeneous requirements apply to the different FIs providing services to low-income clients.

Specific requirements for agents of Money and Transfer Value Service providers[232] (Recommendation 14)

229 See par. 140 and s.

230 Or the principal financial institutions in case the agent works with several of them (in a few markets, agent's exclusivity for a single Mobile Network Operator is not permitted).

231 CGAP (2011a).

232 As defined in the Glossary to the FATF Recommendations, the term "MVTS … refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs."

134. Requirements for money or transfer value providers (MVTS) have obvious implications for financial inclusion. For example, poor migrant workers often rely on MVTS providers to send remittances home. Under Recommendation 14, countries should take measures to ensure that natural or legal persons that provide MVTS are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant ML/CFT obligations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

135. The FATF makes explicit reference to the notion of "agent" in the context of Recommendation 14[233]. In relation to this Recommendation, the Glossary defines an agent as "*any natural or legal person providing money or value transfer service on behalf of an MVTS provider, by contract with or under the direction of the MVTS provider.*" As stated earlier, the FATF views that the agent is an extension of the FI, with the information and documents held by that agent being immediately available to the institution, and the agent being subject to the control of the institution through their contract.

136. Recommendation 14 requires that any natural or legal person working as an agent of an MVTS provider is either licensed or registered by a competent authority, or alternatively, the MVTS provider (the principal) is required to maintain an updated list of agents which must be made accessible to the designated competent authorities in the countries in which the MVTS provider and its agents operate, when requested. It is important to flag that this requirement on agents only exists in the context of money and value transfer services – and not for other types of financial services covered by the FATF Recommendations.

137. Countries have adopted different practices regarding licensing, registration, or listing of agents of MVTS[234]. For example, South Africa, Uganda, and Mongolia require agents to obtain a license. Mexico, Guatemala, and Malaysia require agents to register with a designated competent authority. Where countries require MVTS providers to maintain a list of agents, two approaches have been observed:

1) listing for approval: the MVTS provider must compile a list of agents and obtain approval for them from the designated competent authority. This approach is close to a registration or licensing requirement, and has been adopted by the UK, Jamaica, Nepal, Indonesia, Malawi and Afghanistan.

2) listing for information: the MVTS provider is simply required to maintain a current list of agents and have it available for the designated competent authority when requested. Honduras and the US employ this approach.

138. Recommendation 14 does not require the principal and agent to be in the same jurisdiction. It allows for the possibility that agent in country A could be listed by its principal in country B – provided that authorities in country A and B can obtain the list and the agent follows the AML/CFT requirements applicable to the principal. However, in many countries, if an MVTS agent is operating in a different jurisdiction from where its principal is licensed or registered, the agent is likely to be

233 And indirectly in Recommendation 16 on Wire Transfers.
234 See Todoroki, E., et. al.(forthcoming).

considered an MVTS[235] provider itself in the jurisdiction in which it is operating, and would have to be licensed or registered itself.

139. Finally, INR. 16 par.22 requires MVTS providers to comply with requirements on wire transfers, regardless of whether conducting transactions directly or through their agents.

4.5. INTERNAL CONTROLS

140. The FATF Recommendations require FIs to develop programmes against money laundering and terrorist financing although with some degrees of flexibility considering the ML/TF risk and size of the business (INR. 18). Using this flexibility is crucial, especially for businesses intended to serve the financially excluded or underserved. AML/CFT programmes must include: (i) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees; (ii) an ongoing employee training programme and (iii) an audit function to test the system. FIs must therefore develop an effective internal control structure, including suspicious activity monitoring and reporting and create a culture of compliance, ensuring that staff adheres to the FI's policies, procedures and processes designed to limit and control risks. In addition to complying with the requirements of the country in which they are operating, FIs should also ensure that their foreign branches and subsidiaries comply with the home country AML/CFT requirements. The new Recommendation 18 introduces the requirement that financial groups should have group-wide AML/CFT programmes that include policies on information sharing within the group.

141. The FATF acknowledges that the nature and extent of AML/CFT controls will depend upon a number of factors, including:

- The nature, scale and complexity of a FI's business.
- The diversity of a FI's operations, including geographical diversity.
- The FI's customer, product and activity profile.
- The distribution channels used.
- The volume and size of the transactions.
- The degree of risk associated with each area of the FI's operation.
- The extent to which the FI is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents, or non-face to face access.

142. The FATF considers that the framework of internal controls should include (the list is not exhaustive):

- Providing increased focus on a FI's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals.

235 As defined in the Glossary to the FATF Recommendations, the term "MVTS … refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs."

- Providing for regular review of the risk assessment and management processes, taking into account the environment within which the FI operates and the activity in its marketplace.
- Designate an individual or individuals at management level responsible for managing AML/CFT compliance.
- Provide for an AML/CFT compliance function and review programme.
- Ensuring that adequate controls are in place before new products are offered.
- Implementing risk-based customer due diligence policies, procedures and processes
- Providing for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals.
- Enabling the timely identification of reportable transactions and ensure accurate filing of required reports.
- Incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.
- Providing for appropriate training to be given to all relevant staff.

4.6. OTHER RELEVANT ISSUES

143. Building up an appropriate and balanced AML/CFT regime based on domestic circumstances requires extensive coordination among competent authorities and between public authorities and the private sector. Effective information exchange between the public and private sectors will form an integral part of a country's strategy for combating money laundering and terrorist financing while promoting financial inclusion. To be productive, information exchange between the public and private sector should be accompanied by appropriate exchanges among public authorities. FIUs, financial supervisors and law enforcement agencies should be able to share information and feedback on results and identified vulnerabilities, so that consistent and meaningful inputs can be provided to the private sector.

144. In this regard, the FATF Recommendations promote domestic cooperation mechanisms (Recommendation 2) and encourage public authorities to assist the private sector in adopting adequate and effective AML/CFT measures (Recommendation 34). These principles should guide countries' efforts to implement an effective AML/CFT regime while working towards greater financial inclusion. [236]

145. Lastly, the FATF supports increased cooperation among the private sector, and in particular the building of partnerships between different service providers, aimed at delivering innovative financial products that promote financial inclusion. Mobile-based payment services as well as remittance-linked products that promote the replacement of cash payments by bank accounts, payment accounts or stored-value products constitute examples of innovative products that can effectively promote financial inclusion. The FATF acknowledges the importance of promoting the exchange of experience at an international level, in order to help identify best transferrable practices across FATF countries and beyond.

236 A sample of countries' experiences is provided in Annex 9.

Bibliography

Alliance for Financial Inclusion (2016) *FID Guideline Note: Indicators of the Quality Dimension of Financial Inclusion*, *Alliance for Financial Inclusion*. https://www.afi-global.org/wp-content/uploads/2024/10/Guideline-Note-22-FID-Quality.pdf.

Alliance for Financial Inclusion (2017a) *Financial Inclusion of Forcibly Displaced Persons: Perspectives of Financial Regulator*, *Alliance for Financial Inclusion*. Alliance for Financial Inclusion. https://www.afi-global.org/sites/default/files/publications/2017-07/AFI_displaced%20persons_AW_digital.pdf.

Alliance for Financial Inclusion (2017b) *FIS Working Group Guideline Note: Defining Financial Inclusion*, *Alliance for Financial Inclusion*. https://www.afi-global.org/sites/default/files/publications/2017-07/FIS_GN_28_AW_digital.pdf.

Alper, A. *et al.* (2019) *G20 policy recommendations for advancing financial inclusion and productivity gains through digital public infrastructure*, *World Bank*. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099092023121016458.

Artingstall, D. *et al.* (2016) *Drivers & Impacts of derisking*. https://www.fca.org.uk/publication/research/drivers-impacts-of-derisking.pdf.

Asli, Demirgüç-Kunt et al. (2022) The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19, World Bank. World Bank. https://doi.org/10.1596/978-1-4648-1897-4.

Atkinson, A. and Messy, F. (2015) 'Promoting Financial Inclusion through Financial Education: OECD/INFE Evidence, Policies and Practice,' *OECD Working Papers on Finance, Insurance and Private Pensions*, 34. https://doi.org/10.1787/5k3xz6m88smp-en.

Australian Transaction Reports and Analysis Centre (2021) *AUSTRAC statement 2021: de-banking*. https://www.austrac.gov.au/news-and-media/media-release/austrac-statement-2021-de-banking.

Australian Transaction Reports and Analysis Centre (no date) *Financial services for customers that financial institutions assess to be higher risk*. https://www.austrac.gov.au/news-and-media/media-release/austrac-statement-2021-de-banking.

Basel Committee on Banking Supervision (2015) *Range of practice in the regulation and supervision of institutions relevant to financial inclusion, Basel Committee on Banking Supervision*. Basel Committee on Banking Supervision. https://www.bis.org/bcbs/publ/d310.htm.

Basel Committee on Banking Supervision (2016) *Guidance on the application of the Core Principles for Effective Banking Supervision to the regulation and supervision of institutions relevant to financial inclusion*, *Basel Committee on Banking Supervision*. Basel Committee on Banking Supervision. https://www.bis.org/bcbs/publ/d383.htm.

Better Than Cash Alliance (2024) UN Principles for Responsible Digital Payments, Better Than Cash Alliance. Better Than Cash Alliance. https://responsiblepayments.org/pdfs/UN-ResponsiblePayments.pdf.

Cangiano, M., Gelb, A. and Goodwin-Groen, R. (2019) *Public Financial Management and the Digitalization of Payments*, *Migration and Development Brief*. Washington, D.C., United States of America: Center for Global Development. https://www.cgdev.org/sites/default/files/public-financial-management-and-digitalization-payments.pdf.

Chatain, P.-L. *et al.* (2018) *The decline in access to correspondent banking services in emerging markets: Trends, Impacts, and solutions*, *World Bank*. World Bank.

https://thedocs.worldbank.org/en/doc/786671524166274491-0290022018/original/TheDeclineinAccesstoCorrespondentBanking.pdf.

Clark, J., Metz, A. and Casher, C. (2022) *ID4D Global Dataset 2021: Global ID coverage Estimates*, *World Bank*. World Bank. https://documents1.worldbank.org/curated/en/099705012232226786/pdf/P176341132c1ef0b21adf11abad304425ef.pdf.

Consultative Group to Assist the Poor (2023) Harnessing Inclusive Finance: A path toward thriving and sustainable futures, Consultative Group to Assist the Poor. Consultative Group to Assist the Poor. https://www.cgap.org/sites/default/files/organizational-documents/CGAP%20VII%20Strategy-web.pdf.

Consultative Group to Assist the Poor et al. (2024) G20 Policy Options to Improve Last Mile Access and Quality of Inclusion Through Digital Infrastructure, Including Digital Public Infrastructure (DPI), Consumer Protection, and Other FIAP Objectives, Consultative Group to Assist the Poor. https://www.cgap.org/research/publication/g20-policy-options-for-financial-inclusion-last-mile?auHash=e2SII0Ele54qKWdyixwbRm5WDHdeyLUKcwD-gMaAJeQ.

Cooper, B. *et al.* (2020) *Inclusive Financial Integrity: A Toolkit for Policymakers*. AFI Global Standards Proportionality Working Group; Center for Financial Regulation and Inclusion. https://www.afi-global.org/publication/inclusive-financial-integrity-a-toolkit-for-policymakers/.

De Koker, L. (2009) 'The money laundering risk posed by low-risk financial products in South Africa,' *Journal of Money Laundering Control*, 12(4), pp. 323–339. https://ideas.repec.org/a/eme/jmlcpp/13685200910996038.html.

De Koker, L. (2018) 'ML/FT risk and financial inclusion of the poor: increase the focus on actual usage of formal financial services,' *Journal of Money Laundering Control*, 21(3), pp. 250–252. https://doi.org/10.1108/JMLC-05-2018-0038.

De Koker, L. and Casanovas, P. (2024) ''De-Risking', De-Banking and denials of bank services: an Over-Compliance dilemma?,' in *Ius Gentium: Comparative Perspectives on Law and Justice*. Springer, Cham, pp. 45–70. https://doi.org/10.1007/978-3-031-59547-9_3.

De Koker, L. and Jentzsch, N. (2013) 'Financial Inclusion and Financial Integrity: Aligned Incentives?,' *World Development*, 44, pp. 267–280. http://dx.doi.org/10.1016/j.worlddev.2012.11.002.

De Koker, L., Singh, S. and Capal, J. (2017) 'Closure of Bank Accounts of Remittance Service Providers: Global Challenges and Community Perspectives in Australia,' University of Queensland Law Journal, 36(1), pp. 119–154. https://classic.austlii.edu.au/au/journals/UQLawJl/2017/6.html.

De Koker, L. and Symington, J. (2014) 'Conservative Corporate Compliance: Reflections on a Study of Compliance Responses by South African Banks,' Law in Context, 30, pp. 228–254. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3562092.

D'Hulster, K. *et al.* (2023) *The decline of correspondent banking in Pacific Island countries*, *Pacific Islands Forum*. report. Pacific Islands Forum. https://forumsec.org/sites/default/files/2024-05/CBR%20Report_FINAL.pdf.

Durner, T. and Shetret, L. (2015) *Understanding bank de-risking and its effects on financial inclusion: an exploratory study*, *Global Center on Cooperative Security*. report. Global Center on Cooperative Security. https://oxfamilibrary.openrepository.com/bitstream/handle/10546/582310/rr-bank-de-risking181115-en.pdf?sequence=4&isAllowed=y.

Eckert, S.E., Guinane, K. and Hall, A. (2017) Financial Access for U.S. Nonprofits, Charity & Security Network. Charity & Security Network. https://charityandsecurity.org/system/files/FinancialAccessFullReport_2.21%20(2).pdf.

European Banking Authority (2022) *Opinion of the European Banking Authority on 'de-risking.'* https://www.eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20(EBA-Op-2022-01)/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-risking.pdf.

European Banking Authority (2023) *Guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services*, *European Banking Authority*. Guidelines. European Banking Authority. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2023/1054144/Guidelines%20on%20MLTF%20risk%20management%20and%20access%20to%20financial%20services.pdf.

FATF (2011) *FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*. FATF. https://www.sbs.gob.pe/Portals/5/jer/guiasinf_bp/files/020-AML-CFT%20and%20Financial%20Inclusion%20-%202011.pdf.

FATF (2012a) *FATF's focus on financial inclusion: protecting the integrity of the global financial system*. https://www.fatf-gafi.org/en/publications/Fatfgeneral/Fatfsfocusonfinancialinclusionprotectingtheintegrityoftheglobalfinancialsystem.html.

FATF (2012b) *Ministers renew the mandate of the Financial Action Task Force until 2020*. https://www.fatf-gafi.org/en/documents/documents/ministersrenewthemandateofthefinancialactiontaskforceuntil2020.html.

FATF (2013a) *FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf.coredownload.pdf.

FATF (2013b) *FATF Guidance on National money laundering and terrorist financing risk assessment*, *FATF*. FATF. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Nationalmoneylaunderingandterroristfinancingriskassessment.html.

FATF (2014a) *FATF clarifies risk-based approach: case-by-case, not wholesale de-risking*. https://www.fatf-gafi.org/en/publications/Fatfgeneral/Rba-and-de-risking.html.

FATF (2014b) *FATF Guidance on Risk-Based Approach for the Banking Sector*, *FATF*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Risk-based-approach-banking-sector.html.

FATF (2015a) *Drivers for 'de-risking' go beyond anti-money laundering / terrorist financing*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Derisking-goes-beyond-amlcft.html.

FATF (2015b) *FATF takes action to tackle de-risking*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-action-to-tackle-de-risking.html.

FATF (2016a) *FATF Guidance for a Risk-Based Approach for Money or Value Transfer Services*, *FATF*. FATF. https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html.

FATF (2016b) *FATF Guidance on Correspondent Banking*, *FATF*. FATF. https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/correspondent-banking-services.html.

FATF (2017) *FATF Guidance on Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on CDD*. FATF. https://www.fatf-gafi.org/content/dam/fatf-gafi/images/guidance/Updated-2017-FATF-2013-Guidance.pdf.

FATF (2019a) *FATF Guidance on Terrorist Financing Risk Assessment Guidance*, *FATF*. FATF. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Terrorist-financing-risk-assessment-guidance.html.

FATF (2019b) *FATF Ministers give FATF an open-ended Mandate*. https://www.fatf-gafi.org/en/publications/Fatfgeneral/Fatf-mandate.html.

FATF (2019c) *Public Statement - October 2019*. https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Public-statement-october-2019.html.

FATF (2020a) *COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses*, *FATF*. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/COVID-19-AML-CFT.pdf.

FATF (2020b) *FATF Guidance on Digital Identity*. FATF. https://www.fatf-gafi.org/publications/documents/digital-identity-guidance.html.

FATF (2020c) *Public Statement on Counter Proliferation Financing*. https://www.fatf-gafi.org/en/publications/Financingofproliferation/Statement-proliferation-financing-2020.html.

FATF (2020d) *Statement by the FATF President: COVID-19 and measures to combat illicit financing*. https://www.fatf-gafi.org/en/publications/fatfgeneral/documents/statement-covid-19.html.

FATF (2021a) *FATF Guidance on Risk-Based Supervision*. FATF. https://www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html.

FATF (2021b) *Guidance on Proliferation Financing Risk Assessment and Mitigation*, *FATF*. https://www.fatf-gafi.org/en/publications/financingofproliferation/documents/proliferation-financing-risk-assessment-mitigation.html.

FATF (2021c) *Mitigating the Unintended Consequences of the FATF Standards*. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Unintended-consequences-project.html.

FATF (2022) *Jurisdictions under Increased Monitoring - 21 October 2022*. https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2022.html.

FATF (2023) *Best Practice Paper on Combating the Terrorist Financing Abuse of Non-Profit Organisation*, *FATF*. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html.

FATF (2024a) *FATF Guidance on Money Laundering National Risk Assessment*, *FATF*. FATF. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-National-Risk-Assessment-Guidance.html.

FATF (2024b) *FATF Ministers commit to stepping up efforts to fight money laundering, terrorist and proliferation financing*. https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Ministers-commit-to-step-up-AML-CFT-CPF.html.

Ferwerda, J. and Reuter, P. (2022) National Assessments of Money Laundering Risks: Learning from Eight Advanced Countries' NRAs, World Bank. World Bank. https://documents1.worldbank.org/curated/en/099302204122255265/pdf/IDU02386c9b80f623045e70bf8a09a30b6162595.pdf.

Financial Stability Board (2019) *Remittance service providers' access to banking services: Monitoring of the FSB's Recommendations*, *Financial Stability Board*. Financial Stability Board. https://www.fsb.org/uploads/P290519-2.pdf.

Financial Stability Board (2020) *Enhancing Cross-border Payments - Stage 3 roadmap*. https://www.fsb.org/uploads/P131020-1.pdf.

Frost, J., Gambacorta, L. and Shin, H.S. (2021) 'From Financial Innovation to Inclusion,' *IMF Finance and Development Magazine*. https://www.imf.org/external/pubs/ft/fandd/2021/03/making-financial-innovation-more-inclusive-frost.htm.

G20 and OECD (2022) *G20/OECD High-Level Principles on Financial Consumer Protection*. https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/financial-consumer-protection/G20-OECD-FCP-Principles.pdf.

G20 (2024) *Communiqué: Fourth G20 finance Ministers and Central bank governors meeting*. https://www.g20.utoronto.ca/2024/241024-4th_FMCBG_-_Communique.pdf.

Global Partnership for Financial Inclusion (2010) *G20 Principles for Innovative Financial Inclusion*. https://www.gpfi.org/publications/g20-principles-innovative-financial-inclusion-executive-brief.

Global Partnership for Financial Inclusion (2016a) *G20 High-Level Principles for Digital Financial Inclusion*, *Global Partnership for Financial Inclusion*. Global Partnership for Financial Inclusion. https://www.gpfi.org/sites/gpfi/files/G20%20High%20Level%20Principles%20for%20Digital%20Financial%20Inclusion.pdf.

Global Partnership for Financial Inclusion (2016b) *Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape*, *White Paper*. Consultative Group to Assist the Poor. https://www.gpfi.org/sites/default/files/documents/GPFI_WhitePaper_Mar2016.pdf.

Global Partnership for Financial Inclusion (2023) *G20 2023 Financial Inclusion Action Plan*, *Global Partnership for Financial Inclusion*. https://www.gpfi.org/publications/g20-2023-financial-inclusion-action-plan.

GSMA (2023) *Mobile money activity rates: Exploring barriers to regular use*. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/blog/mobile-money-activity-rates-exploring-barriers-to-regular-use/.

GSMA (2024) *The State of the Industry Report on Mobile Money 2024*, *GSMA*. https://www.gsma.com/sotir/wp-content/uploads/2024/04/GSMA-SOTIR-2024_Report_Executive_Summary_v5-ENG.pdf.

Hernandez, E. and Martinez, C. (2023) *A Technical Guide to Unlock Agent Networks at the Last Mile*, *Consultative Group to Assist the Poor*. technical guide. Consultative Group to Assist the Poor. https://www.cgap.org/sites/default/files/publications/Tech%20Guide_Agent%20Networks_Final.pdf.

IMF (2023) *Financial Access Survey*. https://data.imf.org/en/datasets/IMF.STA:FAS.

Independent Evaluation Group of World Bank (2023) *Financial Inclusion Lessons from World Bank Group Experience, Fiscal Years 2014–22*, *World Bank*. https://ieg.worldbankgroup.org/evaluations/financial-inclusion.

Jenik, I., Kerse, M. and De Koker, L. (2020) *Rapid Account Opening in a Pandemic*. https://www.cgap.org/research/covid-19-briefing/rapid-account-opening-in-pandemic.

Lowery, C. and Ramachandran, V. (2015) *Unintended consequences of Anti–Money laundering policies for poor countries*, *Center for Global Development*. Center for Global Development.

https://www.cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015.pdf.

Lyman, T. et al. (2019) Beyond KYC Utilities: Collaborative Customer Due Diligence for Financial Inclusion, Consultative Group to Assist the Poor. Consultative Group to Assist the Poor. https://documents1.worldbank.org/curated/en/961341625138843266/pdf/Beyond-KYC-Utilities-Collaborative-Customer-Due-Diligence-for-Financial-Inclusion.pdf.

Morawczynski, O., Wallace, L. and May, M. (2022) 'Financial Inclusion-Friendly G2P: Recommendations for Stakeholders,' *Consultative Group to Assist the Poor*, 27 October. https://www.cgap.org/blog/financial-inclusion-friendly-g2p-recommendations-for-stakeholders.

Newnham, R. *et al.* (2018) *Gender Considerations in Balancing Financial Inclusion and AML/CFT*, *Alliance for Financial Inclusion Global Standards Proportionality Working Group Guidance Note*. https://www.afi-global.org/sites/default/files/publications/2018-11/AFI%20GSP_laundering_stg7.pdf.

NYU Paris EU Public Interest Clinic (2021) *Bank De-Risking of Non-Profit Clients: A Business and Human Rights Perspective*, *NYU Paris EU Public Interest Clinic*. https://www.hscollective.org/assets/Uploads/NYU-HSC-Report_FINAL.pdf.

OECD Committee on Financial Markets (2022) *Recommendation of the Council on Financial Literacy*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0461.

Outcomes Statement of the Pacific Banking Forum (2024) *Pacific Banking Forum*. https://treasury.gov.au/sites/default/files/2024-07/p2024-552688_0.pdf.

Operational innovations in AML/CFT compliance processes and financial inclusion: emerging case studies (2014). Consultative Group to Assist the Poor. https://www.cgap.org/sites/default/files/publications/slidedeck/amldeck-150123081748-conversion-gate01.pdf.

Pacific Islands Forum and World Bank (2024) *Pacific Islands Forum & World Bank Event Puts Focus On Corresponding Banking Relationships (CBR) In Pacific*. https://forumsec.org/publications/release-pacific-islands-forum-world-bank-event-puts-focus-corresponding-banking.

Quak, E. (2022) *The Trend Of "De-Risking" In International Finance and Its Impact on Small Island Developing States*, *The Institute of Development Studies and Partner Organisations*. The Institute of Development Studies and Partner Organisations. https://doi.org/10.19088/K4D.2022.079.

Ratha, D. *et al.* (2023) *Leveraging Diaspora Finances for Private Capital Mobilization*, *Migration and Development Brief*. Washington, D.C., United States of America: KNOMAD Trust Fund; World Bank Group. http://documents.worldbank.org/curated/en/099740408142422676.

Reserve Bank of Fiji (2024) National Digital Identification (ID) Program Update - Reserve Bank of Fiji. https://www.rbf.gov.fj/45487-2/.

Select Committee on Australia as a Technology and Financial Centre: Final Report (2021) *Select Committee on Australia as a Technology and Financial Centre*. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/AusTechFinCentre/Final_report.

Sirtaine, S. (2023) 'The Future of Financial Inclusion,' *Consultative Group to Assist the Poor Leadership Essay Series*, 13 September. https://www.cgap.org/blog/future-of-financial-inclusion.

Sivalingam, I. *et al.* (2024) *Scaling Responsible Digital Payments in the Indonesian Cocoa Sector*, *Better Than Cash Alliance*. https://www.betterthancash.org/alliance-reports/scaling-responsible-digital-payments-in-the-indonesian-cocoa-sector.

Sivalingam, I., Budiarso, A., *et al.* (2024) *The Trust Quotient: Unlocking responsible digital payments for micro-merchants*, *Better Than Cash Alliance*. report. Better Than Cash Alliance. https://btca-production-site.s3.amazonaws.com/document_files/752/document_files/241206_BTC_TTQ_PolicyToolkit.pdf?1733482461.

També, N. and Alsancak, F.B. (2024) *Challenges for Counter-Proliferation Finance and Sanctions control in banking*, *Royal United Services Institute for Defence and Security Studies*. Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/challenges-to-pr-sanctions-final_0.pdf.

The U.S. Department of the Treasury (2023) *The Department of the Treasury's de-risking strategy*, *The U.S. Department of the Treasury*. The U.S. Department of the Treasury. https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf.

United Nations (2015) *Transforming Our World: The 2030 Agenda for Sustainable Development*, *United Nations*. https://sdgs.un.org/sites/default/files/publications/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf.

United States Government Accountability Office (2021) Bank Secrecy Act: Views on proposals to improve banking access for entities transferring funds to High-Risk countries, Report to Congressional Committees. report. United States Government Accountability Office. https://www.gao.gov/assets/gao-22-104792.pdf.

Van Broekhoven, L. *et al.* (2023) *The Future of FATF Recommendation 8: A Foresight Piece*, *Human Security Collective*. Human Security Collective. https://fatfplatform.org/assets/Final_R8-Foresight_.pdf.

World Bank (2011) *Global standard-setting bodies and financial inclusion for the poor : toward proportionate standards and guidance*. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/385431468160783371/global-standard-setting-bodies-and-financial-inclusion-for-the-poor-toward-proportionate-standards-and-guidance.

World Bank (2015) *Report on the G20 survey in de-risking activities in the remittance market*, *World Bank*. Washington, D.C., United States of America: World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/679881467993185572/report-on-the-g20-survey-in-de-risking-activities-in-the-remittance-market.

World Bank (2022) *Principles on Identification for Sustainable Development: Toward the Digital Age*, *World Bank Group*. World Bank. http://documents.worldbank.org/curated/en/213581486378184357.

World Bank (2025) *Financial Inclusion*. https://www.worldbank.org/en/topic/financialinclusion/overview#1.

World Bank (no date) *Global ID Coverage, Barriers, and Use by the Numbers: Insights from the ID4D-Findex Survey*, *World Bank*. https://documents1.worldbank.org/curated/en/953621531854471275/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-Insights-from-the-ID4D-Findex-Survey.pdf.