TECHNICAL NOTE

CGAP

RISK-BASED CUSTOMER DUE DILIGENCE

Regulatory Approaches

October 2019

Patrick Meagher

ACKNOWLEDGMENTS

The author thanks the following CGAP colleagues who reviewed the Technical Note and provided invaluable feedback: Greg Chen, Ivo Jenik, Louis de Koker, and Stefan Staschen.

Consultative Group to Assist the Poor
1818 H Street NW, MSN F3K-306
Washington DC 20433
Internet: www.cgap.org
Email: cgap@worldbank.org
Telephone: +1 202 473 9594

CONTENTS

INTRODUCTION

IN THE CONTEXT OF POLICIES ON anti-money laundering and combating the financing of terrorism (AML/CFT), advancing financial inclusion poses special challenges. Regulation must protect the integrity of financial systems and, at the same time, put the least burden on outreach to poor people and the unbanked. Achieving this balance requires a risk-based system of customer due diligence (CDD). Particularly where official identity systems lack universal coverage, imposing strict CDD requirements on the opening and use of accounts may exclude potential customers—whether due to lack of ID or to increased costs (BIS and WBG 2016, p. 30). Allowing simplified procedures in lower-risk settings helps ease entry to the formal financial system for the unbanked, which in turn serves AML/CFT goals.[1]

This Technical Note outlines the main risk-based approaches to CDD, provides examples from regulatory systems across the globe, and weighs the pros and cons of each approach. It begins with a brief discussion of the dynamic context for this analysis. It then discusses three prevailing regulatory options for CDD and its simplification: (i) a principles-based approach, (ii) a single low-risk threshold, and (iii) a framework of multiple risk tiers. Each approach embodies a method of determining what scenarios and financial offerings constitute reduced risk and what processes of simplified due diligence (SDD) might be acceptable for a given level of risk. The last section shines a light on two important cross-cutting issues: (i) the basis for application of the rules (institutions versus activities) and (ii) the conduct of CDD by agents or through electronic channels.

Keep in mind that not only is the surrounding context—both global and national—constantly in flux, but so are the products, services, policies, and regulations discussed in this Note. Information presented here is up to date as of this writing, but this is an area of rapid change. Also, while we address CDD as a whole, our focus on simplification for financial inclusion purposes necessarily emphasizes one component of CDD: customer identification and verification (CIV). This is not to dismiss the importance of the other elements, notably continued transaction monitoring, but simply to focus on aspects most immediately relevant to the inclusion of unbanked and underbanked people.

1 See Staschen and Meagher (2018) and Tomilova and Valenzuela (2018).

CONTEXT: EVOLVING CDD STANDARDS AND IDENTITY SYSTEMS

TWO KEY ELEMENTS OF THE broader AML/CFT context drive the development of risk-based CDD regimes: international standards and identification systems.

FATF guidance

The Financial Action Task Force (FATF) issues the international standards that guide governments and regulators in fighting money laundering and financing of terrorism (ML/FT) (FATF 2012, 2013, 2017). FATF has adopted a risk-based approach to CDD as the most effective way to combat ML/TF. Thus, it provides risk indicators that take financial inclusion into account, allowing for simplified CDD procedures to be used in lower-risk scenarios. Small-value transaction and deposit accounts are often deemed to be low risk (e.g., prepaid low-value products or basic accounts with strict deposit/withdrawal thresholds).[2] In limited cases, at either extreme, certain activities or providers may be exempt from CDD requirements (e.g., where there is "proven low risk"), while higher-risk scenarios—or ones where ML/TF is suspected—require enhanced CDD (FATF 2017, paras. 51–59, 95.) More than 60 countries have financial services regulations that allow CDD exemptions or simplifications (GSMA 2019, p. 13). See Box 1.

Box 1. FATF on CDD

Under FATF Recommendations, CDD has four elements. In accordance with the principle of proportionality, each of the elements may be simplified where the risks are lower (and should be enhanced where risks are higher) (FATF 2012), Rec. 10, INR 10 para. 21):

- **Conducting CIV.** Simplification could, for example, reduce the ID information required or postpone the verification, while allowing initial activities to proceed without it.[a]
- **Identifying the beneficial owner.** Simplification could mean simply asking the question and accepting the customer's response that she/he is opening a low-value deposit account on her/his own behalf, absent indications to the contrary.
- **Obtaining information on the purpose and nature of the intended business relationship.** Simplification could mean inferring this from the type of transaction or the context.
- **Conducting ongoing monitoring and due diligence after account opening.** Simplification means that the degree of monitoring could be reduced based on a reasonable threshold (FATF 2017, paras. 68–102).

a. Subsequent transactions on the account can use the established identity to authenticate the customer. CIV is often termed "Know Your Customer" (KYC). In practice, KYC does not have a standardized definition. See Lyman and de Koker (2018).

2 But low value, by itself, does not always equal lower risk (FATF 2017, para. 69).

FATF states several caveats:

- The category of low-income or nonbanked persons is heterogeneous, and all members of this group are not per se low-risk customers.
- Where risks are lower, some CDD elements may be simplified, but all CDD elements must still be addressed.
- Countries are advised to conduct post-implementation assessments to determine whether low-risk scenarios and simplified CDD measures were appropriately defined (FATF 2017, pp. 6, 18).

While FATF emphasizes CIV in simplifying due diligence for financial inclusion, it also insists on the ongoing monitoring of transactions. The fact that a customer is deemed lower risk at the CIV stage does not necessarily carry over to all stages. Ongoing monitoring may need to remain at the standard level to check that account transactions comport with risk-based thresholds and the customer's risk profile. Indeed, monitoring might need to be tightened to mitigate the inherent risks of the financial products and to compensate for the relaxed initial due diligence checks. Still, FATF calls for risk-based adjustment of this component as well, with the degree of monitoring based on the risks associated with a customer, an account, and products or services used (FATF 2017, pp. 7, 21, 32). Because transaction-monitoring generates substantial costs for financial institutions, simplification is likely to affect the affordability of and access to financial services.

FATF standards accommodate account opening and CDD through agents and through remote (electronic) means. Most digital financial services (DFS) require that customers have access to these methods. In addition, FATF standards consider the use of agents to be equivalent to in-person CDD, while holding the provider accountable for any CDD procedures conducted on its behalf by an agent. The provider in turn must properly analyze the capacity of its agent and supervise the agent's application of CDD (FATF 2017, pp. 32, 67).

On the other hand, FATF considers non-face-to-face scenarios—accounts opened without the customer visiting either the provider or an agent—as potentially posing higher risks. In such cases, it may be impractical to carry out CIV at account opening, and so delayed verification should normally be allowed. Regulators must assess the risks of such non-face-to-face arrangements and may find that the electronic CIV method used either does or does not pose a heightened risk.[3] In the latter case, or where delayed verification is used, a non-face-to-face scenario could be treated as risk neutral—an important consideration for financial inclusion.

Easing CDD constraints with ID upgrades and innovation

Governments are investing in more comprehensive and technologically enabled national identity systems featuring biometrics, uniform ID cards, and digital ID platforms. The effect on CIV can be dramatic. Increasingly, organizations are using national ID databases to conduct electronic KYC (e-KYC) instead of reviewing hardcopy documents to verify identification.

In some countries, mobile phone SIM cards must be registered to identified and verified users. In these cases, the processes already in place may be used to simplify CIV for mobile money accounts. The SIM registration and account-opening processes may be combined or customer data provided for SIM card registration may be accepted as sufficient to open basic mobile money accounts, as is the case in Ghana and Pakistan.[4] Some new systems, such as those in India and Pakistan, cover most of the population and are approaching universal coverage, while more and more services and functions are linked to the digital ID platform (GSMA 2019, pp. 13, 23). These solutions require coordination among policy makers and regulators.[5] Elsewhere, enhanced ID systems have enabled ID requirements for CDD to be tightened (e.g., in Uganda, as discussed in Box 2).

3 See FATF (2012, INR 10, para 15) and FATF (2017, paras 40, 86–93). FATF guidance also facilitates financial inclusion in other ways, e.g., by introducing flexibility into providers' record keeping, agent registration and oversight, and methods of monitoring ongoing business relationships (Noor 2013).

4 This is possible only where the SIM-card CIV and the mobile money CIV requirements are similar. In some cases, the SIM data must be verified against an ID database as part of CDD.

5 Also, as in India, they have prompted legal challenges.

Box 2. Uganda: Mixed impact of improved ID

Uganda's 2013 Mobile Financial Services Guidelines recognized seven types of ID documentation for CDD purposes. However, this in effect was reduced to two types (national ID and foreign passport) by the telecommunications (telcom) regulator's decision in early 2017 to restrict acceptable ID for SIM card registration. The decision followed an ID system reform that increased reliability and availability of the national ID (Staschen and Meagher 2018, p. 26). In Uganda as elsewhere, requirements for obtaining and registering a SIM card are de facto prerequisites for mobile financial services (MFS). Uganda's long-term policy goal is to ensure that MFS customers' duly issued SIM cards are accepted for CIV purposes.

Meanwhile, changes in ID and SIM policies clashed with Uganda's commitment to sheltering refugees. The telcom regulator's decision invalidated the ID component of SIM cards held by those who do not have one of the two accepted forms of documentation. This imposed additional hardship on Uganda's large population of refugees (estimated at 1.4 million), who depend on mobile transfers for humanitarian cash support. United Nation agencies met with Ugandan authorities and eventually persuaded them to accept government-issued refugee IDs as equivalent to national ID cards—and then the agencies worked to get large numbers of refugee SIM cards reregistered (Meagher et al. 2018, pp. 7, 12).[a]

a. Other regulators including the European Banking Authority and the Central Bank of the Philippines have approved the use of SDD for asylum seekers and persons affected by natural disasters, respectively. EBA-Op-2016-07, Opinion of the European Banking Authority on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories, 12 April 2016; FATF (2017, p. 13).

Innovations in ID systems have been reducing frictions in account opening, and new approaches to CDD on the provider side are beginning to have a similar effect. Prominent among these are collaborations among actors in the financial sector to create industry-level solutions or "utilities" that save costs and increase access.[6] Artificial intelligence technology also is helping to decrease the cost of transaction monitoring for CDD purposes.

6 See Lyman et al. (2019).

RISK-BASED CDD FRAMEWORKS: KEY DESIGN OPTIONS

THE CENTRAL QUESTION IN THE design of any risk-based framework for CDD is to what extent key decisions—for example, identifying lower-risk products and services, simplifying CDD procedures—should be within the provider's discretion. Three main options exist, as outlined below. The different approaches are illustrated by frameworks adopted in various countries, ranging from more discretionary to more prescriptive.[7]

Option 1: Principles based

In enabling SDD, regulations sometimes do little more than incorporate the broad language of the FATF Recommendations, leaving it largely to the discretion of financial institutions to determine when and how to apply it (for comparisons, see Table 1 in the Annex). Thus, for example, Bangladesh incorporated FATF provisions in its 2015 guidelines for risk assessment and risk management.[8] Other countries follow this discretionary approach as well, sometimes supplementing it with global caps on transactions and balances (e.g., Kenya and WAEMU).[9] Often, as in Bangladesh and Uganda,[10] the framework focuses mostly on higher-risk scenarios, while a few simple guidelines are given for lower-risk scenarios. This is also true of Pakistan's recently enacted guidelines for electronic money issuers (EMIs) (see Option 3).

A core element of financial services regulation is a set of requirements concerning risk management, including methods for dealing with ML/FT risks. For example, the guidelines applied in Bangladesh call for risk profiling. Seven risk categories are listed, including the nature and scale of the customer's business or job, the mode of opening the account, and the expected number and value of monthly transactions.[11] Institutions are expected to have systems and controls in place to monitor activities on a continuing basis. Financial institutions "should approach socially or financially disadvantaged groups with flexibility." These groups include elderly people, disabled people, students, and minors. Similarly, in Uganda, a risk-management framework is required in any application to the central bank for an agent banking permit, and the AML rules call for regular risk assessments. Such assessments are to be the basis for risk-sensitive CDD.[12]

Central bank regulations define the procedures and documentation requirements for full CDD. In the

7 The term "prescriptive" is used in this paper for convenience, although thresholds and tiers are binding in only one direction. Tiers and thresholds restrict SDD to defined scenarios, allowing simplification within those limits but not mandating it.

8 Bangladesh Financial Intelligence Unit/Bangladesh Bank, *Money Laundering and Terrorist Financing Risk Assessment Guidelines for Banking Sector,* 2015, arts. 3.4–3.6, and *Money Laundering and Terrorist Financing Risk Assessment Guidelines for Financial Institutions,* 2015, arts. 3.4–3.6; Bangladesh Bank, *Managing Core Risks in Banking: Guidance Notes on Prevention of Money Laundering,* chap. V–VI.

9 The West African Economic and Monetary Union, *Instruction N°008-05-2015 régissant les conditions et modalités d'exercice des activités des émetteurs de monnaie électronique dans les Etats membres de l'Union Monétaire Ouest Africaine;* Central Bank of Kenya, E-money Regulation, 2013.

10 Bank of Uganda, *The Anti-Money Laundering Regulations,* 2015, art. 15.

11 There is a general *de minimis threshold* for identification procedures for one-off transactions: US$58.

12 Bank of Uganda, *AML Regulations, 2015, arts. 8, 15, 36; BOU, Agent Banking Regulations, 2017, art.5.*

principles-based approach, simplified CDD processes are largely left to the discretion of the provider (as are risk classification methods). In Bangladesh, the SDD procedures recommended by FATF may be used in lower-risk scenarios, including identity verification after the business relationship, such as an account, is established. A person's identity can be verified from an original or certified copy of a recognized type of document.[13] But in the case of mobile money, the ID requirements for SIM cards become a basic prerequisite for access, even if SDD allows for alternative ID. These standards are set by the telcom regulator and often include a formal national ID, as in Uganda.

WHAT ARE THE REASONS FOR AND AGAINST USING A PRINCIPLES-BASED APPROACH TO CDD?

Pro. The chief difference in approach to CDD is between the principles-based frameworks just discussed and systems that rely on concretely defined thresholds or tiers (see below). The former allow for more contextual fine-tuning by financial institutions. This, coupled with appropriate oversight by the regulator, should enable providers—especially in high-capacity countries—to address ML/TF risks effectively and efficiently. The discretionary model avoids the potential rigidities and costs associated with more prescriptive frameworks, such as the problem of "check the box" compliance. Thus, for example, the European Banking Authority incorporates FATF language on risk-based CDD into the regulations it applies in the European Union. Firms must be able to demonstrate to the regulator that their due diligence is commensurate with the ML/TF risks.[14] This case-by-case approach could be taken a step further, with the regulator authorizing risk thresholds proposed by providers (see the Peru case in the next section).

Con. The weakness of the discretionary approach comes in the tendency of financial services providers (FSPs), especially those in less developed financial sectors, to take an overly conservative, overly compliant approach in order to avoid regulatory scrutiny and sanction. This is sometimes abetted by a lack of regular consultation among the financial institutions, the regulator, and the Financial Intelligence Unit (de Koker and Symington 2011).[15] Relatively weak capacity—in both regulators and providers—likely plays a role in many such settings. A more prescriptive threshold-based or tier-based system, by contrast, would essentially "work with the grain," providing comfort to risk-averse providers and overtaxed regulators by means of unambiguous rules, which are often referred to as "bright-line" rules.

Regulators that afford wide discretion to providers on CDD may not have the capacity to assess and monitor the providers' AML/CFT risk management frameworks. The principles-based approach requires regulators to have a deep knowledge of the sector, a relationship of mutual trust with providers, and sufficient supervisory staff and technical competence (OECD 2001; FSA 2007; Cunningham 2007). Absent these conditions, a principles-based approach is vulnerable to provider malpractice or abuse.

An inherent feature of financial services regulation is ensuring effective risk management. Thus, AML/CFT and CDD regulations normally include at least some broad guidelines here, and the guidelines are often based on the language of the FATF Recommendations. Even where a given regulatory framework is principles based, the provider's exercise of discretion in risk classification and CDD is subject to scrutiny by the supervisor. An explicit rule on simplified CDD would make the standard used by the supervisor clear to all. Otherwise, the basis for supervisory decisions might be considered vague or arbitrary.

13 A certifier must be a suitable person, such as a lawyer, accountant, director, or manager of a regulated institution or notary public. BFIU/BB Banking Sector Guidelines 2015, arts. 3.4–3.6. *Guidance Notes on Prevention of Money Laundering, chap. V–VI.*

14 Directive (EU) 2015/849 of 26 June 2015; EBA, *Final Guidelines on Risk Factors* JC 2017 37 26/06/2017; EBA , *Opinion on the Use of Innovative Solutions by Credit and Financial Institutions in the Customer Due Diligence Process,* JC 2017 81/23 January 2018. EBA also recognizes innovative CDD mechanisms including digital (non-face-to-face) methods and directs national authorities to accept them as valid for CDD purposes if the necessary safeguards are in place.

15 FATF (2017, pp. 23–29).

Option 2: Single lower-risk threshold

Some countries define a single lower-risk threshold for all FSPs, as in Peru, or define thresholds for certain types of providers or services, as in Brazil and India.[16] (See Table 2 in the Annex.) For example, in Brazil, regulations permit simplification of some elements of CDD for "special" or basic banking accounts, subject to quantitative caps (e.g., balance limit of US$750) (FATF 2017, p. 20).[17] Here, CIV can be based on information provided by government programs or on provisional identification using the social insurance number—with a delay of up to six months to complete CIV.

In India, simplified CDD is available for bank accounts under a defined size threshold (e.g., maximum balance of US$780) and for prepaid payment instruments (PPIs) restricted to a semi-closed loop. SDD is not permitted for open-loop PPIs, which are equivalent to electronic money (e-money).[18] Individuals may open small accounts even if they do not have acceptable proof of identity or address. Alternative documentation—"officially valid documents"—may be used.[19] A temporary 12-month bank account can be opened using a self-attested photograph with signature or thumb print certified by a bank official. (The account can be made permanent upon completion of SDD.)

The risk-based approach adopted in Peru is unusual, if not unique (FATF 2017, p. 9). [20] The regulations outline a scheme of simplified CDD that is available in two situations: (i) as provided in regulation or (ii) as proposed by an FSP and approved by the supervisory authority, the Superintendencia de Banca y Seguros (SBS). In either case, providers have the option of offering a basic account using SDD. The regulations define a "basic account," which is deemed low-risk and eligible for simplified CDD, as a banking or e-money account that falls within a monetary threshold (e.g., US$580 consolidated customer balance per institution). Under SDD, only basic information, such as full name, type and number of ID, and address, is collected. Identity verification requires only a valid ID, and this can be presented after account opening. Peru's regulations also require ongoing transaction monitoring on a risk basis by all providers. Thus, providers may simplify (e.g., by reducing the intensity of monitoring) as long as they are effectively able to check customer compliance with account limits, adjust the procedures as needed, and otherwise meet the regulatory requirements just cited.

Where FSPs in Peru wish to get *ex ante* approval of SDD—for example, in scenarios not authorized by regulation—FSPs must apply for the regulator's approval. The application must identify product and service features, the related ML/FT risks, and the system for detecting such risks. SBS has approved SDD regimes for certain nonbank financial services, including some forms of insurance.[21] Other systems afford the regulator a similar role in endorsing provider approaches to SDD, though this is usually framed as the regulator's option to review, reject, revise, or give a tacit no-objection (see the discussion of agent account opening in Uganda at the end of this Note). Peru's approach stands out because it goes beyond the usual implicit, provisional acceptance. It offers explicit authorization, hence legal cover, for the provider to proceed. Importantly, this approval process is in addition to the single threshold set by regulation, thus allowing licensed

16 India sets a threshold for banks and separate requirements for nonbanks.

17 Banco Central do Brasil, *Resolution Nº 3211* of 30 June 2004 and *Resolution Nº 4.480* of 25 April 2016.

18 Semi-closed loop PPIs are electronic accounts useable only within a circuit defined by related organizations. By contrast, open-loop PPIs are in all cases subject to full CDD. FATF (2017, p. 20); Staschen and Meagher (2018); *RBI Master Direction—Know Your Customer (KYC) Direction,* 2016, DBR. AML.BC.No.81/ 14.01.001/2015–16, sec. 3, 16, 22–24; *RBI Master Circular—Policy Guidelines on Issuance and Operation of Pre-paid Payment Instruments in India,* DPSS.CO.PD.PPI. No.01/02.14.006/2016–17, sec. 6–7.

19 This includes a photo ID card issued by a bank or by central regulatory authorities or a letter issued by a gazetted officer with a duly attested photograph of the customer.

20 *Resolución S.B.S. N° 2660-2015, Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo,* arts. 22, 29–31; *Resolución S.B.S. N° 4705 –2017,* arts. 4–5; *Resolución S.B.S. N° 2891-2018, Reglamento de Cuentas Básicas,* arts. 1, 5.

21 Peru's approach to AML/CFT is coming under pressures that may be constraining FSPs' ability to use SDD—notably its 2017 inclusion in the United States' list of major money laundering countries. See http://www.panamatoday.com/international/cuba-ecuador-and-peru-usas-money-laundering-black-list-3707 and https://www.state.gov/documents/organization/268024.pdf.

providers either to operate under the regulatory threshold or to seek approval for an alternative framework. This is a distinctive hybrid of fixed limits and provider discretion.

WHAT ARE THE MERITS AND DRAWBACKS OF CDD SYSTEMS THAT PRESCRIBE A SINGLE LOW-RISK THRESHOLD?

Pro. The use of a low-risk threshold defined in regulation or through case-by-case authorization, as it is in Peru, represents a compromise where a provider can be assured that SDD is legally accepted in defined scenarios. Experience suggests that this assurance makes the use of SDD more likely within the defined threshold. In contrast, without such a threshold or system of tiers, excessively rigid compliance can take over, making it less likely that SDD will be used. Furthermore, beyond a defined threshold, FSPs usually have discretion (*de facto* if not *de jure*) to decide whether full or enhanced CDD applies based on their risk guidelines. Peru's system has a further adaptation that allows providers to propose and seek approval to apply SDD in specified scenarios. This has the advantage of combining the FSP's risk assessment with officially authorized standards.

Con. Creating a single, low-risk threshold constrains both discretionary and rule-based SDD. The sector must work within a framework that may be too rigid for some providers and not detailed enough for others. In defined-threshold systems, the use of simplified CDD beyond the threshold is sometimes prohibited by regulation, or in practice it may be discouraged because discretionary use exposes the FSP to the risk of legal sanction. In this regard, a single threshold is inferior to a system of multiple tiers. The latter may provide legal cover for using SDD in a wider range of situations, with tier-based adjustments.

While a single threshold may simplify implementation by providers and supervisors, it may also make it easier for criminals to find ways to circumvent the rules. Thus, the risk profile of a lower-risk product tends to increase over time, which in turn places a premium on careful monitoring by the supervisor.[22]

Option 3: Multitiered system

Another version of the prescriptive approach translates risk-based CDD into a series of graduated levels or tiers. These tiers accommodate different kinds of transactions, clients, and methods of account opening. Often, there are three tiers or types of accounts:

- **Basic.** Minimal opening requirements and transaction limits.
- **Medium.** Higher ceilings and requirements but less than full CDD.
- **Full CDD.** Higher limits, sometimes including special accounts for businesses (e.g., agents and merchants) with much higher ceilings than individual accounts and more rigorous procedures for account opening.[23]

Although risk-based adjustments mainly focus on CIV procedures, other CDD elements are also affected. In particular, the process of ongoing transaction monitoring is designed to complement CIV by reinforcing it, providing an *ex post* check on compliance, and helping identify any necessary adjustments or enforcement actions.

As shown in Table 3 in the Annex, countries with tiered systems use a range of designs. Three-tiered systems are used, for example, in Ghana, Myanmar, Pakistan, and Tunisia. The quantitative limits on the lowest-level individual accounts range from US$32 for daily transactions and $130 for maximum balance in the case of MFS in Myanmar to US$175 per day and a $1400 maximum balance for branchless banking (BB) in Pakistan.[24] As with single threshold frameworks, multitiered systems are usually intended for a particular segment of institutions or activities.

22 See de Koker (2009, p. 334).

23 Such business accounts are often used by agents and merchants who regularly handle larger amounts of cash and higher transaction volumes than the regular clientele. Costa Rica, Ghana, Myanmar, and Nigeria use this basic structure (Staschen and Meagher 2018). Note that, in addition to the tiers listed here, there is often separate provision for enhanced CDD in higher-risk scenarios.

24 SBP, *Branchless Banking Regulations* (Revised on 12 July 2016), arts. 3–4. In Pakistan and Myanmar, transactions such as utility bill payments do not count toward the quantitative limits.

The tiered CDD framework in Pakistan applies only to BB accounts. These are basic bank accounts that are served through agents and can be used for cash-in/cash-out, bill payment, loan disbursement/repayment, and remittances. Only banks, including commercial banks, Islamic banks, and microfinance banks, may offer such accounts. For Levels 0 and 1, simplified CDD is available, and limited deposits and withdrawals are allowed during account opening. The customer must visit a branch or agent for an initial cash deposit and verification of identity information. [25] CDD requirements are in flux—a recent policy decision requires a biometrically verified SIM card for all levels (this, in effect, invalidates Level 0). The tiered framework does not apply to payments services providers, EMIs, or regular banking. In these instances, providers follow risk-based principles articulated in the AML law and State Bank of Pakistan (SBP) guidelines.[26] As for ongoing monitoring, the BB regulations require providers to have transaction monitoring systems that are able to enforce the ceilings for each relevant tier. Beyond this, the AML/CFT Guidelines allow banks to decrease the frequency of customer ID updates and the degree of ongoing monitoring "based on a reasonable monetary threshold" (identical to the language used by FATF [2017], para. 72).

Some countries see the need for additional tiers. For example, six-tiered frameworks are used in Rwanda[27] (for e-money) and Tanzania[28] (for mobile money). In each case, the two lowest levels serve individuals and are available on the basis of SDD, while higher levels serve businesses and agents of differing scale. The two systems differentiate retail agents from super agents for purposes of CDD. In Tanzania, retail agents require only basic enterprise documents (e.g., business registration and tax ID number), while super agents must be registered corporations and are permitted to distribute e-money and manage retail agents. Treatment also differs based on whether the accounts are registered physically or electronically. Distinct ID requirements apply to cash-out versus cash-in or mobile transactions.[29]

Mexico uses a tiered approach to CDD that includes a four-level system for banking institutions and a three-level system for fintechs, including EMIs.[30] Interestingly, Mexico experimented with anonymous low-level accounts, providing an exemption from CIV requirements within certain limitations including a ceiling of US$225 on deposits per month. Concerns about criminal abuses led to the repeal of this provision in March 2019.[31] The amended regulations allow customer interviews for verification by remote means for Level 3 and Level 4 bank accounts and EMI accounts. Further, Mexico's regulation on identity theft imposes overlapping and inconsistent rules, for example, on customer ID, verification, and authentication methods.[32]

WHAT ARE THE ARGUMENTS FOR AND AGAINST A MULTITIERED SYSTEM OF CDD?

Pro. A tiered system supplies a ready-made risk framework that can provide FSPs some comfort in reaching out to underserved clients. In relatively low-capacity sectors with large unbanked populations, this approach appears to be effective, especially compared to discretionary frameworks. Tiers also help regulators prioritize the allocation of resources.

According to GSMA (2019, pp. 8, 13–15), countries with more proportionate requirements (i.e., simplified or tiered CDD) tend to have higher levels of mobile money growth and digital financial inclusion. GSMA analysis indicates

25 BB ceilings exclude utility bill payments and biometrically verified person-to-person and account-to-person transfers involving nonaccount holders, which have separate limits (*Branchless Banking Regulations,* arts. 3-4; Staschen and Meagher 2018).

26 *Anti-Money Laundering Act 2010;* SBP, *AML/CFT Guidelines on Risk Based Approach for Banks & DFIs,* arts. 7–9. The rules for e-money institutions limit their discretion to decisions about higher-risk scenarios and enhanced CDD. SBP, *Regulations for Electronic Money Institutions (EMIs),* arts. 11, 20.

27 Banque Nationale du Rwanda, *Regulation No 08/2016 of 01/12/2016 governing electronic money issuers,* Appendix I; Bank of Tanzania, *Payment Systems (Electronic Money) Regulations,* 2015, Third Schedule.

28 For card-based e-money in Tanzania, the general rules contained in the AML/CFT legislation (2013) and regulations (2015) apply.

29 Bank of Tanzania, *Electronic Money Regulations,* 2015, Third Schedule.

30 *Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita,* of 17 October 2012, art. 19; S*ecretaría de Hacienda y Crédito Público, Disposiciones de Carácter General* (DCG), [re]...artículo 115 de la Ley de Instituciones de Crédito, as modified by SHCP RESOLUCIÓN 22/03/2019, 24a –25a; *Ley para Regular las Instituciones de Tecnología Financiera,* of 9 March 2018.

31 The original idea was reportedly to bring the many voucher cards used in Mexico into a common framework, with Level 1 accounts therefore limited to a semi-closed-loop function. But the restrictions have been loosened in practice.

32 ID number, full name, fingerprints, population registry, and voter database, unless an alternative is authorized by the banking regulator.

that tiered CDD schemes in particular can contribute to financial inclusion. For example, in the first two years after Mexico introduced its tiered scheme, bank accounts increased by 14 percent, with 77 percent of these new accounts benefitting from SDD. Tiered CDD is likely to have the biggest impact on financial inclusion in countries that do not yet have universal ID coverage.

The key advantage of a multitiered framework over a single threshold is the opportunity it affords to incorporate differentiation and nuance to account for a wide range of needs. This is most obvious if one looks at the lowest and highest levels of the multitiered systems. The base level is a highly circumscribed tier that allows a very low level of activity on the basis of due diligence tailored to the unbanked, in some cases with little or no formal documentation. This design affords the opportunity for a second tier and perhaps a third. These tiers could allow a wider range of activity based on SDD for people of modest means and limited access and those who are able to undergo CDD procedures that are one or two steps up in terms of rigor. Thus, gradations, rather than a single threshold, reduce the risk of excluding people while enabling appropriate safeguards for ML/TF risk.

At the upper end of the tiered CDD scale, there is a further advantage. Differentiation at this level allows for tailored treatment of merchant and agent accounts, such as in Ghana and Tanzania. Agent and merchant accounts have higher ceilings and stricter requirements than individual accounts. For example, opening an account requires an agent or merchant to visit a bank branch, provide documents such as a business registration, and comply with the full CIV (KYC) procedure (as required for regular bank accounts). This agent and merchant tier is useful because it accommodates individuals who handle large volumes of cash and play a critical role in distribution.

Con. Compared with a principles-based framework, a prescriptive system of bright-line rules and tiers increases complexity and rigidity; in some instances, it may also increase costs. The defined threshold or tiers may be incorrectly drawn—that is, they may be at odds with many providers' internal risk guidelines. In low-capacity settings, the potential disadvantage of rigidity may be counterbalanced by the enabling aspect of the rules, such as clear guidance to providers on when and how to use SDD. But this depends on how the framework is configured and on the setting in which it is used. The complexity of some multitiered frameworks, especially where there are overlapping requirements imposed by different regulators and departments, as in Mexico, increases the likelihood of a lack of fit or of undue compliance burdens.

A prescriptive approach substitutes the judgment of the regulator for that of the provider. Policy makers in several instances have found this to be appropriate in light of the context, but it tends to encourage providers' formalistic compliance (i.e., "box-ticking") rather than careful risk assessment. Provider discretion may lead to better targeting. This is where the question of the regulator's involvement comes in. Does the regulator have the capacity to assess and monitor providers' risk frameworks? If the answer is yes, then tiers and thresholds might be unnecessary and, indeed, burdensome.

Innovations in technology can create tension with tiered systems. As ID systems go digital and as SIM registration and e-KYC streamline CDD, multitiered structures—or at least certain tiers, as in Pakistan—may become less relevant. To the extent that technology itself radically simplifies standard CIV across the board, procedural shortcuts become unnecessary. Yet, simplified procedures may continue to have a role in the other CDD steps, and they may be needed for people who are not yet registered in the digital ID system. Thus, decisions on the adoption and design of tiered frameworks must take the dynamism of technology into account. Otherwise, those frameworks risk quickly becoming outmoded or even counterproductive.

ADDITIONAL CROSS-CUTTING DESIGN FEATURES OF CDD FRAMEWORKS

THE BALANCE BETWEEN discretion and prescription is the main but not the only design issue to be addressed in framing CDD regulations. Two other important issues crop up across the different systems: (i) institution-based versus functional regulation and (ii) agent-based and remote CDD.

Institution-based versus functional regulation

Each system must address whether the same set of risk-based CDD provisions applies across all FSPs, or if there should be separate rules for different types of institutions. Some systems treat a particular activity or account the same regardless of the type of institution offering it—a functional approach. Kenya and Peru, for example, apply the same risk-based CDD rules to similar financial services provided by different types of institutions such as banks, nonbanks, and payments services providers (PSPs). In contrast, several other countries apply different sets of rules to different types of institutions, for example, banks and nonbanks, that provide the same or similar financial services such as e-money. Tanzania, for example, has separate CDD provisions for different categories of institutions offering e-money. The rules for nonbanks providing mobile money differ from the rules applied to banks offering card-based e-money. Pakistan also uses this type of institutional approach. Uganda applies separate CDD regulations to banks, nonbanks, and agents, but the rules are broadly consistent.

HOW DOES THE FUNCTIONAL APPROACH TO SIMPLIFIED CDD COMPARE WITH THE INSTITUTIONAL APPROACH?

Pro. A functional approach is as important for CDD as it is for other areas of regulation, such as agent services or consumer protection. The same type of account or activity (with the same risks) should be subject to the same rules regardless of the type of provider or channel. This is necessary to secure a level regulatory playing field and to avoid undue complexity and cost. The functional approach treats the market on its own terms—as an array of DFS offerings that compete for customers regardless of the providers' institutional form.

In contrast, the institutional approach in effect organizes the market to reflect traditional regulatory structures, in which different departments and personnel supervise banks and nonbanks. This results in disparate treatment of customers buying the same product, such as a basic payments account, from different types of providers, such as a bank and an EMI. This approach fails to treat similar risks in like manner, thus tilting the playing field and segmenting the market.

Furthermore, not all differentiation is by design. It sometimes arises from a succession of policies and a lag in addressing anomalies (e.g., DFS-related rules introduced more recently, with emphasis on inclusion, while legacy rules for banks continue to coexist). In such circumstances, the best course is usually to level the playing field rather than allow the disparity to become entrenched.

Con. In many countries, SDD applies to a special type of account that can be provided only by a designated class of entities, for example, MFS in Bangladesh and BB in Pakistan. Thus, CDD differentiated by type of provider is inherent in the broader policy applied to the account. This allows for a more precise targeting of risks than would be permitted by a uniform functional standard. Indeed, such differentiation might have been the providers' preferred choice if they were free to apply the results of their own risk assessments.

Agent-based and remote CDD

A final issue that must be addressed in CDD regulations is whether (and how) customers may be checked and onboarded without being physically present (e.g., visiting a branch of the FSP). FATF recommends that agent-based and remote CDD should be accommodated in the rules, along with delayed verification. This provision is often incorporated in regulations without further elaboration, although many countries specify conditions (FATF 2012, INR 10, para 15; FATF 2017, pp. 32, 67, paras 40, 86–93).

Several countries impose heightened requirements for agents involved in account opening. In WAEMU, for example, any agents handling CDD must themselves be either financial institutions or relevant professionals such as accountants or lawyers. In Uganda, MFS providers using agents to open accounts must ensure that the agents are licensed or registered; have effective, up-to-date AML/CFT policies and systems; and be appropriately trained on AML/CFT and CDD requirements. Financial institutions must set limits on their agents' activities for AML/CFT purposes and report these limits and any changes in them to the central bank, which can order revision if necessary.[33] Bangladesh takes an even harder line; it considers any account opening by an agent on behalf of a bank to be non-face-to-face.[34]

Increasingly, regulations in this area are being adapted in light of technologically enhanced national ID systems. In India, remote CIV through the e-KYC service of the national ID authority (UIDAI) is available if the consumer consents to its use.[35] In Peru, ID verification for basic accounts may be done after the account is opened, whether in person, at an agent, or remotely (electronically). Peru's ID registry facilitates CDD, making available relevant civil, administrative, and financial information to FSPs with permission and for a fee.

Lastly, some countries leverage SIM card registration for CDD. Pakistan pioneered the use of biometric SIM verification for remote opening of mobile money accounts. This is based on the telcom authority's requirement for all SIM cards to be verified against the national ID—which is a unique number linked to adult citizens' basic information and biometrics—held in a central database. Level 1 BB accounts may be opened digitally (e.g., at the point of acquiring a SIM card), with delayed verification allowed (GSMA 2019, p. 20).[36] In Myanmar, SIM registration may be used for opening MFS accounts, with verification against the mobile network provider's database to be completed within 48 hours.

WHAT ARE THE REASONS FOR AND AGAINST REGULATORS' ACCEPTANCE OF AGENT-BASED AND REMOTE CDD?

Pro. The availability of agent-based and remote CDD facilitates outreach, cost containment, and financial inclusion. As noted, FATF guidance considers CDD procedures carried out by an agent and the principal as equivalent, provided that the principal remains responsible and effectively supervises the agent. Further, FATF considers non-face-to-face electronic account opening as potentially posing higher risks, but these can be offset by

33 BOU, *The Financial Institutions (Agent Banking) Regulations, 2017,* art. 16; BOU, *Mobile Money Guidelines 2013,* arts. 7, 11.

34 *Money Laundering & Terrorist Financing Risk Management Guidelines* 2015, art. 6.13. Changes are reportedly on the way, with plans for introduction of remote customer ID and e-KYC.

35 The situation in India has been in flux since the Supreme Court's September 2018 ruling on the unconstitutionality of *Aadhaar* legislation articles dealing with private-sector use. See Lyman et al. (2019). New legislation (July 2019) conforms the law to the constitution and clarifies the lawfulness of private-sector use of e-KYC based on UIDAI data with customer consent.

36 In Pakistan, SIM registration is accepted for CDD purposes but does not substitute for it—the SIM holder's identity must still be checked against the national registry (NADRA).

account restrictions combined with delayed verification and/or secure digitization.

Most countries allow for one or both of these methods. Each jurisdiction must draw limits on the use of such methods, based on contextual factors such as the reliability of remote onboarding methods and agent management capacities. In some systems, such as in Brazil and India, the scope for agent-based or remote CDD is wide, while in others, such as in WAEMU, it is narrowly constrained. In any case, investing effort in this area has a potential double payoff: an increase in financial inclusion and an improvement in the integrity of the system as activities migrate from the informal to the formal financial sector. Moreover, such changes appear increasingly inevitable and, as such, should be embraced sooner rather than later.

Con. The risks of agent-based and remote CDD must be considered. FATF recognizes that they can be safely used only where conditions warrant. Thus, the ability to rely on agents for CDD depends on the relevant entry requirements, risk-management standards, and oversight. This is not strictly part of CDD, but the rigor of agent supervision is a necessary factor in determining whether, in any given scenario, agent-based CDD should be accepted as equivalent to CDD by the principal. Accepting remote account opening and CDD (non-face-to-face) as reliable depends on developments in technology, notably digital national ID systems and electronic onboarding methods. Also, both agent-based and remote CDD in most cases can be done only for basic or lower-risk accounts. In short, while acceptance of agent-based and remote CDD is important for financial inclusion, the scope of permissible use, as with the other techniques discussed, must be tailored in light of contextual risks, capabilities, and technologies.

REFERENCES

BIS (Bank for International Settlements) and World Bank Group (WBG). 2016. "Payment Aspects of Financial Inclusion." Washington, D.C.: BIS and WBG.

Cunningham, Lawrence. 2007. "A Prescription to Retire the Rhetoric of 'Principles-Based Systems' in Corporate Law, Securities Regulation and Accounting." *Vanderbilt Law Review*, Vol. 60, p. 1411.

de Koker, Louis, and John Symington. 2011. "Conservative Compliance Behaviour: Drivers of Conservative Compliance Responses in the South African Financial Services Industry." Capetown: Centre for Financial Regulation and Inclusion. https://cenfri.org/publications/conservative-compliance-behaviour-in-south-africa/

de Koker, Louis. 2009. "The Money Laundering Risk Posed by Low-Risk Financial Products in South Africa," *Journal of Money Laundering Control*, Vol. 12 No. 4, pp. 323-39. https://www.emerald.com/insight/content/doi/10.1108/13685200910996038/full/html

FATF (Financial Action Task Force). 2012. "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, Rec. 1 and 10." Paris: FATF.

———. 2013." Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion." Paris: FATF.

———. 2016. "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations." Paris: FATF. www.fatf-gafi.org/recommendations.htm.

———. 2017. "AML-CFT Measures and Financial Inclusion (with Supplement on Customer Due Diligence." Paris: FATF. www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

FSA (Financial Services Authority). 2007. "Principles-Based Regulation: Focusing on the Outcomes That Matter." London: FSA.

GSMA. 2019. "Overcoming the Know Your Customer Hurdle: Innovative Solutions for the Mobile Money Sector." London: GSMA. https://www.gsma.com/mobilefordevelopment/resources/overcoming-the-know-your-customer-hurdle-innovative-solutions-for-the-mobile-money-sector/

Lyman, Timothy, and Louis de Koker. 2018. "KYC Utilities and Beyond: Solutions for an AML/CFT Paradox?" CGAP blog post, 1 March. https://www.cgap.org/blog/kyc-utilities-and-beyond-solutions-amlcft-paradox_

Lyman, Timothy, Louis de Koker, Chrissy Martin, and Mehmet Kerse. 2019. "Beyond KYC Utilities: Collaborative Customer Due Diligence for Financial Inclusion." Working Paper. Washington, D.C.: CGAP. https://www.cgap.org/research/publication/beyond-kyc-utilities-collaborative-customer-due-dilligence

Meagher, Patrick, Ammar Malik, Edward Mohr, and Yasemin Irvin-Erickson. 2018. "High-Tech Humanitarians: Airtel Uganda's Partnership with DanChurchAid." Washington, D.C.: Urban Institute, October. https://www.urban.org/research/publication/high-tech-humanitarians

Noor, Wameek. 2013. "Anti-Money Laundering Regulation and Financial Inclusion." CGAP blog post, 15 May. http://www.cgap.org/blog/anti-money-laundering-regulation-and-financial-inclusion.

OECD (Organisation for Economic Co-operation and Development). 2002. "OECD Reviews of Regulatory Reform: Regulatory Policies in OECD Countries." Paris: OECD.

Staschen, Stefan, and Patrick Meagher. 2018. "Basic Regulatory Enablers for Digital Financial Services." Focus Note 109. Washington, D.C.: CGAP. https://www.cgap.org/research/publication/basic-regulatory-enablers-digital-financial-services

Tomilova, Olga, and Myra Valenzuela. 2018. "Financial Inclusion + Stability, Integrity, and Protection (I-SIP): Policy Making for an Inclusive Financial System." Washington, D.C.: CGAP. https://www.cgap.org/research/publication/i-sip-toolkit-policy-making-inclusive-financial-system.

ANNEX: TABLES

TABLE 1. **Principles-based approach**

Legal source and coverage	Risk-based approach	CDD/CIV requirements, ID systems	Limits on accounts	Agent-based and remote CDD
Bangladesh				
Source: AML/CFT guidance notes (general) and risk assessment guidelines (separate for banks, FIs). *Coverage:* • Banks, bank subsidiaries, other FIs providing MFS. • Banks may use simplified CDD for MFS, but must apply full CDD to cash agents and in other banking business.	Discretionary. Where risks are lower, simplified CDD measures are allowed. Higher/lower risk profiles are based on: • Type of customer (e.g., public company is low risk) • Products or services • Delivery channels	*Full CDD/CIV:* FSPs to obtain and verify customer's name, parents' names, date of birth, address, details of livelihood and income. ID documents to be presigned with photograph of client. Addresses can be verified by official mailing, voter list, directory, or home/office visit. *SDD:* • Banks may decide to accept alternative ID. • Socially or financially disadvantaged groups to be approached with flexibility. • Reduced ongoing monitoring and updates.	No lower-risk or basic accounts (banking or MFS) defined.	For online (remote) account opening: • Customer identity may be verified (in person) after initial application filed, business relationship established. Account opening at a banking agent is deemed non-face-to-face and subject to full CDD.

Table 1 continues.

Legal source and coverage	Risk-based approach	CDD/CIV requirements, ID systems	Limits on accounts	Agent-based and remote CDD
Kenya				
Source: Regulations and guidelines on AML/CFT, agent banking, payment systems. *Coverage:* Risk-based CDD applies to various financial products and to all FSPs: banks, nonbanks, PSPs.	Discretionary. Regulation allows for a risk-based approach, but no tiers or thresholds.	*Full CDD/CIV:* • All providers must check and record customer ID card, passport, driver's license, or birth certificate. • For a mobile PSP, the SIM card and mobile phone number should be registered. *SDD:* Simplified measures are allowed for lower-risk scenarios.	No lower-risk/ basic accounts defined. Overall e-money limits: per transaction US$680 transactions per month US$9500.	No specific provision.
Uganda				
Source: AML/CFT law, agent banking regulations, mobile money guidelines, directive on SIM card registration. *Coverage:* All FIs.	No CDD tiers set up by laws or regulations. All FIs to do regular risk assessments. General rules provide for risk-based simplified CDD. For banking agents, the principal bank sets the limits for AML/CFT purposes and notifies the central bank.	Many types of ID allowed in principle (financial card, local administration letter, business registration certificate), but SIM registration is a prerequisite—telcom regulator allows only national ID.	No lower-risk/ basic accounts (banking or mobile money) defined.	For agent account opening: MFS providers must ensure that their agents are licensed or registered and that they have effective, up-to-date AML/CFT policies and systems. The principal remains liable for proper completion of CDD. Limits set by providers subject to central bank review.
WAEMU				
Source: WAEMU banking law, AML/CFT directive, e-money and rapid transfers regulations. *Coverage:* All FSPs, but some differences across types.	No CDD tiers in law/ regulation. (Some thresholds defined but highly restrictive.) Discretionary: Where risks are lower, simplified CDD measures are allowed.	*Full CDD/CIV:* • Client's full name, place and date of birth, primary address. Verify by checking "official document" with a photograph and documentation of address. • Merchants must also supply a copy of business registration.	No lower-risk/ basic accounts (banking or e-money) defined. Less strict CDD allowed for no-risk online transfers (restrictively defined). *De minimis* CDD exemption defined for e-money, but not recognized in telcom requirements for SIM cards or in AML/CFT law.	CIV may be done via agents with delayed completion. Agents must be FIs or professionals (e.g., accountants or lawyers).

BB = branchless banking
FI = financial institution
OTC = over the counter

TABLE 2. **Single lower-risk threshold**

Legal source and coverage	Risk-based approach	CDD/CIV requirements, ID systems	Limits on accounts	Agent-based and remote CDD
Brazil				
Source: Central bank regulations. *Coverage:* Deposits and savings accounts.	One SDD threshold.	*Full CDD/CIV:* Full name, names of parents, nationality, date and place of birth, gender, marital status, name of spouse, occupation, type and number of ID, tax number, address, phone number. *Simplified:* Same as full CIV, but information may be obtained from government programs. Completion of CIV may be delayed up to 6 months.	Basic no-frills accounts (*contas especiais*): Balance and monthly deposit limits (both US$750).	Accounts of any level (e.g., basic and regular) can be opened for individuals and entrepreneurs through agents or (remote) electronic channels, with assurance of CIV completion (in person) in case of delay.
India				
Source: AML/CFT rules and guidelines, separate for banks and nonbanks. Payment bank licensing guidelines. *Coverage:* Small-account rules are for all types of banks. Separate rules for nonbank PPI issuers.	One SDD threshold for small-bank account holders. Full CDD required for all open-loop PPIs (e-money), which only banks may issue.	Simplified CIV—alternatives to official ID include: • Letter issued by a gazetted officer with attested photo. • Nonbanks only: introduction from another account holder subject to full CIV, with photo and address. • e-KYC service of UIDAI is valid for CIV if consumer consents. • Self–attested photograph with signature or thumb print certified by a bank official may be used to open temporary (1 year) bank account.	Small bank account threshold: • Balance: US$780 • Credits per year: US$1540 • Aggregate withdrawals per month: US$160	Remote account opening and e-KYC are available. The rules apply to all banks and (with small differences) to nonbank PPI issuers. For agent account opening, banks must ensure agents are licensed/registered and have effective, up-to-date AML/CFT policies and systems. The banks remain liable for proper completion of CDD.

Table 2 continues.

Legal source and coverage	Risk-based approach	CDD/CIV requirements, ID systems	Limits on accounts	Agent-based and remote CDD
Peru				
Source: Central bank AML/CFT regulation, basic account regulation, CDD rules. *Coverage:* All FSPs.	One defined low-risk/ SDD threshold. Or, an FI may determine limits according to its risk-based methodology and get central bank approval. All FSPs to conduct risk classification.	*Full CDD/CIV:* Basic info plus residential address, phone number and/or email address, occupation, and name of employer. *SDD:* Basic info only—full name, type and number of ID, and address; verification by presentation of an ID document. Single national ID for all adult citizens based on Unique ID Registry of Natural Persons.	Low-risk basic account (banking or e-money) limits: • $290 per transaction • $580 balance per customer per provider • $1160 transactions per customer per provider per month	For basic accounts: • ID verification can be done via agent or by remote electronic means. • ID verification may be done after the account is opened.
BB = branchless banking FI = financial institution OTC = over the counter				

TABLE 3. **Multitiered system**

Legal source and coverage	Risk-based approach	CDD/CIV requirements, ID systems	Limits on accounts	Agent-based and remote CDD
Ghana				
Source: AML law, e-money guidelines. *Coverage:* All FSPs covered under AML/CFT rules, but tiered CDD applies only to EMIs.	Tiered CDD for e-money. Levels: Minimum, medium, enhanced. Higher transaction limit for agent and merchant accounts. Lower transaction limit for OTC transactions (no e-money account).	*Full CIV (medium):* Official ID document (list of acceptable forms), name, date of birth, address, phone number. *Minimum CIV:* Any type of photo ID, name, date of birth, address, phone number. *For OTC (no e-money account):* Customer without acceptable ID may be introduced by another person with ID.	Limits for minimum CDD e-money account: • Maximum balance: $190 • Daily transactions: $58 • Aggregate monthly transactions: $570 • One account only	No specific provision.
Myanmar				
Source: FI law, regulations on mobile banking, MFS, CDD. *Coverage:* Tiered CDD applies to nonbanks providing MFS only. Separate regulation for mobile banking (banks).	All providers to conduct regular risk assessments. Tiered CDD for MFS accounts only: • Level 1 (lowest level) and Level 2 for individuals • Level 3 for companies Risk-based CDD allowed, but no tiers, for mobile banking.	*CIV tiers for MFS:* Level 1: National ID, driving permit, or passport to be checked "if and when necessary." Level 2: ID as above, or SIM registration, must be checked. Level 3: Business registration, permanent and mailing address, date of birth, nationality.	Level 1 (lowest) account limits: • $32 for daily transactions • $640 per month • $130 maximum balance Limits apply in aggregate if customer has multiple accounts.	Where SIM registration used for CIV, verification against mobile network operator database to be completed in 48 hours.
Pakistan				
Source: BB regulations, EMI regulations, AML/CFT guidelines. *Coverage:* • BB accounts — Banks only • Separate guidelines for banks (non-BB accounts) and for EMIs.	Tiered CDD for BB accounts (banks) only: • Levels 0 (lowest) and 1 for individuals • Level 2 for individuals and companies Non-BB bank accounts: Risk-based approach, but no tiers. Banks to classify customers as low-medium-high risk. EMIs: Risk-based approach but with no SDD or tiers	*CIV tiers for BB:* Level 0: Formerly based on ID with photo or fingerprint scan, but all accounts now require biometrically verified SIM card. Level 1: Same as Level 0, plus verify phone number (or verify with NADRA if biometrics used). Level 2: Must open account at bank branch with full CDD. Customer profile created before account opening. Levels 0–1: Reduced ongoing monitoring and updates.	Level 0 (lowest): Transaction limits: $175 per day, $280 per month, $1400 per year Maximum balance: $1400. Level 1: Two times Level 0 limits Level 2 (highest): No limits	Levels 0 and 1: Accounts may be opened digitally (remotely), with delayed verification allowed. Limited deposits and withdrawals allowed during account opening.

Table 3 continues.

Legal source and coverage	Risk-based approach	CDD/CIV requirements, ID systems	Limits on accounts	Agent-based and remote CDD
Tanzania				
Source: E-money regulations, AML/CFT law, guidelines for customer ID. *Coverage:* Tiered CDD applies to all mobile money issuers (non-banks only). For card-based e-money (issued by banks), no tiers. General AML/CFT rules apply.	Tiered CDD for mobile money: 1. Electronically registered (individual) 2. Electronically registered with physical documentation (individual) 3. Small and medium enterprises 4. Retail agents 5. Super agents 6. Large businesses	*CIV tiers for mobile money* Tiers 1 and 2: • For cash-in and mobile money transactions: registered phone number and mobile money customer account. • For cash-out: employment ID, social services ID, voter registration, or a letter from the ward/village executive. Tiers 3–6: Full CDD with business documentation.	Tier 1 (lowest) limits: • Transactions: $450 per day • Daily balance: $900	Lowest-level accounts may be registered electronically, including by mobile phone. Ongoing ID requirements depend on types of transactions.
Tunisia				
Source: PSP regulation. *Coverage:* PSPs Separate rules for banking institutions.	Tiered CDD for PSPs including EMIs: Levels 1–3 accounts with graduated ID requirements, transaction and balance limits. Only one account per client. Quantitative account limits do not apply to PSP agent accounts.	*CIV tiers for PSPs* Level 1: Domestic mobile phone number, valid official ID (domestic or foreign) with photo. Level 2: Level 1 info plus create ID record with names, birth date, ID number, address, and company info, if applicable. Level 3: Level 2 info, plus tax ID number and financials for company.	Level 1 account (lowest) limits: • Transactions per day: $80 • Maximum balance: $160 Level 3 account limits: • Transactions per day: $320 • Maximum balance: $1600	Level 1 and 2 accounts may be opened (i) at an agent or (ii) without physical presence of client (remotely, not via agent) where identity documents and data can be transferred by secure digital channel.
BB = branchless banking FI = financial institution OTC = over the counter				


CGAP
cgap.org