COVID-19 BRIEFING

Insights for Inclusive Finance

JULY 2020

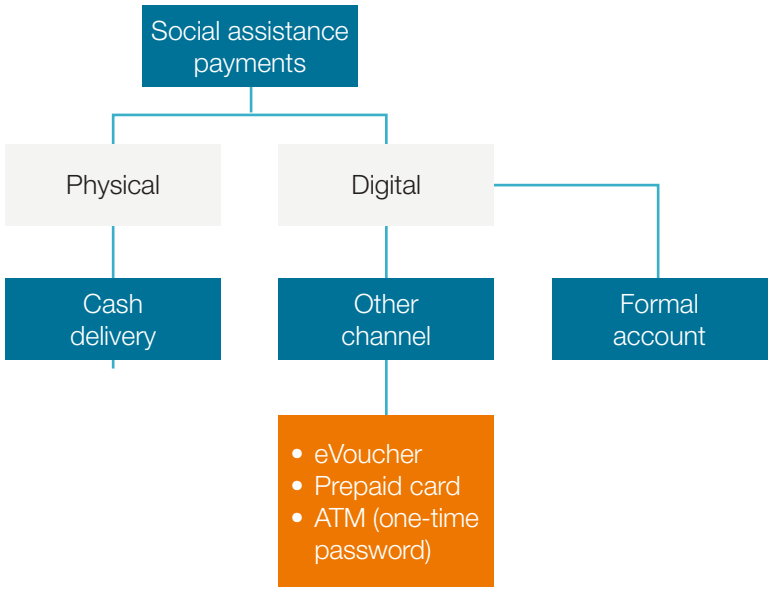
Rapid Account Opening in a Pandemic: How to Meet AML/CFT Rules for Social Assistance Payments

Governments and funders worldwide are responding to the severe economic blow from the COVID-19 pandemic by delivering social assistance payments to families and individuals.[1] Increasingly, they are turning to digital delivery for disbursements, which has accelerated the demand for financial services providers (FSPs) to be able to open formal financial accounts rapidly and with minimal or zero physical contact with customers. This Briefing provides guidance for those designing and deploying social assistance payments to help them work with financial sector regulators and implement social assistance payments that facilitate rapid, remote account opening in compliance with anti-money laundering and counter-financing of terrorism (AML/CFT) rules.

Since the outbreak of the coronavirus pandemic, at least 151 countries have adopted 684 social protection- and labor-related measures. More than half of the measures include social assistance payments (Gentilini, Almenfi, and Dale 2020). Social assistance payments can be disbursed through physical or digital channels (Figure 1). The COVID-19 pandemic has created an urgent need to accelerate digital delivery to minimize the spread of the virus through physical contact. For those who already have accounts with FSPs that are connected to a payments infrastructure, receiving digital government payments can be easy. But there are many people who still must open an account at a participating FSP to receive social assistance. This presents several challenges for governments to structure assistance in ways that achieve rapid disbursal and allow FSPs to process

1 In this Briefing, the term "social assistance payments" refers to financial aid distributed by governments and humanitarian agencies to help individuals and households pay for their basic needs. The payments may be delivered in cash, digitally via direct deposit into a financial account, in the form of a bank card or voucher, or by other means. The term encompasses a range of commonly used phrases, including cash transfers, government-to-person payments, social benefits, welfare, and social protection payments. It excludes in-kind assistance such as food and clothing.

FIGURE 1. **Social assistance payments distribution channels**



account applications quickly and at a physical distance. Barriers to digital delivery can be particularly high for women who may lack documentation, have limited literacy or digital skills, or limited ability to travel. Yet, women frequently are the primary recipients of social assistance payments intended to support the health and welfare of their families.

Rapid and remote opening of financial accounts is feasible, but it requires governments and FSPs to navigate the sometimes-confusing web of AML/CFT rules and standards. This Briefing explains how social assistance payments managers in various government agencies—including social protection, health, education, and welfare—as well as nongovernmental actors can meet the AML/CFT requirements for customer due diligence (CDD) at both the national and the global level.

Importantly, under AML/CFT rules, social assistance payments often can be considered a lower risk for money laundering and terrorist financing than other forms of account opening. Therefore, such accounts often qualify for a **simplified CDD or even complete exemption.** Social assistance payments with the following characteristics often have lower risk profiles:

- **Known sender.** Payments come from government (and/or a trusted international donor).
- **Legitimate funds**. Money laundering involves proceeds of crime, whereas social assistance payments are legal at origin. They may involve proceeds of crime only where, for example, the recipient obtained it through fraud—something social assistance managers actively seek to limit.
- **Targeted recipient**. Recipients often are targeted and have been preidentified by government programs. This identification can be sufficient for AML/CFT purposes.

- **Small amounts.** As the programs are focused on poor people, payment amounts often are small and are therefore recognized for being proportionately at lower risk for money laundering.
- **Simple and known use**. Most people who receive social assistance payments simply cash out their funds and do not use their accounts for illicit transactions. Where other kinds of transactions are made, the accounts usually are tracked as a part of social assistance payments monitoring.
- **Program monitoring**. While FSPs monitor the accounts of recipients as part of their AML/CFT obligations, program managers also monitor the use patterns of accounts to ensure that program objectives are being achieved. This adds a further layer of oversight compared to that of other types of commercial accounts.

Where some or all of these characteristics are present, social assistance managers can take several steps to facilitate compliant, rapid, and remote account opening. However, they may not have the power to adopt all the measures and may need to engage with the AML/CFT regulator. To help in this regard, this Briefing explains the constraints that regulators face and how they can be overcome, bearing in mind that the application of rapid, remote account opening always will be context specific.

This Briefing offers many country examples, and readers should always consult the original text of the referenced regulation. Measures implemented in one country or by one provider should not be automatically implemented by another country or provider without first appropriately analyzing the applicable law, conducting appropriate risk assessments, and creating a risk mitigation plan. These elements are vital to a risk-based approach to AML/CFT. Keep in mind that this Briefing offers guidance that should not be construed as legal advice.

Responding to the COVID-19 pandemic

There are two ways governments can facilitate remote account opening to allow more beneficiaries to receive their money safely and conveniently. First, design and implement social assistance payments in a way that makes compliance with AML/CFT requirements easier. Second, engage with the AML/CFT regulator if required and with industry to modify the requirements, either temporarily or permanently.

COMPLIANCE-FRIENDLY SOCIAL ASSISTANCE PAYMENTS

Here are some tips on how to design and implement social assistance payments to make compliance with AML/CFT requirements easier:

1. **Share information about the beneficiaries with FSPs.** When opening an account, the FSP must establish who the customer is by collecting key personal data, such as full name, date of birth, and address, and by verifying the data against a reliable, independent source, such as an official ID document or database. Managers running social assistance programs often already have most of the data verified to their satisfaction. They should share the relevant, verified data with FSPs so that FSPs do

not duplicate that work for CDD purposes. If privacy and data protection concerns prevent sharing the data, social assistance managers can enable FSPs to securely verify customer data of recipients against their own databases.

2. **Profile beneficiaries of social assistance payments.** Social assistance managers often know beneficiaries well; they often have information that includes beneficiary names, addresses, ages, income levels, sources of income, and marital status. These data can be used to determine the risk profile of beneficiaries for AML/CFT purposes. As part of their CDD obligations, FSPs must determine the money laundering and terrorist financing risk profile of each customer. By sharing their information with FSPs, social assistance managers make the FSPs' task easier. The managers also can coordinate with the AML/CFT regulator and categorize beneficiaries into standardized risk profiles approved by the regulator, obviating the need for FSPs to conduct their own assessment.
3. **Minimize the risk of terrorist financing.** From a money laundering perspective, social assistance payments pose a very low risk because the money comes from the government or a trusted donor. But there is a remote possibility that a beneficiary will use the social assistance payments to finance terrorism. While the risk may be low, there are ways to mitigate it. The first is to check beneficiary lists against terrorist lists, such as the United Nations Security Council sanctions list. Second, social assistance managers monitor customer transactions, especially whether they take cash out, which is the most common transaction. Third, when accounts are used for purchases or other electronic transactions, these can be followed closely if needed.

When implementing any of these measures, privacy of the beneficiaries always must be a priority. Regardless of whether a legal framework for privacy and data protection is in place, social assistance managers and FSPs should collect and use only the data required for social assistance and AML/CFT purposes, treat individuals' data as sensitive, and ensure that data are used with beneficiaries' consent and to their benefit. Data theft or leakage may undermine the integrity of the assistance and of CDD controls.

There is a good chance that, with smart design, a social assistance manager can convince the AML/CFT regulator to apply **a proven low risk exemption** (see Annex). Such an exemption would allow FSPs to open clearly defined types of accounts without applying all the elements of standard CDD in instances where the accounts pose a low risk of money laundering and terrorist financing. For instance, until recently, banks in Mexico were allowed to open anonymous Level 1 accounts, providing exemption from customer identification and verification requirements within certain limitations, including a ceiling of US$196 in deposits per month.

COORDINATION WITH AML/CFT REGULATOR

The AML/CFT regulator needs to understand the task of social assistance managers. The objective of social assistance managers is to get money to those in need quickly and safely while overcoming the challenges of beneficiaries not having and/or struggling to open accounts. But AML/CFT regulators operate within limits. At the international level, these limits are determined by Financial Action Task Force (FATF) Recommendations, the international AML/CFT standards that all countries must meet.[2] At the national level, they often are informed by **the national risk assessment** that defines the level of money laundering and terrorist financing risk each country faces.

Social assistance managers should ask the AML/CFT regulator about the risk assessment. If it is still under development or it is outdated, the manager should suggest running a more limited and urgent exercise focused on the social assistance payments that are being considered. This exercise should involve the social assistance managers; the AML/CFT regulator; and other financial sector regulators, law enforcement agencies, and FSP representatives. With such a risk assessment, social assistance managers can push for appropriate responses, including (i) tier-based, simplified CDD; (ii) authorization of digital identification; and (iii) assistance to FSPs.

TIER-BASED SIMPLIFIED CDD

Simplified CDD may take different forms and shapes in different countries, reflecting the identified risks and available infrastructure (see Box 1). For FSPs, implementing a simplified CDD regime is a complex process that takes time. To make it easier and quicker, social assistance managers should convince the AML/CFT regulator to adopt a tier-based CDD model that spells out the tiers and control measures for FSPs (see Table 1; for explanation of the concept see Annex). Why does it help? Because it largely lifts the burden of individual risk assessment and risk control design from FSPs.

2 FATF has recently issued a statement on COVID-19 urging countries to use digital identification, fintech, regtech, and suptech to the fullest extent possible to facilitate implementation of AML/CFT requirements (see FATF 2020c). The statement was later complemented with FATF (2020a).

BOX 1. **Simplified CDD in response to COVID-19**

Ukraine. In response to the COVID-19 pandemic, the National Bank of Ukraine has waived the requirement of physical presence to open bank accounts. The new AML/CFT law, enforced as of 28 April 2020, allows banks to conduct identification and verification remotely. The following verification procedures can be used by the banks:

- "Full-fledged" verification and identification not subject to limits, such as using bank identification and qualified e-signature and using video identification.
- "Simplified" verification and identification, such as using bank identification, using qualified e-signatures, making payment from the account opened in a client's name, reading of the electronic chip on a biometric passport/ID card using a mobile phone near-field communication module, verification of data via credit bureau, and confirmation of mobile phone number via one-time password.

The following limits apply for simplified procedures: total payments shall not exceed US$1,470 per month, US$14,700 per year, and a maximum balance of US$1,470. Limits are calculated per all accounts opened in a specific bank.

The Philippines. On 1 April 2020, the Central Bank of the Philippines eased the requirement for the presentation of a valid ID document for customer onboarding and transactions during the period of enhanced community quarantine and until 30 June 2020. The measure has been adopted with the objective to facilitate the delivery of welfare funds to identified beneficiaries who have no valid ID documentation or transactional account with any FSP. The central bank relaxed the CDD requirements because the accounts involved are considered low risk. The relaxed CDD requirements apply to both over-the-counter transactions and electronic or online transactions. The central bank introduced control measures to guard against money laundering and terrorism financing risks: (i) the transactions in the account shall not exceed US$985 per day, (ii) qualified customers are those who reside or conduct business in the area that has been declared to be under enhanced community quarantine or community quarantine, (iii) customers are required to certify that they have no valid identification, and (iv) customer account activities shall be subject to ongoing monitoring. FSPs are expected to obtain the required minimum information from the customer and perform risk-based CDD measures.

Ghana. All mobile phone subscribers have been permitted to use their mobile phone registration details to be onboarded for minimum know-your-customer accounts.[a]

WAEMU. E-money issuers in WAEMU have been authorized to activate mobile money accounts on the basis of data from mobile network operators, subject to collecting by any means the agreement of the customer and to performing the due diligence related to the remote identification, within the limits of regulatory ceilings, for a period of three months. After three months, the customer will have to be identified according to the regulatory requirements.[b]

a "AFI COVID-19 Policy Response," AFI, https://www.afi-global.org/afi-covid-19-policy-response.
b BCEAO's 1 April 2020 Communique, Section 7, https://www.bceao.int/fr/communique-presse/communique-relatif-aux-mesures-de-promotion-des-paiements-electroniques-dans-le.

TABLE 1. **Examples from countries with tiered CDD requirements**

	CDD requirements	Limits
Pakistan[a]	Tiered CDD for branchless banking: Level 0 and Level 1 for individuals; Level 2 for individuals and companies. • Level 0: Formerly based on identification 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. • Levels 0 and 1: Accounts may be opened digitally (remotely), with delayed verification allowed. Limited deposits and withdrawals allowed during account opening.	Transaction limits • Level 0 (lowest): US$156 per day, US$250 per month, US$1,251 per year; maximum balance: US$1,251 • Level 1: US$313 per day, US$500 per month, US$5,003 per year; maximum balance: US$2,502 • Level 2 (highest): No limits
Tunisia[b]	Tiered CDD for payment services providers (PSP), including e-money issuers. • Level 1: Domestic mobile phone number, valid official identification (domestic or foreign) with photo. • Level 2: Level 1 information 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 and 2 accounts may be opened (i) at an agent or (ii) without physical presence of client (remotely, not via agent) where ID documents and data can be transferred by secure digital channel. • Only one account per client. • Quantitative account limits do not apply to PSP agent accounts.	• Level 1 account (lowest) limits: Transactions per day: US$80; maximum balance: US$160 • Level 3 account limits: Transactions per day: US$320; maximum balance: US$1,600
Mexico	Tiered approach for banks • Level 1: Before March 2019, it was an anonymous account. After that date, banks must collect full name and date of birth, but no verification is required. • Level 2: Basic customer information to be collected (full name, date of birth, address). The requirement of in-person interview with the customer is lifted if his/her data are verified online. Address verification is not required. In this case, additional data (i.e., gender and place of birth) are required. • Level 3: Level 2 information plus additional information such as nationality, occupation, phone number, email (no hard copies required). • Level 4: Full CDD. • Level 1 and Level 2 accounts only for individuals. • Remote account opening is allowed for all levels. Level 3 and Level 4 customers can make remote interviews for account opening.	• Level 1: Maximum deposits per month: US$196; maximum balance: US$261 • Level 2: Maximum deposits per month: US$783; in the case of government support funds, the previous limit is US$1,567 • Level 3: Monthly transactions: US$2,613 • Level 4: No limit. If remote interview used for account opening, maximum deposits per month: US$7,833

a. State Bank of Pakistan, 2016; Meagher, 2019.
b. Meagher, 2019.

AUTHORIZATION OF DIGITAL IDENTIFICATION FOR SIMPLIFIED CDD

Remote account opening is easier when there is a digital ID system. If there is a digital ID system, convince the AML/CFT regulator to authorize FSPs to use it for simplified CDD purposes.[3]

BOX 2. **Examples of authorized digital ID systems**

Singapore's MyInfo platform. The Singaporean government is developing a digital ID service stack for residents and businesses. MyInfo is the trusted ID data service of the National Digital Identity program. It includes government-verified data from various government agencies and contains more than 100 personal data items. It provides citizens and residents access to and control over the sharing of their data. Users are able to autofill their government-verified personal information on public and private sector e-services via a reliable and independent channel upon the individual's consent.

As of March 2020, more than 60 FSPs in Singapore leveraged MyInfo for over 220 digital services to onboard and perform CDD on customers. Consent of customers is sought before any personal data on MyInfo profiles are retrieved by FSPs. The Monetary Authority of Singapore (MAS) has issued guidance called "Use of MyInfo and CDD Measures for Non Face-to-Face Business Relations" (AMLD 01/2018). Where MyInfo is used, FSPs will not be required to obtain physical documents to verify a customer's identity and also will not be expected to separately obtain a photograph of the customer. MAS has clarified that it considers MyInfo to be a **"reliable and independent source"** for the purposes of verifying the customer's name, unique ID number, date of birth, nationality, and residential address. FSPs are required to maintain proper data records, including data obtained from MyInfo, in accordance with regulatory requirements in Singapore.

Pakistan's biometric-based digital ID system. Pakistan's biometric-based national digital ID system developed and managed by the National Database and Registration Authority (NADRA) has been used for more than 10 years to support account opening by poor people. According to NADRA, Pakistan's Computerized National Identity Card (CNIC)—a smart card that stores demographic and biometric data of a citizen and has a unique 13-digit ID number—covers nearly 100 percent of the adult population.[a] CNIC can be issued to citizens of Pakistan who are 18 years of age or older. NADRA data are used for ID verification of individuals relating to both bank account opening and mandatory mobile SIM card registration. NADRA provides an online verification system where, for a fee, FSPs can verify the identity of a customer. Where a user holds a SIM card that is already verified, an FSP may remotely open a basic account for that person (SBP 2016).[b]

a. Other estimates put the coverage at 79 percent (Global Findex Database, World Bank, 2017, https://globalfindex.worldbank.org/).
b. For details of Pakistan's tiered approach to CDD, see Table 1.

Source: FATF Guidance on Digital Identity, 2020, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html, and Lyman, de Koker, Martin Meier, and Kerse (2019).

3 For more information on the use of digital IDs for AML/CFT purposes, see Annex.

ASSISTANCE TO FSPS

AML/CFT measures are implemented by each FSP individually. FSPs tend to be risk averse to avoid fines (de Koker and Symington 2011). The AML/CFT regulator can ease FSP concerns that they will violate standards by:

- Providing appropriate information and guidance on how they can benefit from the simplified CDD framework in the country.
- Issuing no-objection letters relating to contactless onboarding models.
- Providing access to government data that may inform FSP risk management, including ID verification as well as fraud and other crime data and information.
- Facilitating industry collaboration on simplified CDD (Lyman, de Koker, Martin Meier, and Kerse 2019)—for example, help FSPs and mobile network operators enable FSPs to improve customer data quality where this may be facilitated by data collected during SIM card registration processes, clarify respective roles and responsibilities, promote collaboration to improve customer data where required, and joint investigation of suspected identity fraud.
- Supporting a noncompetitive, simplified CDD compliance and risk management discussion among participating FSPs to share information, experiences, and emerging practices.

Long-term view on emergency measures

While many are focusing on facilitating social assistance payments for pandemic-related relief programs in the short term, it is important to consider long-term implications, including the following:

- Will FSPs have customers who were subject to the COVID-19 simplified CDD measures and other customers, with similar profiles, who were not? If so, how will they distinguish between the two groups?
- If the simplified measures are only temporary, how will customers be identified in the future to regularize their CDD requirements (e.g., by submitting ID verification data or documents)? What will FSPs do when customers are not able to verify their identities? Will their accounts be frozen? If so, will they lose access to monies in those accounts?
- How will FSPs spot identity fraud?

Identity fraud can be addressed through strengthened customer profiling—by collecting data on where a customer lives; how they normally earn a living; whether they operate a business and what type of business it is (Isern and de Koker 2009); their estimated weekly expenses pre- and post-COVID-19; and whether they regularly receive and send remittances, and from/to whom. These data will help FSPs spot fabricated and synthetic identities as well as fraud related to money laundering and terrorist financing. Profiling must be subject to adequate privacy and data protection rules. If FSPs have limited information on customers and their identities, their monitoring is less effective.

BOX 3. **Examples of regulatory assistance to FSPs**

Australia. Australia's AML/CFT regulator, AUSTRAC, issued guidance on 1 April 2020 on how FSPs could comply with customer identification and verification requirements during the COVID-19 pandemic.[a] AUSTRAC also amended its AML/CTF rules temporarily to provide further flexibility in cases where COVID-19 measures made it impossible to follow standard ID proofing processes. The guidance leverages AUSTRAC guidance on identifying customers who do not have conventional forms of identification, most recently amended on 28 May 2020. AUSTRAC's guidance provides practical examples of how FSPs might apply a flexible, risk-based ID proofing process by:

- Using alternative proof-of-ID processes (including video calls and selfies).
- Using electronic copies (scans or photographs) of reliable and independent documentation, in accordance with their AML/CFT program, to verify the identity of individual customers or companies.
- Relying on disclosure certificates to verify certain types of information about customers who are not individuals, where measures put in place by industry as part of its response to the COVID-19 pandemic mean that such information is not otherwise reasonably available from other sources.

New Zealand. The Reserve Bank of New Zealand, Financial Markets Authority and Department of Internal Affairs, published guidance for FSPs on conducting CDD during COVID-19 (FMA 2020). The guidance also reminds FSPs that they can apply a risk-based approach in line with the AML/CFT Act. The guidance includes the following:

- A new business relationship with a customer could be established if verification is completed as soon as practicable after COVID-19 alert levels have been lifted. FSPs need to consider how to effectively manage risks associated with money laundering and financing of terrorism during this time.
- FSPs that are continuing to operate and establish new business relationships would implement transaction limitations—limited transfers or withdrawals—until verification requirements were completed.
- For current customers, FSPs have the discretion to not necessarily view certain documents in certain circumstances, depending on the FSP's risk assessment. FSPs can accept scanned copies of documents as an interim measure, with the originals to be viewed at a reasonable later time (i.e., upon lifting of alert levels).

Hong Kong. In a recent guidance, the Hong Kong Monetary Authority (HKMA) states that where FSPs identify lower money laundering and terrorist financing risks, AML/CFT regulations allow adoption of simplified CDD measures.[b] Also, FSPs are encouraged to continue to work closely with HKMA to provide greater convenience for account opening and continued access, physically and digitally, to essential banking services to the public during the pandemic. HKMA also supports public–private partnership in the sharing of information and typologies to help prioritize and address key money laundering and terrorist financing risks, particularly those related to fraud linked to COVID-19. In addition, HKMA emphasizes that it is using its supervisory tools flexibly during this period and reiterates that its risk-based approach to AML/CFT supervision does not require or expect a "zero-failure" outcome.

United Kingdom. The United Kingdom's Financial Conduct Authority issued a guidance on 31 March 2020 for firms providing services to retail investors for customer verification.[c] The guidance emphasizes that AML/CFT regulations already provide for customer ID verification to be carried out remotely and give

Continued on the next page.

BOX 3. **Examples of regulatory assistance to FSPs** *(continued)*

indications of appropriate safeguards and additional checks firms can use to assist with verification. It states that such firms can, for example:

- Accept scanned documentation sent by e-mail, preferably as a PDF.
- Ask customers to submit selfies or videos.
- Use commercial providers who triangulate data sources to verify documentation provided.
- Gather and analyze additional data to triangulate the evidence provided by the customer, such as geolocation, IP addresses, and verifiable phone numbers.
- Verify phone numbers, e-mails, and/or physical addresses by sending codes to the customer's address to validate access to accounts.
- Seek additional verification once restrictions on movement are lifted for the relevant customer group.

a. "How to Comply with KYC Requirements during the COVID-19 Pandemic," AUSTRAC, https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/kyc-requirements-covid-19.

b. "Coronavirus Disease (COVID-19) and Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Measures," letter by Carmen Chu, executive director (Enforcement and AML), Hong Kong Monetary Authority, 7 April 2020, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200407e1.pdf.

c. "Dear CEO Letter to firms providing services to retail investors about coronavirus (Covid-19)," letter by Christopher Woolard, interim chief executive, Financial Conduct Authority, 31 March 2020, https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-coronavirus-update-firms-providing-services-retail-investors.pdf.

There also are broader concerns that go beyond the scope of AML/CFT rules. Opening and funding accounts is pointless unless recipients can withdraw money or use the account in cashless transactions (Hernandez and Kim 2020). Opening new accounts may facilitate social assistance payments, but to have a lasting impact on financial inclusion, these accounts need to bring long-term value to customers. This may mean giving recipients the freedom of choice to select an account provider that addresses their needs best (Baur-Yazbeck, Chen, and Roest 2019). This also means that policy makers (and FSPs) should avoid temptations to unnecessarily restrict account use. Restrictions may limit risks but have deleterious effects on customers' long-term trust in the financial system and deepening of financial inclusion.

Importantly, CDD requirements often are **a barrier to account ownership for women,** as women may lack the necessary documentation ranging from ID documents, proof of residence, to proof of income for opening bank accounts. For example, a study in Côte d'Ivoire found that women are more likely to use SIM cards registered in the names of others (Caribou Digital 2020). Another study shows that in the Solomon Islands and Papua New Guinea, young women are expected to stay close to home and women with families have more duties around the home, so they have less time to travel to banks and agents (Payne 2020). In the Solomon Islands, women reported having to travel 4–5 hours to the nearest bank branch and one-and-a-half hours to the nearest bank agent. Thus, efforts to facilitate remote account opening should consider women's documentation, mobility, and comfort and familiarity with digital tools. These efforts also need to address unique privacy concerns women may face, including potential harassment by FSPs agents or financial abuse by those close to them.

ANNEX: AML/CFT Rules Explained

Customer due diligence

The main purpose of AML/CFT requirements is to protect the financial system against abuse by criminals and terrorists. In setting the requirements, countries are bound by international standards set by FATF (2012–2019). Failure to comply with the standards introduces risks that may compromise market integrity and lead the international community to adopt measures that may negatively affect the economy of the noncompliant country.

In relation to social assistance payments, the most important rules relate to CDD measures. When opening a new account and managing it, an FSP must conduct CDD measures (see Table A-1). The main purpose of these measures is to reliably identify customers and ensure that they are not using the account for illicit activity.

TABLE A-1. **Customer due diligence process**

CDD measures	Actions	Social assistance payments context
Identify the customer and verify their identity (ID proofing)	Establish who the customer is by collecting key personal data (e.g., full name, date of birth, address) and verifying veracity of the information against a reliable, independent source (e.g., an official ID document or data). This process is often referred to as know your customer.	Social assistance managers can use databases established for their national programs with information about beneficiaries to facilitate identification and verification.
Identify the beneficial owner	An account can be opened on behalf of or for the benefit of a third person (e.g., where a family member is opening an account for an elderly relative), whose identity must be known to the FSP.	This is not a major concern for social assistance payments as beneficiaries are known. Most programs target either a household unit or an individual. In the latter case, usually programs require an account in that person's name but might allow a "caretaker" to collect payment on behalf of an elderly person.
Define customer's risk profile	Collect information to understand the purpose and intended nature of the business relationship and to create a risk profile of the customer. This includes checking customers and beneficial owners against sanctions and blacklists and determining whether the customer is a "politically exposed person" (e.g., senior politicians, senior civil servants, and their relatives who may be vulnerable to corruption).	The origin of funds is not in question, and recipients generally are targeted for being disadvantaged in some way and left out of the power system. At the same time, the risk of leakages (fraud, corruption) and abuse of funds (terrorist financing) must be addressed. Social assistance managers often have sufficient data on recipients to facilitate such risk profiling by FSPs.
Monitor customer's activities	Monitor transactions and report suspicious and unusual activity to a national financial intelligence unit (e.g., a transaction that does not correspond to the customer's risk profile and may indicate criminal activity).	Despite continuous digitalization, a large share of social assistance payments is simply withdrawn as cash.

Source: Lyman, de Koker, Martin Meier, and Kerse, 2019.

Note: For more details, see Recommendation 10 of FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (2012 and subsequently updated), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

Risk-based approach

Rigid customer identification and verification regulations have long had a negative impact on financial inclusion of poor people who lack proof of official identity (Isern and de Koker 2009). Since 2012, FATF standards require countries to adopt a risk-based approach. In terms of this AML/CFT approach, regulation and CDD measures must be adjusted to mitigate the nature and assessed level of money laundering and terrorist financing risk. Where the risk of abuse is low, less stringent CDD requirements may be allowed (Meagher 2019).

Implementing a risk-based approach requires countries and FSPs to understand the risks based on **money laundering and terrorist financing risk assessments**. The World Bank, for instance, has developed the World Bank National Risk Assessment tool to support country risk assessments.[4] Depending on the level of risks identified, policy makers have two options to simplify CDD requirements: (i) by adopting an exemption based on proven low risk or (ii) by allowing FSPs to simplify CDD measures in relation to products, channels, and customers that pose a lower money laundering and terrorist financing risk.

BOX A-1. **Example on monitoring customer's activities**

Fiji issued guidelines that enabled FSPs to rely on birth certificates and a letter from a "suitable referee" to verify the identity of customers who do not have sufficient formal ID documents (FIJIFIU 2009). 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, FSPs were advised by the Fiji Financial Intelligence Unit to specifically monitor customer accounts and transactions for unusual transactions or pattern of transactions when account opening relied on a referee certificate (FIJIFIU 2007; FATF 2013–2017).

Proven low risk exemption. In line with FATF standards, where there is proven low money laundering and terrorist financing risk emerging from government assessments, exemptions from AML/CFT regulation, whether in full or partial, may be created in strictly limited and justified circumstances and with regard to a particular type of FSP or activity. Countries should make clear the conditions for and potential beneficiaries of the exemptions.

Simplified CDD. CDD measures are risk-control measures. Countries may allow FSPs to simplify these controls where the risks are lower. Which elements to simplify, to what extent, and how to counter-balance them depend on the risk assessment and the controls required to limit the risk. In some cases, it may be appropriate to simplify the verification of the identity of a customer based on the FSP's risk assessment. However, having a lower money laundering and terrorist financing risk for customer identification and verification does not automatically mean that the same customer poses a lower risk for other CDD measures including monitoring of customer activities. Monitoring might need to remain at the standard level to check that the transactions in the account remain within the risk-based thresholds and in line with the customer's risk profile. Or monitoring might need to be tightened to mitigate the inherent risks of the products and services and to compensate for the relaxed initial due diligence checks.

4 "Risk Assessment Support for Money Laundering/Terrorist Financing," World Bank, 29 February 2016, https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support.

BOX A-2. **Example on delayed verification**

Brazil permits simplification of some elements of CDD for "special" or basic banking accounts, subject to quantitative limits (e.g., balance limit of US$750). Customer identification and verification 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 customer identification and verification (Meagher 2019).

In other cases, ID verification may be conducted within a prescribed time frame or postponed until the customer's transaction amounts cross a specified monetary level.

Such simplification of ID verification may be of particular benefit to customers who are poor, underserved, without ID documents or data required to meet the standard verification processes, and cannot travel to a branch for in-person verification. The level of risk can be actively lowered through product design. In many cases, FSPs have designed products with built-in restrictions to keep money laundering and terrorist financing risks low. Such restrictions may be voluntary or required by regulation and may include (i) transaction limits (allowing only small-amount, low-risk transactions), (ii) customer limits (allowing only individuals to open accounts), and (iii) function limitations (not allowing cross-border transactions).

To make things easier, regulators may adopt a **tier-based approach** to CDD, defining tiers of products whose complexity increases with the complexity of CDD steps undertaken. Often, there are three tiers or types of accounts (Meagher 2019):

- **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.

Remote account opening

Traditionally, customers were identified in person. They presented ID documents that were inspected and recorded to verify their identities. AML/CFT authorities have been concerned about identity fraud risks where remote or contactless ID proofing took place, for example, where the customer could photograph his or her ID document and send the photograph to the FSP without any contact with bank staff or agents. The development of trustworthy digital identities has ushered in a new approach.

To determine whether the use of a digital ID system is consistent with customer identification and verification and ongoing monitoring requirements, government authorities and FSPs should (i) determine reliability/independence of the digital ID system based on the assurance levels determined by its technology, architecture, and governance and (ii) analyze whether the digital ID system, given the assurance level, is appropriate for use in ID proofing and other CDD elements.[5]

5 "Assurance level" refers to the level of trustworthiness or confidence in the reliability of each component (e.g., identity proofing and enrollment, authentication) of the digital ID process.

To encourage use of digital identification, FATF has issued guidance on the adoption of digital identity for CDD purposes (FATF 2020b). It broadened the use of digital ID solutions that provide different levels of ID proofing reliability. A digital identity providing a sufficient but lower assurance that identified persons are who they claim to be, for example, can be considered as an element of simplified CDD to provide access to a lower risk product. Importantly, FATF stated that non-face-to-face customer identification and transactions that depend on reliable, independent digital ID systems with appropriate risk mitigation measures in place may present a standard, or even lower level of risk.

FATF's decision process helps FSPs decide whether the use of a specific digital identity is appropriate for customer identification and verification and ongoing monitoring (FATF 2020b):

- If the government has authorized the use of a specific digital ID system for CDD purposes, an FSP can use such digital ID system without performing its own level of assurance assessment.
- If the government has assigned assurance providers, an FSP should use its services to determine the level of assurance provided by a system and match it for CDD purposes to the money laundering and terrorist financing risks of its accounts and products.
- Where the government has not authorized the use of specific digital ID systems for CDD or assigned assurance providers, an FSP must undertake the assurance assessment itself and match the level of assurance to the money laundering and terrorist financing risks of its accounts and products.

BOX A-3. **India's digital ID program: Aadhaar**

India's Aadhaar ID program uses several biometrics, such as fingerprint and iris scan and biographic information, as well as official ID documentation where it is available, to provide a digital identity to all residents. The Unique Identification Authority of India (UIDAI) Aadhaar enrollment process has flexible ID evidence requirements to ensure comprehensive coverage in a jurisdiction where many people lack basic ID documents and that relies on biometrics to establish the uniqueness of individuals. Enrollment must be in person but is conducted at authorized registrars throughout the country, using software and biometric capture and other equipment prescribed by UIDAI.

UIDAI accepts many different types of ID documents to verify core attributes at enrollment: 32 types of ID documents containing name and photo (AADHAAR 2020), 14 proof-of-relationship documents, 10 date-of-birth documents, and 45 proof-of-address documents. If an individual does not have any of the "notified" ID documents, the individual can enroll in Aadhaar if a family entitlement document includes his or her name and the head of family in the entitlement document enrolls in Aadhaar, using required proof-of-identity and proof-of-address documents and introduces the family member while he or she is enrolling. Where no proof-of-relationship or other required documents are available, a resident may use "introducers" or "certifiers"—individuals notified by the registrar or regional UIDAI office and who are available at the enrollment center.

Use of Aadhaar for CDD is strictly voluntary and must be based on the customer's informed consent. Regulated entities may verify the identity of their customers by (i) authentication or offline verification of Aadhaar, (ii) passport, or (iii) any other documents notified by the central government.

Source: FATF, 2020b.

References

Aadhaar. 2020. "List of Acceptable Supporting Documents for Verification." 9 May. https://uidai.gov.in/images/commdoc/valid_documents_list.pdf

Bangko Sentral ng Pilipinas. 2020. "BSP Relaxes KYC Requirements to Facilitate Access to Financial Services." Media Release, 1 April. http://www.bsp.gov.ph/publications/media.asp?id=5342

Baur-Yazbeck, Silvia, Gregory Chen, and Joep Roest. 2019. "The Future of G2P Payments: Expanding Customer Choice." Washington, D.C.: CGAP. https://www.cgap.org/research/publication/future-g2p-payments-expanding-customer-choice

BCEAO. 2020. "Communiqué relatif aux mesures de promotion des paiements électroniques dans le contexte de la lutte contre la propagation du Covid-19." Media Release, 1 April. https://www.bceao.int/fr/communique-presse/communique-relatif-aux-mesures-de-promotion-des-paiements-electroniques-dans-le

Caribou Digital. 2020. "Which DFS Features Matter More to Women Than Men? Experiences from Côte d'Ivoire and Kenya." Blog post, 6 March. https://medium.com/caribou-digital/which-dfs-features-matter-more-to-women-than-men-3a21765b2236

de Koker, Louis, and John Symington. 2011. "Conservative Corporate Compliance: Reflections on a Study of Compliance Responses by South African Banks." ***Law in Context***, 30: 228–54, 2014. https://ssrn.com/abstract=3562092

FATF (Financial Action Task Force). 2012–2019. "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation." Paris, France: FATF. www.fatf-gafi.org/recommendations.html

———. 2013–2017. "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion—With a Supplement on Customer Due Diligence." Paris, France: FATF. www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

———. 2020a. "COVID-19-Related Money Laundering and Terrorist Financing–Risks and Policy Responses." Paris, France: FATF. https://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html

———. 2020b. "Guidance on Digital Identity." Paris, France: FATF. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

———. 2020c. "Statement by the FATF President: COVID-19 and Measures to Combat Illicit Financing." Paris: FATF, 1 April. https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html

FIJIFIU (Fiji Financial Intelligence Unit). 2007. "Advisory: Financial Transactions Reporting Act." https://www.fijifiu.gov.fj/getattachment/Pages/Guidelines-and-Policy-Advisories/Policies-advisories-on-the-FTR-Act/Advisory-2_2007-CDD-of-Customers-Who-Have-Insufficient-or-No-Official-Identification-Documents-(1).pdf.aspx

———. 2009. "Guideline 4: Financial Transactions Reporting Act." https://www.fijifiu.gov.fj/getattachment/Pages/Guidelines-and-Policy-Advisories/Guidelines/Guideline-4_Customer-Due-Diligence-Aug-2009.pdf.aspx

FMA (Financial Markets Authority). 2020. "Guidance: Complying with AML/CFT Verification Requirements during COVID-19 Alert Levels." 26 March. https://www.fma.govt.nz/assets/Guidance/AMLCFT-Supervisor-Guidance-COVID-19-Alert-26-March-2020.pdf

Gentilini, Ugo, Mohamed Almenfi, and Pamela Dale. 2020. "Social Protection and Jobs Responses to COVID-19: A Real-Time Review of Country Measures." Washington, D.C.: World Bank. http://documents.worldbank.org/curated/en/383541588017733025/pdf/Social-Protection-and-Jobs-Responses-to-COVID-19-A-Real-Time-Review-of-Country-Measures-April-24-2020.pdf

Hanmer, Lucia, and Marina Elefante. 2019. "Achieving Universal Access to ID: Gender-Based Legal Barriers Against Women and Good Practice Reforms." Washington, D.C.: World Bank. http://documents.worldbank.org/curated/en/606011569301719515/pdf/Achieving-Universal-Access-to-ID-Gender-based-Legal-Barriers-Against-Women-and-Good-Practice-Reforms.pdf

Hernandez, Emilio, and Dave Kim. 2020. "Agent Networks: Vital to COVID-19 Response, in Need of Support." CGAP blog post, 27 April. https://www.cgap.org/blog/agent-networks-vital-covid-19-response-need-support

Isern, Jennifer, and Louis de Koker. 2009. AML/CFT: Strengthening Financial Inclusion and Integrity. Focus Note 56. Washington D.C.: CGAP. https://www.cgap.org/research/publication/amlcft-strengthening-financial-inclusion-and-integrity

Kazzaz, Zachary. 2020. "Emergency Disbursements During COVID-19: Regulatory Tools for Rapid Account Opening and Oversight." Washington, D.C.: Glenbrook Partners, LLC. https://www.findevgateway.org/paper/2020/07/emergency-disbursements-during-covid-19-regulatory-tools-rapid-account-opening-and

Lyman, Timothy, Louis de Koker, Chrissy Martin Meier, 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-diligence

Meagher, Patrick. 2019. "Risk-Based Customer Due Diligence: Regulatory Approaches." Technical Note. Washington D.C.: CGAP. https://www.cgap.org/research/publication/risk-based-customer-due-diligence-regulatory-approaches

Payne, Rose. 2020. "Five Reasons Women in Solomon Islands and Papua New Guinea Are Financially Excluded." Pacific Financial Inclusion Programme blog post, 5 June. http://www.pfip.org/five-reasons-women-in-solomon-islands-and-papua-new-guinea-are-financially-excluded/

State Bank of Pakistan. 2016. "Branchless Banking Regulations." http://www.sbp.org.pk/bprd/2016/C9-Annx-A.pdf

The authors of this Briefing are Ivo Jenik, Mehmet Kerse, and Louis de Koker of CGAP. The authors thank Gregory Chen, CGAP, for overall guidance. Thanks also go to Robert J. Palacios, World Bank Group, and Stefan Staschen and Silvia Baur-Yazbeck, of CGAP, for their insightful reviews. Joep Roest and Yasmin Bin-Humam provided valuable insights.