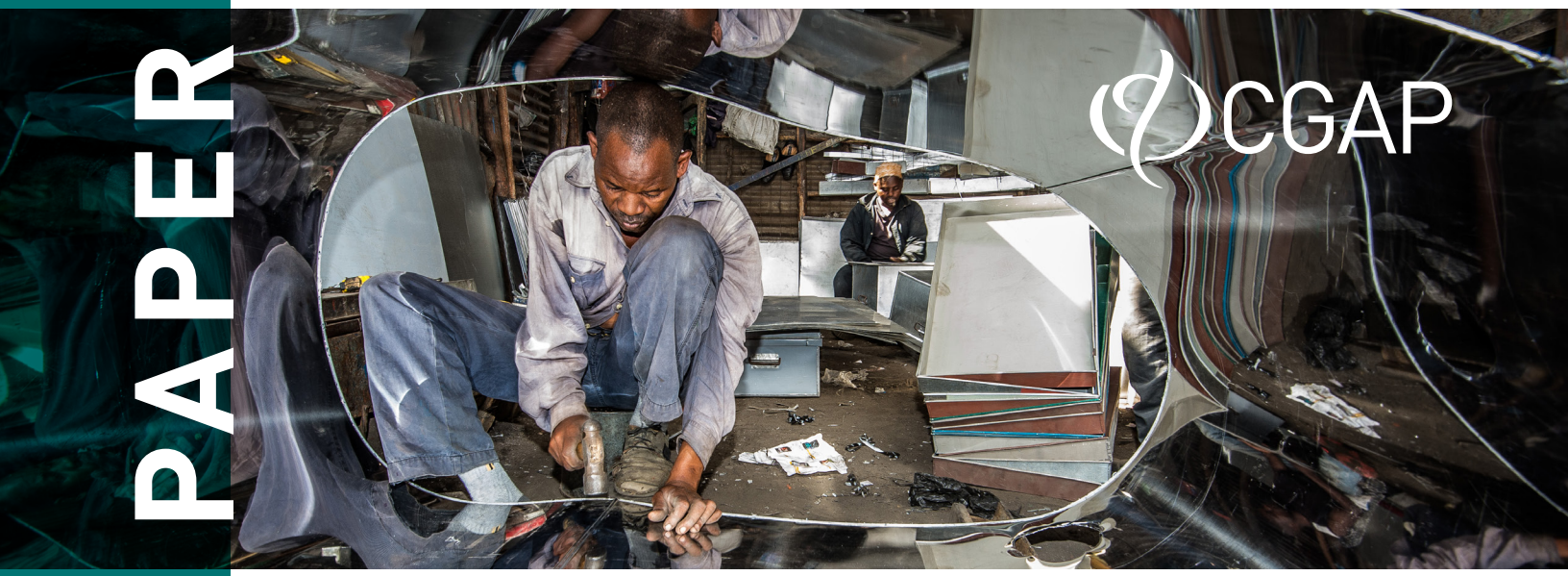
WORKING PAPER



CGAP

BEYOND KYC UTILITIES

Collaborative Customer Due Diligence for Financial Inclusion

August 2019

Timothy Lyman, Louis de Koker, Chrissy Martin Meier, and Mehmet Kerse

ACKNOWLEDGMENTS

This Working Paper grows out of a six-month internal CGAP research project designed by Timothy Lyman, Louis de Koker, and Matthew Soursourian and led by Chrissy Martin Meier. Soursourian coined the term “collaborative customer due diligence.” The authors express their appreciation to CGAP’s Greg Chen, Michael Tarazi, Stefan Staschen, and Silvia Baur-Yazbeck for their editorial and content contributions, as well as to CGAP staff and consultants who commented on the examples or facilitated access to regulatory and institutional experts who shared information about collaborative approaches to customer due diligence.

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

Cover photo by Wim Opmeer.

CONTENTS

EXECUTIVE SUMMARY

PRIVATE COMPANIES AND THE PUBLIC SECTOR, SEPARATELY AND together, are increasingly leveraging new collaborative approaches to help financial services providers (FSPs) meet international customer due diligence (CDD) requirements. To overcome well-documented financial inclusion challenges posed by required measures to combat money laundering and the financing of terrorism, FSPs and governments are exploring and adopting different types of collaboration, including sharing data and the compliance function, on a level that was previously unthinkable. These approaches, while different in form and function, can be collectively described as "collaborative CDD." By pooling resources, these collaborative approaches have the potential to lower CDD costs and increase the effectiveness of anti-money laundering and combating the financing of terrorism measures, making it more feasible for FSPs to serve low-income customers with limited financial histories or those who are members of higher crime risk groups such as those living in or fleeing conflict.

These approaches use biometric data, data mining, artificial intelligence, distributed ledgers, and other technologies to help discharge such CDD obligations as conducting customer identification and verification, establishing beneficial ownership, and monitoring transactions for any suspicious behavior, which may signal money laundering or the financing of terrorism.

CGAP has developed a typology to help policy makers, regulators, and FSPs make sense of the expanding range of collaborative approaches to CDD and evaluate their likely impact on financial inclusion. We apply this typology to nine examples of collaborations and consider their opportunities, challenges, and potential to affect financial inclusion.

This exercise surfaced three key issues and three policy questions that shape any assessment of what role collaborative CDD might play in advancing financial inclusion.

Policy Questions

Will ongoing cost savings from collaborative CDD approaches justify the upfront investment costs?

How can collaborative CDD approaches balance the benefits of data sharing with the need for data protection and privacy?

What risks need to be monitored to ensure that collaborative CDD does not unintentionally create new barriers to inclusion?

- **None of the approaches examined alone offers a comprehensive solution** that addresses the full range of CDD requirements an FSP must meet. Understanding the specific requirements that are addressed by a given collaborative approach helps in evaluating potential benefits for expanding financial inclusion.

- **Most collaborative CDD approaches are in the early stages,** making it difficult to assess their viability, cost effectiveness for an FSP, and ultimate potential impact on financial inclusion.
- **Financial inclusion impact will likely increase when and if governments get more involved.** Formal regulatory approval that allows FSPs to rely on specific collaborative CDD approaches unlocks the potential benefits these approaches hold.

SECTION 1
INTRODUCTION

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF terrorism (AML/CFT) measures, particularly those relating to customer due diligence (CDD), are critical to financial integrity. Yet, the well-documented burden of compliance with AML/CFT standards remains a financial inclusion pain point (Bester et al. 2008; Isern and de Koker 2009; Lyman and Noor 2014; FATF 2017). Poor people often have no formal proof of identification and tend to have small data footprints, making it expensive for providers to perform CDD on them.

To overcome these challenges and increase the effectiveness of AML/CFT measures, financial services providers (FSPs) and governments are exploring and adopting different approaches to CDD, including sharing data and compliance functions—approaches that involve a level of collaboration that was previously unthinkable. These approaches, while different in form and function, can be collectively described as "collaborative CDD."

New technologies, including biometric data, distributed ledgers, and artificial intelligence, are creating new options for CDD. Collaborative CDD leverages these technologies to create new approaches that are more cost-efficient and effective. Private- and public-sector actors are also collaborating on aspects of CDD in new ways that position both sides to discharge their due diligence responsibilities with greater understanding of money laundering and terror financing risks. If implemented well, collaborative CDD approaches, potentially combined with simplified CDD, may be able to address two enduring financial inclusion challenges: (i) lowering the cost of compliance for FSPs, thus rendering it more feasible and cost-effective to serve low-income customers with limited financial histories, and (ii) increasing access for people living in or fleeing higher crime risk contexts (e.g., by improving risk profiling of people who are in groups deemed to pose a higher crime risk based on factors such as their nationality).

This paper offers a typology of collaborative CDD approaches. The typology intends to support policy makers, regulators, and FSPs who are looking for more effective tools for AML/CFT compliance and for expanding financial inclusion, but who are challenged to make sense of the range and variety of new collaborative CDD approaches. It provides a lens through which to understand collaborative CDD developments and a common framework for discussing collaborative CDD. It shows that although CDD is most often associated with customer identification and verification (CIV), collaborative approaches are expanding beyond CIV to other elements of CDD. At the same time, it highlights that development is uneven and

some collaborative CDD models are currently limited to CDD elements of lower relevance to low-income customers. The typology offers a starting point for analyzing collaborative CDD approaches to understand their possible or likely impact on financial inclusion. Based on the application of the collaborative CDD typology to nine examples, the paper concludes with six observations and policy questions to consider as the models develop and spread.

SECTION **2**

DEFINING COLLABORATIVE CDD

WE USE THE TERM "COLLABORATIVE CDD" TO CLUSTER EXISTING and emerging approaches that relieve, through some measure of collaboration, the burden of CDD compliance that traditionally was carried individually by FSPs or that improves the effectiveness of CDD processes (de Koker, Singh, and Capal 2017). These approaches include creative partnerships that may be private-sector led, public-sector led, or hybrids that are public- *and* private-sector led. Some resemble traditional outsourcing arrangements. Yet many others can be distinguished from outsourcing by factors such as design, scale, impact on industry-wide data standardization, explicit basis in regulation, and above all, the role of multiparty collaboration.

Likely the best-known collaborative CDD approaches are know-your-customer (KYC) utilities—(sometimes called KYC registries)—which are services that store customer identity data in a single repository for use by multiple FSPs. Collaborative CDD is a broader concept that extends to approaches that are not utilities in the classic sense of the word and that cover a broader range of compliance functions than those covered by the term KYC.[1]

While most collaborative approaches are in the early stages, some examples of collaborative CDD, such as the identity verification approach of the National Database & Registration Authority (NADRA) in Pakistan, are relatively mature. Still, their broader collaborative significance is becoming clear only now as more collaborative CDD examples and patterns are emerging.

Not all collaborative CDD approaches are directly relevant to financial inclusion. Many are designed to support CDD for established businesses or correspondent banking relationships and/or are focused on developed markets. Analyzing the range of functions that collaborative CDD can address helps to identify those approaches that are, or may have the potential to be, significant to financial inclusion of the poor.

1 Although "KYC" (which lacks a standard, internationally accepted definition) is sometimes used synonymously with "CDD," in this paper it refers only to the customer identification and verification elements of CDD and, in this context, only to circumstances where the term has passed into common usage even among AML/CFT experts. See Section 4 and Lyman and de Koker (2018).

SECTION 3
OVERVIEW OF CDD

TO UNDERSTAND COLLABORATIVE CDD, WE MUST FIRST REVIEW THE definition of CDD and the various CDD compliance measures FSPs are required to undertake. International AML/CFT standards set by the Financial Action Task Force (FATF) require FSPs to perform specific CDD measures both upfront when approached by a prospective customer and during the relationship. In practice, this means several tasks need to be done (see Table 1 describing the various elements of CDD).

TABLE 1. CDD Elements

CDD measures	Associated actions
Customer identification and verification	• Collecting identifying particulars of prospective customers and establishing the veracity of the key identifying particulars using reliable, independent source documents, data, or information
Establishing beneficial ownership	• In relation to individuals, determining whether a person is acting on behalf of another or on behalf of a group (such as a household or a savings scheme in the financial inclusion context) • In relation to legal entities, trusts, and arrangements, determining who is the actual controller of a customer or the beneficiary of a business relationship, service, or transaction • In practice, depending on the information found, undertaking further processes to identify other associated persons that may give rise to AML/CFT risk relevant to the business relationship
Risk assessment and profiling	• Collecting information to understand the purpose and intended nature of the business relationship and to create a risk profile of the customer • The collection process includes checking customers, beneficial owners, and associated persons against sanctions and blacklists and determining whether the customer is a "politically exposed person" (PEP) (e.g., senior politicians, senior civil servants, and their relatives who may be vulnerable to corruption)
Transaction monitoring and reporting	• Continuously monitoring transactions to detect and investigate any unusual transactions and report those that are potentially suspicious to the Financial Intelligence Unit (FIU)—a governmental body set up to receive and analyze such transaction reports • Continuously monitoring transactions to identify ones that, though not necessarily suspicious, are nonetheless reportable, such as transactions involving more than a set amount in cash in countries with cash reporting requirements • Assisting the FIU with further enquiries regarding reported transactions

Source: FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (2012 and subsequently updated) Recommendation 10.

In 2012 FATF adopted a risk-based approach that enables regulators to allow simplified CDD where money laundering or terrorist financing risks are lower. This approach generally supports financial inclusion because it allows accounts and services to be offered with risk-mitigation features (such as transaction limits) and fewer CDD requirements—and hence at a lower cost.

Simplified CDD is of particular benefit to so-called thin-file customers, who are often poor and underserved people who may not have the identity documents required to meet the full range of CDD when standard-risk services are involved. Unfortunately, those who find themselves in or fleeing from higher crime risk contexts may not benefit from simplified CDD because they—and by extension the products they use—may not be assessed as posing a lower risk. These groups include, among others, refugees who are members of communities that are associated with terrorist financing and people living in rural areas where illicit drug crops are cultivated. Even if simplified CDD does apply, an FSP may still determine that it is too expensive to onboard a customer segment that may not be highly profitable. In both cases, collaboration on one or more of the associated CDD elements outlined above may lower FSP compliance costs and thereby address a financial inclusion pain point, as explored in Section 4.

SECTION **4**

COLLABORATIVE CDD TYPOLOGY

THE COLLABORATIVE CDD TYPOLOGY SEEKS TO MAP THE FUNCTIONS of the growing variety of collaborative CDD approaches emerging around the world. The common thread is the element of collaboration to share CDD burdens and/or improve the effectiveness of CDD. The typology, visualized in Figure 1, classifies collaborative CDD approaches by (i) which of the four types of required CDD measures are addressed and (ii) whether the approach in question is a public-led, a private-led, or a public-private partnership. The former helps us to understand how an approach may (or may not) address financial inclusion challenges across all elements of CDD. The latter, at the most basic level, identifies the parties to the collaboration in question. But it is more significant than this. Different mixes of public and private actors in the various elements of CDD present different opportunities and challenges. For instance, data-sharing and data-protection challenges may differ depending on whether it is purely a private or purely a public collaboration, or if the collaboration requires sharing data between public and private entities. The roles (if any) played by the public sector hold particular importance because government involvement and support potentially permits FSPs to rely on information that a particular collaborative CDD approach yields—reducing compliance burdens and costs far more than any purely private approach that does not have any governmental engagement.

In this section, we reference nine examples to illustrate how the typology can be used to categorize different collaborative CDD approaches and analyze how the collaboration may affect the potential to support financial inclusion.[2] The nine examples cover a range of collaboration approaches and are organized by the required CDD measures each example addresses.

2 These examples are presented solely to exemplify the use of the collaborative CDD typology. They are based on publicly available information, interviews with the providers, or both and, to the best of the authors' knowledge, are current and accurate as of 31 May 2019. No endorsement should be inferred from their inclusion.

FIGURE 1. **Collaborative CDD Typology with Examples**

Leadership			CDD Elements					
			Customer Identification and Verification			Risk Assessment & Profiling		Transaction Monitoring & Reporting
			Individuals	Legal entities	Beneficial Ownership	Upfront	Continuing	
	Public	eKYC (India)	X					
		Centralized KYC (India)	X	X (in a next phase)	X			
		eKYC (NADRA) (Pakistan)	X					
		eKYC (Singapore)	X	X (being piloted)	X (being piloted)			
	Private	Yoti	X			X (sanctions & PEP screening & adverse news monitoring)		
		Gravity	X					
		Refinitiv		X	X	X (sanctions & PEP screening & adverse news monitoring)	X (sanctions & PEP screening & adverse news monitoring)	
		Fintel Alliance (Australia)						X (only joint projects)
	Public-Private Partnership	ABS utility project (Singapore) (suspended)		X	X	X	X (sanctions & PEP screening & adverse news monitoring)	

4.1 Customer identification and verification

Legal identification, or lack thereof, is a significant and well-documented barrier to financial inclusion (G20 2018). Identification—collecting the identifying particulars of a prospective customer—is not enough for CDD compliance. The FSP must also *verify* the customer's identity using reliable, independent source documents, data, or information. In the case of thin-file customers, this

verification may be inconclusive, and the FSP may choose not to establish a relationship with the customer. As mentioned, when FSPs assess the money laundering and terror financing risk as lower, simplified CDD may be justified, but this is not an option when risks are assessed as standard or higher and may still be deemed too expensive when weighed against the likely profitability of the relationship. Promising CIV-related collaborative CDD solutions that can be combined with simplified CDD to better address these challenges include:

- Electronic KYC (eKYC) programs led by the public sector
- Centralized KYC solutions
- Identity management solutions led by the private sector

eKYC PROGRAMS LED BY THE PUBLIC SECTOR

National identity authorities that support digital identity verification by FSPs are an important group of collaborative CDD providers, given the reach of their programs. India, Pakistan, and Singapore have experience with eKYC initiatives and provide useful perspectives on CIV programs led by the public sector.

India. eKYC in India leverages the Aadhaar ID program, which provides a unique biometric identifier to more than 1.2 billion people.[3] The authority responsible is the Unique Identification Authority of India (UIDAI), which has made eKYC and authentication services available. An FSP can verify a customer's identity using the customer's Aadhaar number and a fingerprint and/or iris scan. When the identity of a prospective customer is confirmed biometrically, the account opening form is, with the consent of the customer, automatically populated with the customer's basic demographic data.[4] Critically important is that UIDAI vouches for the person's identity. This means that FSPs can rely on the results of a valid query without further identity verification. Since reaching national scale, UIDAI has faced increasing public questions regarding rights to opt out of Aadhaar and data privacy, and it has made various changes to increase the level of data protection. In September 2018, the Supreme Court of India ruled that a section of the original Aadhaar Act relating to private-sector use of eKYC failed to meet constitutional tests. As a result, FSP access to eKYC services was terminated. eKYC use for the provision of public services, such as opening an account to receive social assistance payments, was upheld, and these services therefore continued to be offered. To address private-sector use of eKYC, a temporary ordinance was adopted in early 2019 that legally enables private entities, and in particular FSPs and telecommunication companies, to enroll customers once again offering UIDAI's eKYC as an option. [5] Many expect the government to finalize a data privacy law and adopt permanent fixes to the Aadhaar Act. While permanent resolution of these issues may take more time, most uses of Aadhaar continued. Another notable change is that eKYC fees were introduced by UIDAI in March 2019, changing the commercial incentives to use eKYC with possible implications for financial inclusion (Alawadhi and Choudhury 2019).

3 "Enrolment dashboard," Unique Identification Authority of India, 2019, https://uidai.gov.in/aadhaar_dashboard/india.php.

4 These are name, date of birth, gender, address, email ID, and mobile number. The last two are optional. See "What Is Aadhaar," Unique Identification Authority of India, https://uidai.gov.in/what-is-aadhaar.html.

5 Aadhaar and Other Laws (Amendment) Ordinance, 2019.

Pakistan. eKYC in Pakistan, similar to that in India, leverages the country's extensive national biometric ID system developed and managed by NADRA. eKYC 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 with the unique 13-digit ID number storing demographic and biometric data of the citizen—covers nearly 100 percent of the adult population.[6] CNIC can be issued to citizens of Pakistan who are 18 years of age or above. NADRA data are used for identity 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 an already-verified SIM card, an FSP may remotely open a very basic account for that person (SBP 2016). The fee to use NADRA's verification services initially constrained the use of its services, but the introduction of cheaper services increased its use.

Singapore. Singapore successfully trialed and implemented an eKYC program that enables customers to use their registered profile on MyInfo—a consent-based identity profile platform for Singaporeans—to open accounts. The platform contains the data provided by the user and the data pulled from the databases of various government agencies, such as national ID number, passport number, registered address, and date/country of birth.[7] Consent of customers is sought before any personal data on MyInfo profiles are retrieved by FSPs. An FSP that has been allowed access to a customer's MyInfo data, does not need to obtain further identity verification or photographs of the customer.[8] Singapore has recently started to pilot MyInfo Business, which will allow businesses to share their government-verified data, such as their corporate profile, financial performance, and ownership information through the platform, with FSPs. The business would have less overhead (e.g., filling in forms) and a reduced need to provide supporting documentation for verification processes. MyInfo Business services are being piloted with three local banks to facilitate identification and credit assessments of businesses (Smart Nation Singapore 2019).

Potential to support financial inclusion goals. eKYC models backed by AML/CFT regulation that explicitly allow FSPs to rely on the results of valid queries without the need for further verification of the CIV data have proven powerful in advancing inclusion. This has been the case in Pakistan, notwithstanding the legal challenges in the case of India and uneven pricing practices in both India and Pakistan. However, while eKYC solutions have shown they can support financial inclusion, privacy and data protection need to be managed with care to ensure trust of customers, FSPs, and regulators as well as legal and operational certainty. Commercial certainty is also required: the imposition of even modest fees that were not anticipated may adversely affect FSPs' trust in the model, while higher fees will likely price services for low-income customers out of the market.

6 Other estimates put the coverage at 79 percent ("Global Findex Database," World Bank, 2017, https://global-findex.worldbank.org).

7 "Frequently Asked Questions: MyInfo data related queries," Singapore Government, 2019, https://www.gov.sg/.

8 Monetary Authority of Singapore, Circular No.: AMLD 01/2018. http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Anti_Money%20Laundering_Countering%20the%20Financing%20of%20Terrorism/Circular%20on%20MyInfo%20and%20CDD%20on%20NFTF%20business%20relations.pdf

CENTRALIZED KYC SOLUTIONS

An important group of collaborative CDD service providers holds centralized, verified identity particulars of persons or businesses and makes these available to multiple FSPs for a fee. Some of these providers also furnish additional information on customers (e.g., adverse media profiles) and/or PEP and sanctions screening services that support risk profiling (see Section 4.3). These approaches differ from typical outsourcing arrangements in that they require participating FSPs to standardize their customer data in accordance with an agreed format and contribute the data to the central pool. India's centralized KYC is an example of a centralized KYC model led by the public sector.

Centralized KYC in India. In 2015 India established a centralized KYC registry for CIV data of individuals and legal entities and authorized the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) to operate it. While eKYC made it easier to verify a customer's identity particulars upon first enrollment at one FSP, centralized KYC relieves the burden of repetitive CIV processes when a customer interacts with more than one FSP.

This centralized KYC scheme established standards for the collection and verification of customer identity data by FSPs such as banks, insurance companies, asset management companies, and pension funds. Participating FSPs have to collect a range of customer data (more than the information required for Aadhaar enrollment), including address, using a standardized customer enrollment form.[9] Requirements differ for normal, simplified, and small accounts as well as for accounts opened using eKYC. Upon enrollment, a customer's CIV data may be verified using eKYC or other verification processes. Once completed, the customer's electronic enrollment data are copied to the registry. The registry issues each new customer with a KYC identifier. Customers can use the identifier when they deal with another FSP. As of May 2019, the centralized KYC is still in an early phase where the database is being built with new CIV information. Once the scheme is fully operational, customers will need to provide their enrollment data to only one provider for that verified information to be available to all other FSPs with whom the customer may deal. When a customer's record is updated at the registry, all linked FSPs (those that have previously either uploaded or downloaded that customer's record) will receive an electronic update notification and may download the latest customer record. Centralized KYC via CERSAI is currently capturing only data relating to individuals (RBI 2018).

CERSAI is burdened by its costing structure, where institutions must pay a fee to upload and update data instead of charging only the FSPs that directly benefit from the centralization. The data upload processes are also resource intensive, creating further burdens on participating institutions and increasing cost barriers to serving low-income people.[10] Slow updating of data and failure to update customer data will affect data quality and undermine the usefulness of centralized KYC. Whether the centralized CIV database performs a sufficiently useful function will become clearer only once it is comprehensively populated with data.

9 In addition to the mandatory information collected for Aadhaar enrollment, the FSPs must also collect other customer information for centralized KYC enrollment such as occupation type, residential status, and marital status, among others. For the other information collected, see the individual customer application, "Central KYC Registry," Central Registry of Securitisation Asset Reconstruction and Security Interest of India, https://testbed.ckycindia.in/ckyc/?r=download.

10 See Kagade (2019) for these observations and other suggestions.

Potential to support financial inclusion goals. In principle, centralized KYC can reduce costs and friction for customers who wish to open an account with a second FSP or change providers, once they already have an account with an initial FSP. However, it doesn't make the onboarding process at the first FSP any easier. Centralized KYC models are also challenged by the fact that the FSP participants need to standardize their CIV processes and trust the quality of CIV undertaken by other FSPs. In the case of CERSAI, the trust challenge was addressed by regulation. A significant aspect of the CERSAI model is that FSPs are explicitly entitled and, in fact, compelled, to rely on the registry's data. In other words, they may not, without a good reason (such as a change in information), require a customer to submit the same records, information, or any other additional identification documents or details twice. Whether or not centralized KYC is able to impact financial inclusion will depend on factors such as data quality and whether these models can develop a cost structure that is attractive to FSPs and supports the provision of services to low-income customers.

IDENTITY MANAGEMENT SOLUTIONS LED BY THE PRIVATE SECTOR

Another group of CIV services enables customers to manage their own identification data digitally and provide selected information at a specific point in time for CIV purposes. In contrast to the centralized registry approach, these services decentralize data and empower customers to hold and manage their own identity data. These identity management solutions, sometimes called identity wallets, provide a means for an individual to hold all of his or her identity information in one virtual location and share information when required.

Typically, identity data are held on one or more distributed ledgers.[11] In some cases, the identity is still based on a government-issued ID and then complemented by additional data such as social media footprints or similar data reflecting a person's pattern of life. In other cases, services are attempting to build trusted identities that do not require the user to have a government-issued ID. While these are still largely experimental, they may hold promise for forcibly displaced persons (FDPs) and the estimated 1.1 billion people worldwide who do not have access to a formal, government-issued ID (ID4D 2017).

In addition to allowing customers to control their own data, these services may lower the cost of CIV if FSPs are able, and willing, to use such data. However, many questions remain. First, these services require, in many cases, the active collaboration of the customer to stock, manage, and use the identity wallet—which may be perceived as a benefit by some and as a burden by others. It remains to be seen whether significant numbers of financially excluded or underserved customers are willing and able to manage their own identity data appropriately. In addition, it is not yet clear how to create sufficient trust in, and acceptance of, these new services.

These opportunities and challenges are highlighted through two examples of identity management solutions: Yoti and Gravity.

Yoti. U.K.-based Yoti provides a free app-based service for individuals from over 160 countries who want to have their own identity wallet. Yoti verifies identities using a combination of facial

11 A distributed ledger is a database that is spread across several nodes where each node independently records and saves an identical copy of the ledger and where changes are determined by consensus. Blockchains are one form of distributed ledger technology.

recognition software, government-issued identity documents (passport, a national ID card, or a driving license), and where possible, biometric passport chips (ePassports). For a small fee, and with customer consent, FSPs can use Yoti to verify a customer's identity and perform PEP and sanctions checks (see Section 4.3).[12] Customers can share their information through Yoti at no charge. Whether Yoti is sufficient to meet an FSP's CDD obligations depends on several factors, such as local regulation and the risk level of the customer.[13]

Gravity. Gravity is building a self-sovereign digital identity management solution that is intended to be sufficient for CIV. Currently piloting in Kenya, the service allows users to verify their identity through a range of means that contribute to an identity score, including using a customer's social network to confirm that the data are true and accurate. Gravity users can increase their score by getting a government official to confirm data (e.g., a police officer attesting to having reviewed the customer's government-issued ID card). These inputs are used to create the customer's identity score. The identity score increases based on the quality and quantity of verifications received, accounting for the different levels of trust placed in the various actors within a community or an ecosystem (GSMA 2017). The authenticity of the verifications is guaranteed by leveraging blockchain technology and peer-to-peer certifications. Gravity has a pay-per-data revenue model: services providers are charged a fee to access customer data for identification. A part of the fee is returned to the customer as compensation for the collection and use of personal data. Gravity is currently collaborating with a nongovernment organization (NGO) in northern Kenya to implement a self-sovereign digital ID education wallet for refugee students that would allow the NGO to better track student attendance and course completion.[14]

While FATF standards allow simplified CDD where risks are lower, FSPs still need to be comfortable that they have properly identified their customers—and have verified the customers' identity with independent and reliable source documents. Whether private-sector-led identity management solutions, especially those that do not rely on government-issued IDs, will be embraced by FSPs for CIV purposes remains to be seen. In addition, sustainable solutions require appropriate privacy and data protection measures, preventing over-collection of data and supporting their users to release information responsibly.

Potential to support financial inclusion goals. Digital identity management solutions have promise to increase financial inclusion by making identity easier to manage and access. Where these services do not rely on government-issued documents, their model may provide a path to inclusion for thin-file customers and people from riskier countries who may not have IDs or who hold IDs that are not trusted internationally (as is the case of FDPs fleeing sanctioned countries). However, securing regulatory and FSP support for the use of such services for CIV purposes remains a major challenge. On the other hand, FSPs may use digital identity management solutions to supplement standard CDD by providing a richer profile of customers. This could enable FSPs to control customer-related money laundering and terror financing risk more effectively, thereby increasing the scope of clientele they are willing to serve.

12 "Business Pricing," Yoti, 2019, https://www.yoti.com/business/pricing/.
13 "Can Yoti Be Used for KYC and AML Compliance?" Yoti, 2019, https://yoti.zendesk.com/hc/en-us/articles/360006947293-Can-Yoti-be-used-for-KYC-and-AML-compliance-.
14 See "Use Cases," Gravity, https://www.gravity.earth/use-cases#overview.

4.2 Establishing beneficial ownership

FATF standards require FSPs to determine whether individual customers are acting on their own or on behalf of another person or persons. While no collaborative CDD approaches have yet emerged to support beneficial ownership checks for individuals, there have been some attempts to do so for companies and nonprofit organizations. Some countries have been collecting more extensive beneficial ownership information as part of their company registries, some of which may be available for CDD purposes. Services providers, including credit bureaus, have also been collating beneficial ownership data that can be accessed for a fee.

ABS corporate customer utility project. The corporate customer utility project of the Association of Banks in Singapore (ABS) is an example of an approach that underpins these solutions—and complexities associated with them. A private-sector-led utility committee explored the establishment of a KYC utility that would support both CIV and beneficial ownership checks in relation to corporate customers. The committee included local and foreign banks and reported to the Council of the ABS. It worked closely with the Monetary Authority of Singapore and companies such as Refinitiv (see Section 4.3). The project was put on hold by ABS in September 2018 because the model proved too costly. The combination of utility set-up costs, the expenses of migrating historical bank data into the utility, the investment required by each bank to procure and implement required technology, and the organizational changes undermined the viability of the business case (ABS 2018).

As the ABS example shows, collaboration does not necessarily save CDD costs, especially not in the start-up phase. The system needs to be designed to benefit FSPs that have differing levels of development, maturity, and sophistication and that currently manage CDD in different ways. Standardizing CIV data across national and foreign institutions with different CDD policies and processes can be challenging. The complexity of the market in Singapore (though not atypical, at least as to the number of different categories of FSPs under supervision) increased the costs of the ABS model.[15] It remains to be seen whether it will be possible to adopt the model with greater success in a less complicated market in a way that will serve financially excluded or underserved customers.

Potential to support financial inclusion goals. Improved beneficial ownership information will improve FSP risk profiling and management, enabling FSPs to do business with customers who they previously considered to be too risky (see Section 4.3). This said, the example offers little in the way of collaborative solutions to challenges that arise commonly in the financial inclusion context (e.g., where a household or village savings scheme uses an account opened and operated by one individual). However, if collaborative approaches can drive down costs of establishing beneficial ownership or if innovative private-sector-led identity management solutions are broadened to cover beneficial ownership, they may eventually be extended to individuals.

15 The banking supervision authority in 75 percent of low-income jurisdictions responding to the Basel Committee on Banking Supervision survey on regulation and supervision of institutions relevant to financial inclusion had supervisory responsibility for four or more different categories of FSPs, whereas in high-income respondents, 61 percent had supervisory responsibility for only three or fewer types of FSPs. Market complexity in low-income respondents was also reflected in the number of different functional areas of supervisory responsibility, with high-income jurisdictions being least likely to have banking supervisors with both a high number of functional responsibilities beyond prudential supervision and responsibility for more than three categories of institution. This combination of multiple functions is more commonly seen in low-income jurisdictions. See BCBS (2015).

4.3 Risk assessment and profiling

A well-established group of CDD services provides FSPs with access to combined lists of sanctions, PEPs, blacklists, and persons of interest, as well as tools to enable them to screen prospective and current customers. These screening services are sometimes combined with KYC registry services to deliver richer customer data to participating FSPs. By sharing data, participating FSPs do not have to perform their own screening, which has the potential to lower compliance costs. As compared with other approaches, these services look more like traditional outsourcing to a third-party data aggregator and analyst than active collaboration among FSPs or among FSPs and public bodies. Nonetheless, there is an important element of passive collaboration because each participating FSP contributes at least marginally to enriching the data pool.

Refinitiv's KYC as a Service. KYC as a Service by Refinitiv, formerly Thomson Reuters' financial and risk business, is a prominent private-sector example of this model. Refinitiv touts KYC as a Service as "an innovative and cost-effective identity verification, entity unwrapping, and screening service."[16] It provides information that can help an FSP to conduct counterparty due diligence on another entity (including another FSP) to establish or maintain a business or customer relationship with larger corporations (including correspondent banking relationships). Refinitiv's broader suite of linked risk-management products includes PEP and sanctions screening and related risk profiling services. World-Check, for example, the firm's PEP and person of interest database, provides data to users and allows users to report an individual or entity that has raised compliance concerns for inclusion in the World-Check database. This fosters a limited collaborative element and enriches the data available to all customers.

The fee-based nature of a private-sector led KYC as a Service model such as Refinitiv's raises obvious questions as to its usefulness in the financial inclusion context, where costs of compliance constitute one of the most significant enduring challenges. In theory, at least, the negative cost impact could be lessened if the services are provided to—and through—a KYC registry, where all participating FSPs share directly in the efficiency-enhancing benefits of centralizing their risk assessment and profiling data.

Potential to support financial inclusion goals. These services may improve FSP risk profiling and management, enabling them to do business with customers who were previously deemed to pose too high of a risk. Currently, however, none is focused on individuals and the types of high-risk populations that experience financial exclusion, such as those living in or fleeing higher crime risk contexts. Improved data analytics and information sharing should increasingly lower the costs of such services, allowing their scope to be broadened to individuals. For the time being, there are no examples of such a collaborative CDD approach specifically aimed at reaching the financially excluded and underserved.

16 See "Screening Resolution Service," Refinitiv, https://www.refinitiv.com/en/products/kyc-screening-resolution-service.

4.4 Transaction monitoring and reporting

Transaction monitoring and reporting are vital elements of financial integrity, and yet they can be extremely challenging for both government agencies and FSPs. Indeed, 80–90 percent of such reports do not provide operational value to active law enforcement investigations (Maxwell and Artingstall 2017). This assessment, while of great concern as a matter of public policy effectiveness, is hardly surprising. Unless they are parties to a collaborative approach, FSPs generally see only their own customers' transactions, and law enforcement tend to closely guard information about criminal investigations that would help FSPs do more effective risk profiling and monitoring. Thus, it is in this space that we are observing some of the most promising collaborative approaches emerge under joint public-private leadership.

Fintel Alliance (Australia). A pioneer among these collaborations is Fintel Alliance in Australia, which allows FIUs, law enforcement agencies, and FSPs to share information about criminal behavior and to launch joint investigations into specific priority crimes and criminals.[17] Fintel Alliance is a public-private partnership led by Australia's AML/CFT regulator, AUSTRAC. It brings together intelligence analysts from a range of public entities and FSPs to collaborate on investigative and intelligence projects intended to address specific priority crimes and challenges. Many transactions and customers may not appear suspicious if monitored by only individual FSPs (and possibly only a single FSP). However, viewing patterns across several FSPs and across other potential areas of criminal activity can identify suspicious transactions and customers that would have otherwise gone unnoticed. Fintel Alliance brings together government analysts and designated FSP employees to support information sharing on priority projects. In addition, it informs AUSTRAC's innovation hub, which designs, tests, and improves AML/CFT technologies.

Working alongside government analysts, designated FSP employees improve their own understanding of significant crimes, crime trends, and related national security and law enforcement needs and priorities. Improved understanding, in turn, promises to inform more effective CDD by FSPs and, in particular, customer risk profiling and transaction monitoring.

Potential to support financial inclusion goals. The collaborative aspect of Fintel Alliance has the potential to change mindsets, as public- and private-sector participants actively share their different knowledge and skills sets. This may help participating FSPs to gain confidence and engage customers that were previously denied services because they were incorrectly deemed to be too risky. Not only do these FSPs now communicate better with public-sector agencies that understand aspects of such risk, but individual FSP employees could develop risk-management skills they can use to more effectively and efficiently assess risks of new customer segments.[18] Fintel Alliance could be particularly powerful if it launched projects to combat cash-based money laundering and terrorist financing. These would have the potential to inform innovative approaches to balance inclusion and AML/CFT compliance for population segments otherwise presumed to be high risk.

17 Similar intelligence-sharing models have been launched in countries such as the United Kingdom, the United States, the Netherlands, Hong Kong, Singapore, Malaysia, Canada, and Argentina. See Chadderton and Norton (2019) and Maxwell (2019).

18 This may, for example, help limit so-called de-risking (e.g., a risk-informed approach to terminate and refuse financial services) of customers deemed to pose either a high money laundering and terror financing risk or a risk that is not profitable for the FSP. See GPFI (2016); de Koker, Singh, and Capal (2017); and FSB (2018).

SECTION 5

COLLABORATIVE CDD: OBSERVATIONS AND FORWARD-LOOKING POLICY QUESTIONS

THE EXAMPLES IN THE PREVIOUS SECTIONS HELP TO ILLUSTRATE how collaboration across FSPs' CDD obligations is playing out—or how it may play out in the future—to lower the cost of financial services for poor people and increase access for people living in or fleeing higher crime risk contexts. The aim is to contribute to the discussion and analysis about how collaborative CDD approaches may already be having a positive effect on inclusion, but also to prompt ideas of other ways collaborative approaches could be used. The exercise of mapping even this modest selection of examples across the collaborative CDD typology gives rise to six observations and forward-looking policy questions worthy of discussion among stakeholders interested in eliminating financial inclusion pain points in AML/CFT:

To evaluate the potential benefit of a collaborative CDD approach, it is important to consider which CDD elements are (and are not) addressed.
None of the collaborative CDD approaches exemplified provides support for addressing all of the CDD measures FSPs need to take to meet AML/CFT obligations.[19] An assessment of the potential impact of collaborative approaches to CDD should therefore consider how FSPs will deal with relevant CDD responsibilities that are not addressed by a given approach—and whether there is a role for collaboration beyond the approach in question. For instance, today many CIV services focus only on customer enrollment processes (where CIV obligations first arise). They may not necessarily help FSPs keep customer data current on an ongoing basis or to adjust customer risk profiles during the course of the business relationship. The cost-lowering impact can therefore

19 Not all elements of CDD may be equally relevant to either financial inclusion or the prevention of money laundering and terror financing. Depending on the local context and regulation, for example, beneficial ownership checks may be less important from a risk perspective but also figure lower among FSPs' reasons for not serving a particular excluded or underserved customer segment than other required CDD measures.

be expected to be modest because the key components of CDD will still need to be performed individually by each FSP. Ideally, collaborative CDD services that are currently provided only during customer enrollment will expand over time to also support updates of customer data to help FSPs keep their records current and to support continuous risk profiling of customers that risk-based AML/CFT regulations require. Policy makers can encourage collaborative approaches where they are not used or considered across all four types of required CDD measures.

Most collaborative CDD approaches are in nascent stages and provide important case studies for regulators and stakeholders to monitor.
While a small number of approaches are mature (e.g., the NADRA model of eKYC in Pakistan), most others are far more recent. Some are still in the initial build-out phase, while the development of the ABS model in Singapore has been suspended. Whether a given approach will have a positive impact on financial inclusion will depend on many locally specific factors such as market structure, partnership considerations, and regulatory factors and on other factors such as product design and costs. For example, despite the fact that the Indian eKYC model had been able to reduce the cost of the CIV component of customer enrollment,[20] questions about data protection, privacy, legal validity, and costs created uncertainty in private-sector use of the service. The impact of these concerns may be lessened by regulatory action that enhances legal certainty and data protection, but whether and how such actions may have impact will become clear only over time.

Financial inclusion impact will likely increase when and if governments get more involved.
Government involvement has been shown to increase the validity and usefulness of identity data for initial customer enrollment. eKYC or centralized KYC services could, in theory, be expanded to help FSPs screen customers against sanctions lists, PEP lists, and other relevant blacklists. Such services would alert FSPs that further investigations may be required, thereby saving FSPs the costs of undertaking these checks individually.

It is also important to note that some collaborative CDD models raise new questions for regulators. The sooner regulators address them, the sooner private-sector entities will gain the clarity and certainty they need to justify further investment in collaborative CDD and outreach to currently financially excluded and underserved customers. Clarity regarding regulatory approval will be key to achieving the financial inclusion potential of collaborative CDD approaches generally. FSPs will be reluctant to embrace collaborative CDD services unless the AML/CFT regulator makes it clear that they are allowed to rely on such services and that they will not be held liable for incorrect data provided, or errors made, by the collaborative CDD services provider if the FSP acted reasonably. The explicit regulation in India allowing FSPs to rely on eKYC identity verification provided by the government was a key reason for its widespread adoption by FSPs. In the case of public-private collaborations on transaction monitoring and reporting, FSPs' interest in participating will likely be enhanced by explicitly factoring in such support when regulatory sanctions for noncompliance with AML/CFT laws are considered.

20 Some estimated that with the increased queriability, digitization, and interoperability of the Aadhaar system, average customer onboarding costs could be lowered from approximately 1,500 rupees ($23) to 10 rupees (US$0.15) (ID4D 2018). These estimates predate the 2018 limitations to the use of eKYC and the 2019 introduction of fees.

Will collaborative approaches be able to manage upfront investment costs to create ongoing cost savings?

The shelving of the ABS utility project in Singapore as a result of cost concerns (see Section 4.2) shows that collaboration does not necessarily present sufficient short- or even medium-term savings to justify the required public- and private-sector investment. In particular, the data standardization required by a centralized KYC registry may be costly. eKYC models are not free from cost concerns either, as illustrated by the NADRA model in Pakistan and since March 2019 by the eKYC model in India. We need to understand how best to ensure commercial viability for FSPs that serve low-income persons and/or target the financially excluded or underserved because the imposition of new fees or increases in existing fees may have a disproportionate impact on their business models. One partial solution may lie in using a collaborative CDD approach to support not only AML/CFT but also other compliance and risk-management objectives, for example, fraud prevention, data protection, and potentially cybersecurity.

How can collaborative CDD approaches balance the benefits of data sharing with the need for data protection and privacy?

The story of Aadhaar eKYC illustrates the importance of a sound legal basis for a scheme as well as appropriate privacy and data protection measures. To support the growth of collaborative CDD, regulators need to adopt appropriate rules, including an enabling (yet adequately protective) information-sharing framework. Various laws and regulations—such as customer-banker confidentiality, public-sector secrecy, data protection laws, and AML/CFT laws—address valid policy objectives. Yet, the gradual accumulation of layers of rules over many years has given rise to inadvertent information-sharing barriers that need to be addressed. Accelerating change with the digitization of financial services broadly—much of it driven by the use of alternative data and advanced data analytics—is also challenging the adequacy of existing rules on data sharing and data protection. New information-sharing frameworks need to reflect privacy and data protection principles and allow for the collaboration necessary to lower compliance costs. These will increase the effectiveness of AML/CFT measures while also supporting financial inclusion (Watts, Medine, and de Koker 2018).[21]

What risks need to be monitored to ensure that collaborative CDD does not unintentionally create new barriers to inclusion?

Collaborative CDD models that offer services to FSPs for a fee may shut out smaller FSPs, including those, such as financial cooperatives, that are more likely to target or aspire to target poor customers, the financially excluded, and the underserved. This could, in turn, limit competition, thereby raising prices. Competition may also suffer if smaller FSPs are excluded because a collaborative CDD approach embraced by large FSPs has a high upfront cost—as may be the case with new technologies, such as biometrics and artificial intelligence. These technologies, which are often used for AML/CFT-oriented regtech and suptech solutions, require participating FSPs to make significant investments in hardware and software, which may be beyond the reach of smaller providers, at least in the absence of public subsidy. Where regulators are sensitive to these considerations, they may be able to shape collaborative CDD approaches that manage and allocate costs so as to allow for competition, to help ensure that the new collaborative models serve the market as a whole.[22]

21 Another issue worth considering is data localization laws, which are often defended by recourse to data protection concerns, but which render cross-border collaborative CDD solutions very difficult, if not impossible.

22 Exclusion may be reinforced if some customers struggle to meet new technology-driven identification requirements. See Makin and Martin (2018).

REFERENCES

ABS (Association of Banks in Singapore). 2018. "Industry Banking KYC Utility Project After-Action Report—Knowledge Sharing." Singapore: ABS. https://abs.org.sg/docs/library/kyc-aar_15-nov-2018.pdf.

Alawadhi, Neha, and Karan Choudhury. 2019. "Govt Move to Charge Us for Aadhaar e-KYC to Make Services Costly: Industry." *Business Standard*, 10 March. https://www.business-standard.com/article/economy-policy/govt-move-to-charge-us-for-aadhaar-e-kyc-to-make-services-costly-industry-119031000010_1.html.

BCBS (Basel Committee on Banking Supervision). 2015. "Range of Practice in the Regulation and Supervision of Institutions Relevant to Financial Inclusion." Basel: BCBS. https://www.bis.org/bcbs/publ/d310.pdf.

Bester, Hennie, Doubell Chamberlain, Louis de Koker, Christine Hougaard, Ryan Short, Anja Smith, and Richard Walker. 2008. "Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines." Washington, D.C.: First Initiative. http://www.finmark.org.za/wp-content/uploads/2016/01/Rep_ImplementingFATFstandards_2008.pdf

Chadderton, Paula, and Simon Norton. 2019. "Public-Private Partnerships to Disrupt Financial Crime: An Exploratory Study of Australia's Fintel Alliance." The SWIFT Institute Working Paper No. 2017-003. London: The SWIFT Institute. https://swiftinstitute.org/wp-content/uploads/2019/05/SIWP-2017-003-Information-Sharing_FINTEL_Alliance_FINAL.pdf.

de Koker, Louis, Supriya Singh, and Jonathan Capal. 2017. "Closure of Bank Accounts of Remittance Service Providers: Global Challenges and Community Perspectives in Australia." *University of Queensland Law Journal* 36(1): 149–51. http://www6.austlii.edu.au/cgi-bin/viewdoc/au/journals/UQLJ/2017/6.html

FATF (Financial Action Task Force). 2017. "FATF Guidance on AML/CFT Measures and Financial Inclusion, with a Supplement on Customer Due Diligence." Paris: FATF. https://www.fatf-gafi.org/fr/publications/inclusionfinanciere/documents/financial-inclusion-cdd-2017.html?hf=10&b=0&s=desc(fatf_releasedate)

FSB (Financial Stability Board). 2018. "FSB Action Plan to Assess and Address the Decline in Correspondent Banking: Progress Report to G20 Summit of November 2018." http://www.fsb.org/wp-content/uploads/P161118-3.pdf.

G20. 2018. "Digital Identity Onboarding." Washington, D.C.: World Bank Group, xiii. http://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

GPFI (Global Partnership for Financial Inclusion). 2016. "Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape." GPFI: 68–72. https://www.gpfi.org/publications/global-standard-setting-bodies-and-financial-inclusion-evolving-landscape

GSMA. 2017. "Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid." London: GSMA, 13–15. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf.

ID4D (Identification for Development). 2017. "Making Everyone Count." Brochure. Washington, D.C.: World Bank Group. http://pubdocs.worldbank.org/en/726141507833458171/ID4DBrochure101217.pdf.

———. 2018. "Private Sector Economic Impacts from Identification Systems." Washington, D.C.: The World Bank Group, p. 13. http://pubdocs.worldbank.org/en/219201522848336907/PrivateSectorEconomicImpactsIDSystems-Web.pdf.

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

Kagade, Mandar. 2019. "Reforming the Centralised KYC Infrastructure." MEDICI. https://gomedici.com/reforming-ckyc-infrastructure/

Lyman, Timothy, and Wameek Noor. 2014. "AML/CFT and Financial Inclusion: New Opportunities Emerge from Recent FATF Action." Focus Note 98. Washington, D.C.: CGAP. https://www.cgap.org/research/publication/amlcft-and-financial-inclusion

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

Makin, Paul, and Chrissy Martin. 2018. "6 Things You May Not Know About Biometrics." CGAP blog post, 26 July. https://www.cgap.org/blog/6-things-you-may-not-know-about-biometrics

Maxwell, Nick, and David Artingstall. 2017. "The Role of Financial Information-Sharing Partnerships in the Disruption of Crime." London: Royal United Services Institute for Defence and Security Studies, 5. https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_artingstall_web_4.2.pdf.

Maxwell, Nick. 2019. "Expanding the Capability of Financial Information-Sharing Partnerships." London: Royal United Services Institute for Defence and Security Studies. https://rusi.org/sites/default/files/20190320_expanding_the_capability_of_financial_information-sharing_partnerships_web.pdf.

Monetary Authority of Singapore, Circular No.: AMLD 01/2018. http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Anti_Money%20Laundering_Countering%20the%20Financing%20of%20Terrorism/Circular%20on%20MyInfo%20and%20CDD%20on%20NFTF%20business%20relations.pdf

RBI (Reserve Bank of India). 2018. "Report of the High-Level Task Force on Public Credit Registry for India." Mumbai: RBI. https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=895.

SBP (State Bank of Pakistan). 2016. "Branchless Banking Regulations for Financial Institutions Desirous to Undertake Branchless Banking." http://www.sbp.org.pk/bprd/2016/C9-Annx-A.pdf.

Singapore Government. 2019. Frequently Asked Questions: MyInfo data related queries. http://www.ifaq.gov.sg/MyInfo/apps/fcd_faqmain.aspx?qst=hRhkP9BzcBImsx2TBbssMsxu7lqt6U-JK70a1wAEVmydttHp4N5VLM%2bu7UlaUdH-GatinMA5SwC2DAyFUscBIXDMJgUH4CrJB6i-hYKyCPa2YdxAxrO13B2HTPKEYEV6LLFRcg9qv-FRQcWGdUEjfa1T2g%3d%3d#FAQ_237751.

Smart Nation Singapore. 2019. "MyInfo Business." Media Factsheet. Singapore: Smart Nation Singapore. https://www.smartnation.sg/docs/default-source/press-release-materials/media-factsheet---myinfo-business.pdf.

Watts, David, David Medine, and Louis de Koker. 2018. "Customer Due Diligence and Data Protection: Striking a Balance." CGAP blog post, 9 August. https://www.cgap.org/blog/customer-due-diligence-and-data-protection-striking-balance.