Focus Note: The Use of eIDs and eKYC for Customer Identity and Verification in Developing Countries:

Progress and Challenges

Perlman, L[1] and Gurung, N[2]

ABSTRACT[3]

Increased use of electronic identification (eID) over physical identification is paving the way for adoption of electronic Know Your Customer (eKYC) systems to fulfill customer identification and verification (CIV) obligations. The impact of eKYC can however manifest beyond CIV to other Customer Due Diligence (CDD) processes.

Successful implementation of eKYC while important for Anti Money Laundering (AML) and Countering the Financing of Terrorism (CFT) purposes requires more than just a robust eID and affects SIM card registrations and opening of Digital Financial Services (DFS) accounts and hence financial inclusion.

To highlight this trend, this Note discusses current implementations of eIDs and eKYC and its impact on, access to and provision of DFS. However, with multiple stakeholders in the system, issues of regulatory coordination, technological capacity, and data protection and privacy affect the use of eKYC for financial inclusion.

The eKYC systems that have been launched have as their overriding goals to advance a person's access to services, reduce identity fraud, and increase financial inclusion. Country examples and challenges – public policy, privacy, harmonization, security, legal, financial and infrastructural - in the rollout are discussed.

---

[1] Leon Perlman, PhD, Head: Digital Financial Services Observatory, Columbia Institute for Tele-information, Columbia University, New York.

[2] Nora Gurung, primary author. Research Associate: Digital Financial Services Observatory, Columbia Institute for Tele-information, Columbia University, New York.

[3] This research was funded through a grant from the Bill and Melinda Gates Foundation, which facilitated the creation of the Digital Financial Services Observatory, a DFS policy and regulatory research project of the Columbia Institute for Tele-information at Columbia University in New York. See www.dfsobservatory.com

ABBREVIATIONS

AFIS	Automated Fingerprint Identification System
AML	Anti-Money Laundering
API	Application Program Interface
BIS	Bank for International Settlements
BVN	Bank Verification Number
CBN	Central Bank of Nigeria
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CICO	Cash In/Cash Out
CIV	Customer Identification and Verification
DFS	Digital Financial Services
DFSP	Digital Financial Service Provider
DLT	Distributed Ledger Technologies
EDD	Enhanced Due Diligence
EAC	East African Community
eGov	e-Government
eID	Electronic ID
eKYC	Electronic Know Your Customer
FATF	Financial Action Task Force
FI	Financial Institution
Fintech	Financial Technology
FIU	Financial Intelligence Unit
FSB	Financial Stability Board
ID	Identification Document
KYC	Know Your Customer
MFS	Mobile Financial Services
ML	Money Laundering

MNO	Mobile Network Operator
MoU	Memorandum of Understanding
NCC	Nigerian Communications Commission
NDI	National Digital Identity
NIC	National Identification Card
NID	National ID
NIDB	National Identity Database
NIMC	National Identity Management Commission
PAN	Permanent Account Number
PEP	Politically Exposed Persons
PPP	Public Private Partnership
PSP	Payments Service Provider
RBI	Reserve Bank of India
RBA	Risk Based Approach
SARB	South African Reserve Bank
SBS	La Superintendencia de Banca, Seguros
SDD	Simplified Due Diligence
SIC	Smart ID Card
SIM	Subscriber Identity Module
SSB	Standard Setting Body
TF	Terrorist Financing
UCC	Uganda Communications Commission
UIDAI	Unique Identification Authority of India
UNCDF	United Nations High Commission For Refugees
UNHCR	United National High Commissioner for Refugees
USAID	United States Agency for International Development
VID	Virtal ID
WEF	World Economic Forum

1. INTRODUCTION

Financial inclusion[4] has increased globally with 69% of adults having access to formal financial services.[5] This increase is mainly driven by the uptake of mobile phones and access to the internet.[6] Yet, 1.7 billion people still remain financially excluded.[7]

A successful innovation in addressing the provision of basic financial services and at relatively low cost serving financial inclusion goals is known Digital Financial Services (DFS).[8] It mimics the basic transactional – and mostly non-credit - capabilities of bank accounts, but is provided by banks as well as non-banks such as mobile network operators (MNOs) and third parties known as Digital Financial Services Providers (DFSPs). Access to DFS is (primarily) via low-cost mobile phones,[9] and is sometimes also termed 'mobile money' and 'mobile financial services' (MFS). There are now 270 live DFS implementations in over 90 countries.[10]

Sign-up for a DFS account usually requires provision of an acceptable form of identity to an 'agent' of the DFSP. These agents are sometimes called 'human ATMs' to recognize their critical role in providing (and accepting) digital 'mobile money' to and from customers by exchanging cash. This facility is often known as 'cash in/cash out' (CICO).[11]

However, the sign-up for DFS and acquisition of necessary MNO SIM cards for mobile access is often handicapped by a lack of acceptable forms of identity that may be required by national regulations relating to Anti-Money Laundering and Counter Terrorist Financing (AML/CFT) [12] policies often issued by a central bank, telecommunications regulator or financial intelligence unit (FIU) as the case may be.[13] AML/CFT requirements to detect and counter money laundering (ML) and terrorist financing (TF)[14] may be part of what has historically been referred to as Know Your Customer (KYC)[15] but which is now

---

[4] For an overview of financial inclusion, see Perlman, L (2018) *Digital Financial Services Primer 2018*, available at dfsobservatory.com

[5] World Bank (2018) *The Global Findex Database 2017,* available at https://globalfindex.worldbank.org/

[6] *ibid.*

[7] *ibid.*

[8] For an introduction to and overview of DFS, see Perlman, L (2018) *Digital Financial Services Primer 2018*, available at dfsobservatory.com

[9] For an overview of the mobile phones and technologies used in DFS, see Perlman, L (2017) *Technology Inequality: Opportunities and Challenges for Mobile Financial Services*, available at https://bit.ly/2pAHOBw

[10] Naghavi, N & Scharwat, C (2018) *Mobile money competing with informal channels to accelerate the digitisation of remittances*, available at http://bit.ly/2KcHqAH

[11] Cash-in is process of exchanging cash for electronic value, what is often known as 'e-money', and cash out is the process of exchanging electronic value/e-money to cash. AFI (2016) *Digital Financial Services Basic Terminology,* available at https://bit.ly/2fipB9g

[12] The Association of Certified Anti-Money Laundering Specialists (ACAMS) defines AML as: 'The system designed to assist institutions in their fight against money laundering and terrorist financing. At a minimum, the AML program should include (a) written internal policies, procedures and controls (b) a designated AML compliance officer; (c) on-going employee training; and (d) independent review to test the program. See ACAMS (2018) *AML Glossary of Terms*, available at https://www.acams.org/aml-glossary/

[13] Financial Intelligence Units are often also known as the 'AML Unit' (AMLU) or the Financial Intelligence Agency (FIA), and are usually independent state bodies with their own powers of investigation, but which in some cases may be a division within the central bank.

[14] ML refers to the conversion or transfer of property or any association, knowing it is derived from criminal activity, for the purpose of hiding its origins, nature, location, disposition, movement, ownership. Similarly, TF is the provision or collection of funds to contribute to the commission of specific offences while in complete knowledge that they are being used or will be used for such purposes. Summarized from EIB (2018) *Anti-Money Laundering and Combating Financing of Terrorism Framework,* available at https://bit.ly/2HX4QMH. See also CGAP (2005) *AML/CFT Regulation,* available at http://www.cgap.org/publications/amlcft-regulation; and IMF (2018) *Anti-Money Laundering/ Combating the Financing of Terrorism (AML/CFT)*, available at https://www.imf.org/external/np/leg/amlcft/eng/

[15] ACAMS defines KYC as: 'AML policies and procedures used to determine the true identity of a customer and the type of activity that is "normal and expected," and to detect activity that is "unusual" for a particular customer.' ACAMS (2018) *AML Glossary of Terms*, available at https://www.acams.org/aml-glossary/

known as procedures for customer identification and verification (CIV).[16] These CIV procedures are in turn usually part of what is known as customer due diligence (CDD)[17] requirements. CIV and CDD are procedures, principles and processes that stem from efforts by national regulators and supranational Standard Setting Bodies (SSBs) such as the Financial Action Task Force (FATF)[18] to prevent and identify ML and TF. Local regulators will set these AML/CFT policies and principles that what are generally known as 'reporting institutions' – such as banks and DFSPs - must follow when dealing with customers and risk fines and other limitations on their activities if they do not.

Customer Identification and Verification (CIV) is the 'modern' catch-all description for identifying, verifying and undertaking due diligence on customers. Although FATF largely discarded the term 'KYC' in its documents onwards from 2003,[19] KYC as the overall descriptor for CIV and related processes is still firmly embedded in the minds of national regulators, compliance officers, industry associations,[20] academic works,[21] and customers.[22]

Distinguishing between and outlining the relationships between, AML, CDD, CIV, and KYC is best shown through the final rule[23] issued by the US FIU, FinCEN. The rule describes its ideal AML program as including four core elements of CDD: (a) CIV (b) beneficial ownership identification and verification, (c) understanding the nature and purpose of customer relationships to develop a customer risk profile; and (d) ongoing monitoring for reporting suspicious transactions and, on a risk-basis, maintaining and updating customer information.

[16] CIV is also known as 'Customer and beneficial owner identification and verification' in some jurisdictions. CIV may involve identification data such as a person's full name; date of birth; ID number; nationality; and residential address. Some countries may also require additional information such as contact details, profession or occupation, source of funds, or tax number (depending on country context). See Finmark Trust (2015) *AML/CFT due diligence and related matters*, available at https://bit.ly/2S8NP47

[17] ACAMS defines CDD in terms of ML controls, as requiring 'policies, practices and procedures that enable a financial institution to predict with relative certainty the types of transactions in which the customer is likely to engage. CDD includes not only establishing the identity of customers, but also establishing a baseline of account activity to identify those transactions that do not conform to normal or expected transactions.' As part of CDD, providers it says should identify and verify the customer's identity using reliable and independent sources; identify and verify the beneficial owner so as to know whether they are the actual parties of interest; obtain information on the purpose and intended nature of the business relationship; assess the risks associated with the business relationship; monitor transaction to check if it is consistent with the knowledge of the customer, their business and risk profile and conduct ongoing due diligence. FATF (2012) *The FATF Recommendations,* available at https://bit.ly/1e7w0Gl. Similarly, but in the context of financial inclusion, CGAP says CDD 'involves identifying a client and verifying the client's identity by checking his or her identity documentation or data and, where appropriate, conducting background and beneficial ownership checks. Clients are then profiled and their transactions are monitored to identify discrepancies that may trigger a suspicious transaction report to be filed with the country's FIU.' See Lyman, T & de Koker, L (2018) *KYC Utilities & Beyond: Solutions for AML/CFT Paradox?*, available at https://bit.ly/2OqOgso. See also Exhibit 1 outlining the FinCEN view of the differences and interconnectedness between KYC, CDD, and CIV and their relationship to an AML program.

[18] FATF is an inter-governmental body that sets standards and promotes effective implementation of legal, regulatory and operational measures for combating ML, TF and other related threats to the integrity of the international financial system. Its 'Recommendations' relate to financial and non-financial institutions. FATF (2018) *About,* available at http://www.fatf-gafi.org/about/. FIUs will usually create principles for AML and CIV based on principles from FATF and within a country conext.

[19] Lyman, T & de Koker, L (2018) *KYC Utilities & Beyond: Solutions for AML/CFT Paradox?*, available at https://bit.ly/2OqOgso

[20] See also AFI (2013) *Risk-based Approaches to AML/CFT: Balancing financial integrity and inclusion*, available at https://bit.ly/2S6yHnX

[21] For example, de Koker, L (2014) *The FATF's customer identification framework: fit for purpose?,* available at https://bit.ly/2S8QZF2; and Arner, D; Zetzsche, Buckley, R *et al.* (2018) *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*, available at https://ssrn.com/abstract=3224115. See also FATF (2012) *The FATF Recommendations,* available at https://bit.ly/1e7w0Gl

[22] The terminology communicated by banks, MNOs and other financial providers such as DFSP to their customers when they sign up for services mostly refer to 'KYC' as the identity-verification descriptor.

[23] FinCEN (2016) *Customer Due Diligence Requirements for Financial Institutions*, available at https://bit.ly/2ySJMQS

In many cases CIV or CDD are conflated with 'KYC' to mean the same thing, whereas KYC is now considered to be only but one - the identity input - component of a CIV procedure[24] that, in turn, is part of the ongoing[25] CDD process.[26] All of these components together form part of an AML/CTF program for all covered financial institutions.[27] Similarly, the capture and use of biometric data of citizen, resident or scheme participants for general identification purposes and specifically for AML purposes has assumed the moniker eKYC.

eKYC refers to the electronic means to conduct customer identification and allow online and/or digital verification of the customer's identity. When biometric-based, eKYC may require capture of the customer's biodata, which may include fingerprints, facial, voice and iris scans. Similarly, an identity with electronic and/or biometric components to it is known as an electronic ID (eID).[28]

There is often a distinction made between eID and digital IDs, or the terms are used interchangeably as essentially a distinction without a difference. To be consistent and importantly to maintain the link to eKYC focus of this Note, this Note uses the term eID as to represent the electronically (digitally) captured and stored - and not solely physical[29] - representation of an ID and the biographical data therein, unless noted otherwise. In the use cases described in this Note, the eID will always have a biometric component to it.

Exhibit 1: A Word on Identity and AML-related Terminology

There is however a significant 'identification gap' in the developing world, with some 1.5 billion people lacking proof of legal identity.[30] The proof could be a birth certificate, or a document or ID issued by a sectoral authority that indicates that the holder

[24] For Southern African Development Community (SADC) countries, the verification of customer identity data may involve use of independent (external) sources such as an address validation and verification service; bank statement; cellular or telephone account; credit reference agency, insurance policy; lease or tenancy agreement; national database or register; personal visit to the home of the applicant; rates or utility bill; reference from a bank; reference from customary authority; reference from known customer of bank; reference from well-known professional/government official; reference or affidavit from an employer; revenue service; telephone book; and television license. See Finmark Trust (2015) *AML/CFT due diligence and related matters*, available at https://bit.ly/2S8NP47

[25] Authorities, the financial sector and other designated entities – such as lawyers and real estate agents – must provide what are known as 'suspicious transaction reports' (STRs) to the FIU if activity that could indicate ML or TF is suspected by that entity. Suspicious activity may be irregular or questionable customer behavior or activity that may be related to ML or other criminal offense, or to the financing of a terrorist activity. It may also refer to a transaction that is inconsistent with a customer's known legitimate business, personal activities, or the normal level of activity for that kind of business or account. See ACAMS (2018) AML Glossary of Terms, available at https://www.acams.org/aml-glossary

[26] Where contextually required, the distinction between the terms KYC, CIV, CDD will be highlighted. See further on terminology used in the context of financial transactions and ML. See de Koker, L (2014) *The FATF's customer identification framework: fit for purpose?,* available at https://bit.ly/2S8QZF2; and Watts, D, Medine, D & De Koker, L (2018) *Customer Due Diligence and Data Protection: Striking a Balance,* available at https://bit.ly/2KKJAHk; Lyman, T & De Koker, L (2018) *KYC Utilities & Beyond: Solutions for AML/CFT Paradox?*, available at https://bit.ly/2OqOgso

[27] An effective AML program, FinCEN says, should include (i) a system of internal controls; (ii) designation of an AML-focused compliance officer (iii) training; (iv) testing and auditing; that CDD-covered institutions understand the nature and purpose of relationships so as to develop a customer risk profile, conduct ongoing monitoring for reporting suspicious transactions, and, using a risk-based approach, maintain and update customer information. FinCEN (2016) *ibid.*

[28] Electronic ID (eID) is a form of identification used for online or offline identification process often in the form of a photo-card with an embedded chip that contains information. Some eIDs can contain biometric information and are often referred to as Smart Identity Cards (SIC) described in Exhibit 4. MicroSave (2017) *Progress and Challenges with KYC and Digital ID,* available at https://bit.ly/2teQXAN; and World Bank (2018) *Principles On Identification For Sustainable Development: Toward The Digital Age*, available at https://bit.ly/2mgZktJ

[29] The physical representation of the electronically captured and stored data may also be in the form of a SIC.

[30] Identity is a set of attributes that uniquely describes an individual or entity. World Bank (2018) *Principles On Identification For Sustainable Development: Toward The Digital Age*, available at https://bit.ly/2pZWkBY. The UN's Sustainable Development Goals (SDGs) aims to achieve 'legal identity for all, including birth registration' by 2030. See 'Target 16.9' of the UN SDGs, available at https://sustainabledevelopment.un.org/sdg16. As the World Bank notes, identification is also a key enabler of Target 1.3 (implementing social protection systems), 1.4 (ensuring that the poor and vulnerable have control over

is that same person. With fake IDs though, attestation – a higher forms of verification – is unlikely. eKYC and eIDs usually are able to provide that required attestation of the veracity of the holder's ID by an issuing authority.

Without legal and acceptable means to identify themselves, some 20% of the financially excluded are unable to access DFS facilities because they lack the necessary proof of identity documentation mandated by regulators for opening financial services accounts[31] and for obtaining mobile SIM cards.[32]

As noted by WEF[33] and others,[34] there is the need to disentangle the terms 'legal identity,' 'citizenship,' 'identification,' 'registration' and 'ID documentation.' We agree, but such an exercise is beyond the scope of this paper, which will simply refer to these concepts per their colloquial use, and within the framework of CIV processes and the need to address AML/CFT concerns.

Data from the World Bank's ID4D program[35] shows that of the over 1 billion people without an official proof of identity 81% live in Sub-Saharan Africa and South Asia; that 47% are below the national ID age of their country, highlighting the importance of strengthening birth registration efforts and creating a unique, lifetime identity; that 63% live in lower-middle income economies, while 28% live in low-income economies, which the World Bank say reinforces the fact that lack of identification is a critical concern for the global poor.[36] Also, over 45% of women lack a foundational ID compared to 30% of men.[37]
The forms of identity that are available and which may be acceptable for CIV purposes for SIM card and/or DFS registration range from 'analogue' physical paper or laminated cards, and documents or booklets that contain the CIV-required information, to electronic versions of these documents in the form of a card, or more advanced versions with the customer's biometric data – usually their fingerprints – stored on a smart chip embedded on the card.[38] Other multi-modal biometric parameters such as iris scans or palm prints may be stored on remote server controlled by a central authority that enrolled the citizen, resident or customer as the case may be. The capture – as an eID - and use of biometric data of citizen, resident or scheme participants for CIV purposes and specifically for AML/CFT purposes is commonly referred to as eKYC.

---

land, property, and financial assets), 5a (giving poor women equal access to economic resources, including finance), 5b (enhancing the use of technology, including ICT to promote women's empowerment), 10.7 (safe and responsible migration and mobility), 10c (reducing the cost of remittance transfer), 12c (phasing out harmful fuel subsidies), 16a (strengthening the capacity to fight terrorism and crime), 16.5 (reducing corruption). The World Bank also notes that there are national and international effects involving donors and private-sector partners to strengthen legal identification systems, including civil registries, national IDs, population databases, voter registries, social transfer databases, and travel documents. World Bank (2018) *Principles Of Identification For Sustainable Development: Toward The Digital Age,* available at https://bit.ly/2pZWkBY.

[31] World Bank (2018) *The Global Findex Database 2017,* available at https://globalfindex.worldbank.org/

[32] Where an MNO also acts as a DFSP, a 'basic' – that is, limited in transaction balances, transfer and frequency - transactional DFS account is often provided automatically to a customer on their sign-up for a mobile SIM card. Additional documentation provided later by the customer may remove these initial DFS-related limitations. See also World Bank (2018) *ibid*.

[33] WEF (2015) *What is the future of legal identity?*, available at https://bit.ly/2J9Bg4t

[34] Dahan, M & Gelb, A (2015) *Role of Identification in the Post-2015 Agenda, Center for Global Development,* available at https://bit.ly/2ytboMP

[35] The ID4D program operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and legal issues. It brings global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems. See World Bank (2018) *About Us*, available at http://id4d.worldbank.org/abouts-us

[36] See World Bank (2018) *ID4D Data: Global Identification Challenge by the Numbers*, available at http://id4d.worldbank.org/global-dataset.

[37] World Bank data from 2015 showed the vast majority of 198 countries its surveyed have fragmented, single-purpose ID systems. In particular, 8% have no eID; 12% have an eID used for identification only; 72% eID used for one or more services; and 7% have fully integrated, multi-purpose ID systems. See World Bank (2015) *Identification for Development (ID4D) Integration Approach*, available at https://bit.ly/2xPv51Z. A similar study in 2018 showed that 42% of 198 countries surveyed collected some biometric data such as fingerprint or iris. The World Bank's ID4D data also indicates that countries with the greatest gender gaps in 'foundational' ID coverage also tend to be those with legal barriers for women's access to ID. In Afghanistan, Benin, and Pakistan, for example, a married woman cannot apply for a national ID in the same way as a married man. See Desai, V (2018) *The global identification challenge: Who are the 1 billion people without proof of identity?*, available at http://tinyurl.com/ydfps6zq

[38] Cards with biometric information stored on them are often known as Smart ID Cards (SICs). See Exhibit 4.

In many country cases, the means – analogue and/or electronic - to identify and verify the person is issued by a national authority or agent, but this may not include a centralized, single identifier. That is, there is no national ID number that permanently identifies that person to the state and others in perpetuity. Often there is no such authority to issue that national ID number or physical representation thereof, either because of public-policy considerations[39] or due to a lack of infrastructure and/or capacity to capture citizen/resident data, and then issue national ID numbers and associated ID documents. The former situation is characteristic of some developed countries[40] where citizens believe such centralization will violate their privacy and the latter of many developing countries.[41]

Frustration with central government initiating issue of a unified, single national ID has however given rise to various authorities and agencies issuing their own eIDs, initiating their own CIV/eKYC programs. For example, telecommunications regulators and MNOs[42] for SIM card registration; the national electoral authorities for voting; transport authorities for driver's licenses; and a central bank for access to financial service. The disparate and non-interconnected systems – although critical for each of their own ecosystems - complicate AML/CFT efforts as often only some of these are acceptable forms of ID for financial transaction-related CIV. As they each become entrenched into their own system with their own procedures and technical standards, harmonization of the individual ecosystem biometric databases becomes ever more difficult and costly.[43] The World Bank estimates that there is USD 50 billion in potential annual savings by 2020 for governments that adopt nationwide, single eID systems.[44]

In many cases, eKYC systems that use an eID could be the critical input mechanism for centralized but shared facilitates that improve customer sign-up times and quickly detect incidents of ML and fraud. The eKYC[45] programs and systems that have been launched and described here have overarching goals to advance a person's access to services, reduce identity fraud, and increase financial inclusion. Country examples and challenges – *inter alia*, policy, legal, security, design, financial and infrastructural - in the rollout are discussed below.

It is to be noted that there are also attempts by private sector actors to develop so-called self-sovereign IDs[46] where a person will self-enroll to obtain a digital token or representation of their identify using recently-developed blockchain-type[47] Distributed Ledger Technologies (DLTs) protocols. It is however trite that in most cases acceptance by financial institutions – and regulators - of these IDs for account opening and CIV purposes is largely still lacking and are likely to be so for a number of years as the technology matures. Many of the newest private-sector innovations in ID using DLTs are gaining better traction and acceptance though, when a person is required to provide ID credentials connected to an official, trusted, state-issued identity.[48]

---

[39] See Section 4.2.1 on legal issues surrounding national IDs and eKYC.

[40] For example in the UK and Australia where there are no national ID systems mostly due to resistance from the public.

[41] See Section 4.2.1 on legal issues surrounding national IDs and eKYC.

[42] As occurs in Tanzania where the MNOs share a common eKYC enrollment for mandatory SIM card registration platform using smartphones and biometric capture devices.

[43] See below in the case of Ghana (see Section 5.2), where harmonization of nine separate databases has complicated efforts as a single NIDB system. In Nigeria (See 5.6), the government announced in September 2018 that of the various biometric databases, only the central bank controlled biometric database would be acceptable. For its new national ID database.

[44] Dahan, M & Sudan, R (2015) *Digital IDs for Development:* A*ccess to Identity and Services for All,* available at http://hdl.handle.net/10986/22297.

[45] The ID4D program indicates that there are 161 countries with ID systems 'using digital technologies.' This is not the same as eKYC, and only refers to the digital technology used for capture and storage of data. In this context, eKYC is deemed to include a process of biometric capture and storage of individual user data. See World bank (2018) *ID4D Data: Global Identification Challenge by the Numbers*, available at http://id4d.worldbank.org/global-dataset

[46] Self-sovereign digital identities are created and managed by individuals, and enable them to maintain their digital identities independent from residence, national eID infrastructure and market-dominating service providers. See Der, U; Jähnichen, S & Sürmeli, J (2017) *Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution*, available at https://arxiv.org/pdf/1712.01767

[47] For an overview of blockchain and DLTSs, see Perlman, L (2017) *Distributed Ledger Technologies and Financial Inclusion*, available at https://bit.ly/2nyxpBG

[48] See www.civic.com, described below and the GSMA's M4D Digital Identity program. The latter program works with the mobile industry, governments and the development community to explore the role and potential of the mobile industry in both

2. THE ROLE AND IMPACT OF THE FINANCIAL ACTION TASK FORCE (FATF)

As noted above, FATF is the global SSB underpinning and driving all supranational AML/CFT efforts. Over time it has issued standards on measures countries should implement to combat ML, TF and financing of proliferation of weapons of mass destruction (PF).[49] Core to the FATF scheme is the need to identify those engaged in financial transactions and if needed, monitor their activities if any ML or TF activities are suspected.

Initial standards issued by FATF relating to what is now known as DFS were however often seen as too restrictive[50] given the low values often involved as well as the systemic lack of identity infrastructure in countries attempting to increase financial inclusion.[51] In an attempt to ensure that AML/CFT provisions it promoted do not unduly hinder access to formal financial services to the underserved and unbanked, it issued a 'guidance' in 2013[52] to balance, it hoped, both financial inclusion and AML/CFT objectives. It introduced what is now known as FATF's risk-based approach (RBA).[53] RBA affects several different aspects of CIV and CDD processes in AML/CFT for financial inclusion environments by having as its *grundnorm* the premise that risk management and mitigation measures should be proportionate to the identified and assessed risks. Another FATF guidance relating to financial inclusion was also issued in 2017[54] as a supplement to its 2013 Guidance.

As part of a RBA, the country's FIU must conduct a national risk assessment based on surveys and assessments of its financial sector and other ecosystems which may pose a ML risk. Appropriate RBA rules and regulations must follow, or existing rules and regulations updated if needed. The report must be submitted to FATF. Peer groups will also visit the country as part of FATF's mutual evaluation program[55] to assess levels of implementation of the FATF Recommendations, and to provide an in-depth description and analysis of that country's approach to and system for detecting and preventing criminal abuse of the financial system, which includes CIV processes. The peer review group will follow FATF's 'M*ethodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems,'* which sets out how the FATF will determine whether a country is sufficiently compliant with the 2012 FATF Standards and whether its AML/CFT system is working effectively. If any deficiencies are found – in the visit and in the national risk assessment – the country could

state-led and private-sector led digital ID offerings. See Wilson, M (2016) *Digital Identity: a prerequisite for Financial Inclusion?*, available at https://bit.ly/2PMHjhX

[49] The FATF framework is composed of the 1) FATF Recommendations; (AML/CFT) standards, and methodologies to assess the effectiveness of AML/CFT systems. See Arner, D; Zetzsche, Buckley, R *et al* (2018) *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*, available at https://ssrn.com/abstract=3224115. See also FATF (2012) *The FATF Recommendations,* available at https://bit.ly/1e7w0Gl.

[50] Non-risk based approach to AML/CFT safeguards both in the onboarding stage and ongoing relationships when providing financial services. FATF (2017) *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence*, available at https://bit.ly/2taubZM

[51] See for example Financial Action Task Force (2012) *International Standards On Combating Of Money Laundering And The Financing Of Terrorism And Proliferation: the FATF Recommendations* available at https://bit.ly/1e7w0Gl; FATF's Recommendation 10 read with its Interpretative Note sets out the requirements regarding customer identification and verification. For detailed commentary on these 2012 Recommendations, see de Koker, L (2014) *The FATF's customer identification framework: fit for purpose*? Available at https://bit.ly/2S8QZF2

[52] FATF (2013) *Guidance For A Risk-Based Approach Prepaid Cards, Mobile Payments And Internet-Based Payment Services*, available at https://bit.ly/2jEAiAl

[53] FATF (2017) *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence*, available at https://bit.ly/2taubZM

[54] *ibid.*

[55] As of June 2018, FATF says it has reviewed over 80 countries and publicly identified 65 of them as being high-risk. Of these 65, 55 have since made the necessary reforms to address their AML/CFT weaknesses and have been removed from the process. See FATF (2018) *High-risk and other monitored jurisdictions*, available at https://bit.ly/1RA355J

be labelled as one of FATF's categories of 'risk'[56] and be monitored by FATF, but is usually given a period to correct any deficiencies.[57] If these are not fixed, sanctions or restriction on integration into the world's financial system may follow.

3. CUSTOMER IDENTIFICATION AND VERIFICATION METHODOLOGIES AND FINANCIAL INCLUSION

3.1 CDD Processes That Enhance Financial Inclusion Efforts

FATF issued another guidance relating to financial inclusion in 2017[58] as a supplement to its 2013 Guidance. The 2017 document noted that[59] CDD requirements can often act as barriers to financial access and acknowledged that ML/TF risks may be relatively lower for financial products and services that provide appropriately defined and limited services to certain types of customers. Based on the level of risk of a product offering, offeror or offeree, countries should do an assessment as to what products can be offered - and by whom - and what level/type of identification is required. A 'tiered'[60] CDD approach may be used (in DFS). As such, where the ML risk is assessed to be low, simplifying AML/CFT, identity and CDD requirements may be possible. This is known as Simplified CDD (SDD).[61] Access to the basic, first level set of services may be provided upon minimum identification,[62] and depending on the extent and acceptance of identification provided and verification thereof performed by providers,[63] customers may be given access to more services and allowed to hold higher balances, and transact at higher values and with more frequency.

Because DFS involves lower transactional value and volumes,[64] it may be styled as 'low risk' and hence allows SDD requirements for access to DFS compared to that for opening bank accounts. Some countries have implemented SDD practices in lower risk cases that successfully align with financial integrity and financial inclusion policy objectives.[65] In 2015 in Peru

---

[56] The *Methodology* is available at https://bit.ly/1MoYVaY. The level of compliance with each FATF Recommendation will be indicated with one of the following ratings: compliant, largely compliant, partially compliant or non-compliant. The effectiveness assessment will assess the extent to which a country achieves a defined set of outcomes that are central to a robust AML/CFT system and will analyze the extent to which a country's legal and institutional framework is producing the expected results.

[57] A FATF Eastern and Southern Africa Anti-Money Laundering Group mutual evaluation report of Uganda in February 2014 found deficiencies in its AML/CFT programs. These included deficiencies in its FIU, the DFS/Mobile Money operations and lack of AML-related regulations. It then placed Uganda on the 'high risk' category. Uganda addressed the concerns by *inter alia* amending its Financial Institutions Act to make its FIU the central agency for receiving STRs, issuing and implementing regulations for the freezing of terrorist assets, issuing AML regulations for implementation of AML requirements, and issuing AML/CFT inspection manuals for financial sector supervisors. It was removed from monitoring by FATF in 2017.

[58] FATF (2017) *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence*, available at https://bit.ly/2taubZM.

[59] FATF (2013) *Guidance For A Risk-Based Approach Prepaid Cards, Mobile Payments And Internet-Based Payment Services*, available at https://bit.ly/2jEAiAl.

[60] Also called a progressive approach.

[61] SDD is characterized by a simplified CDD process for customers with a low risk profile. Less information or less robust verification of the customer's identity and their intentions behind the business relationship may be required or verification may be postponed. It can ease difficulties for people to access financial services. FATF (2014) *Guidance for Risk-based Approach: The Banking Sector,* available at https://bit.ly/1thpYyY. The 2017 FATF *Supplement* provides country examples of simplified CDD (SDD) measures adapted to the context of financial inclusion. Those examples illustrate how SDD can support both financial inclusion and financial integrity policy objectives, especially where supported by alternative forms of identity verification, for example the use of e-identity tools. See FATF (2017) *Guidance On AML/CFT Measures and Financial Inclusion, With A Supplement on Customer Due Diligence*, available at https://bit.ly/2wLMObN

[62] FATF (2017) *ibid*

[63] FATF (2017) *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence*, available at https://bit.ly/2taubZM

[64] MicroSave (2017) *Progress and Challenges with KYC and Digital ID,* available at https://bit.ly/2teQXAN

[65] South Africa in 2008 implemented an SDD for banks providing low value products. Known as 'Exemption 17,' it was intended to simplify identification and verification requirements for low value products. It was withdrawn in 2017 ostensibly because SDD-type procedures are included implicitly in the modifications to AML legislation which requires a risk-based approach that allows an accountable institution to determine which business relationships or transactions pose a lower ML/TF risk and apply the necessary CDD requirements as described in the institution's risk management and compliance policies. See

for example, SDD measures were authorized by the banking supervisor (SBS)[66] for specific product and services.[67] Use of just the national ID number is sufficient for opening a basic DFS account: providers had to only collect the full name, and type and number of the ID document of the customer, with the verification done through the National ID, or passport for foreigners. The conventional CDD involved provision of their nationality, residence, phone number and/or e-mail address, occupation and name of employer of that person.

SDD however requires moderation: in particular, circumstances and risk profiles of customers and services may change, requiring a reassessment of whether an SDD process still fulfils financial integrity goals.[68] If the assessment of a service or person shows medium or high risk, it would not be appropriate to apply SDD and other simplified AML/CFT measures.[69] SDD measures will also not be applicable if there is any suspicion of ML or TF. In high risk circumstances – such as where politically exposed persons (PEP) are considered – what is known as enhanced due diligence (EDD)[70] may be required.

Specific requirements for 'tiered' access to DFS account features vary by country but usually involve provision of designated forms of ID: for locals, residents and citizens, this may be a type of ID issued by an authority in that country as well as proof of recent address. Or for foreign visitors, it may be their passport, a passport-style picture, as well as a copy of an entry stamp or visa.[71]

Following the 'tiered' approach', DFS accounts can also often then be obtained when providing documentation when obtaining a SIM card.[72] These DFS accounts opened contemporaneously and automatically when a new customer obtains a SIM card and mobile phone number are often known as 'basic' accounts[73] They are however characterized by significantly limited transaction capabilities[74] such as transaction restrictions, limited account value storage, as well as limited agent-related CICO and Over-the-Counter[75] transactions. Further documentation and attestation of the customer's identity may be required to increase transaction and account storage limits.[76] In such 'low risk' cases, a notional, state issued ID would be sufficient for critical

---

FIU (2017) *Draft Withdrawal Notice Of Exemptions In Terms Of Financial Intelligence Centre Act, 2001, Published For Public Comment*, available at https://bit.ly/2Pg8aG4

[66] La Superintendencia de Banca, Seguros

[67] SBS Resolution N° 2660-2015 implemented the integral risk management system for enterprises under the supervision of the SBS. This Resolution is applicable to all banking and financial institutions under the scope of the SBS. See PwC (2016) *Know Your Customer: Quick Reference Guide*, available at https://pwc.to/2ijumjA

[68] It has been noted that criminal abuse patterns change and risk levels of products assessed as lower risk may increase over time, especially where criminals start to exploit simplified controls. See De Koker, L (2009) *The Money Laundering Risk Posed by Low-Risk Financial Products in South Africa: Findings and Guidelines*, available at www.emeraldinsight.com/journals.htm?articleid=1817094. FATF says that post-implementation assessments should be done to determine whether in practice, the risks were actually lower, the SDD measures were appropriate, and the effect of SDD on financial inclusion goals. FATF (2017). See also AFI (2013) *Risk-based Approaches to AML/CFT: Balancing financial integrity and inclusion*, available at https://bit.ly/2S6yHnX

[69] FATF (2017) *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence*, available at https://bit.ly/2taubZM

[70] EDD is usually an additional due diligence process on top of the 'standard' CDD for high risk customers. It may involve obtaining additional identifying information from a wide variety or more robust sources, commissioning an intelligence report, verifying the source of funds or wealth involved in the business relationship, seeking additional information from the customer about the purpose and intended nature of the business relationship. FATF (2014) *Guidance for Risk-based Approach: The Banking Sector,* available at https://bit.ly/1thpYyY

[71] This is the case in India for CDD for foreigners buying SIM cards.

[72] AFI (2018) *Digital Financial Services,* available at https://bit.ly/2IuOBGW

[73] Gelb, A (2016) *Balancing Financial Integrity with Financial Inclusion: The Risk-Based Approach to 'Know Your Customer',* available at https://bit.ly/2MiLXlU

[74] MicroSave (2017) *Progress and Challenges with KYC and Digital ID,* available at https://bit.ly/2teQXAN

[75] A transaction that the agent conducts on behalf of a sender or recipient or both from the sender's or agent's mobile money account. ITU (2016) *Over the Counter Transactions: A Threat to or a Facilitator for Digital Financial Ecosystems?,* available at https://bit.ly/2ywZrbA

[76] SIM registration may sometimes be sufficient to open a DFS account that does not allow cash-out, but additional CDD is required for full functionality. In some countries, the number of DFS accounts also may be limited. In Jordan for example, a user may only have two DFS accounts, even though they may have multiple mobile numbers and SIMs. Gelb, A (2016)

DFS-related SDD: that is for SIM card registration or their replacement and for DFS sign up at agents and bank branches.[77] Since some 1 billion of the world's 1.7 billion unbanked adults own a mobile phone, the use of SIM registration data for DFS sign up can potentially increase access to financial services.[78]

3.2 The Need for Robust Identity Systems

SDD – and effective CDD generally for that matter - is dependent on access to reliable and timely customer data, especially for CIV purposes. This may include the ability to verify identity documents, awareness of any red flags for certain customers or classes of customers, and checking for incidences of 'smurfing'[79] and other suspicious behaviors.[80]

As noted by FATF,[81] one of the main obstacles to providing financial services is the lack of reliable or standardized ID and poor processes to verify these IDs as part of a CIV processes. The issue of standardization is particularly acute in countries where there is no national ID system – that is, where there is no standard, persistent, unified, verifiable ID number attached to a person - and where the process of identification needs to navigate a verifiable identity tower of babel. Usually multiple, disparate authorities will issue their own ID documents that can be used as ID for some, but not all (financial) services. These may include interior ministries issuing passports and voter IDs, or transport departments issuing driver's licenses. It becomes a huge challenge for those – especially smaller DFSPs with limited resources for compliance - required to do CIV to collect and validate identity documents generated by other and multiple government departments.[82] Insufficient data to identify and assess risks of such customers raises costs and risk for providers, making it less profitable, if at all, to try to provide services to the financially excluded. The effect is even more pronounced for those in rural areas or who work in informal sectors, as they may not have a formal proof of ID or other CIV-related documents such as proof of address to begin with.[83] In essence and in large measure, those without IDs deemed sufficient for onboarding for DFS cannot become customers of DFSPs.

3.3 Electronic Identification Methods and eKYC

It is trite that 'analogue' IDs and processes that accept them can easily be gamed by bad actors using fake IDs.[84] In many cases, a fake ID can be bought cheaply on web sites that specialize in such goods. There are however emerging digital initiatives to systematize and standardize ID issuance, management and use. These innovations in identity management – which have assumed the industry-wide moniker of eIDs - may help address these concerns and assessments.

FATF has largely endorsed[85] the use of eIDs and other emerging electronic identity tools and innovative fintech solutions to support financial inclusion while simultaneously mitigating ML/TF risks and fraud. This is particularly impactful for AML/CFT purposes where the eID is used in eKYC where - as noted earlier – it includes a systematic method to use captured biometric data of citizen, resident or scheme participants for CIV purposes.

Balancing Financial Integrity with Financial Inclusion: The Risk-Based Approach to 'Know Your Customer,' available at https://bit.ly/2MiLXlU

[77] Where DFS is provided by MNOs, and where biometric data captured during the SIM registration is stored on a central server and can be accessed and verified, this registration data can be used as a proof of identity – that is KYC – for DFS services offered by that MNO, where the customer gives consent for their ID to be used. This seamless use of the stored identity may of course not be in place where the DFS is provided by a non-MNO third party and where the database is not online.

[78] Findex (2018) *The Global Findex Database 2017,* available at https://bit.ly/2A9LNtu

[79] The breaking down large amounts for transfer into smaller amounts to avoid detection by authorities.

[80] For example 'smurfing'.

[81] FATF (2017) *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence*, available at https://bit.ly/2taubZM

[82] This is especially so where proper infrastructure and capacity to produce these documents is lacking.

[83] FATF (2017) *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence*, available at https://bit.ly/2taubZM

[84] Failure to confirm customers' information could allow registrations with other person's IDs and the mismatch of the customer's photos with the one on the ID.

[85] FATF (2017) *Guidance On AML/CFT Measures and Financial Inclusion, With A Supplement On Customer Due Diligence*, available at https://bit.ly/2wLMObN

Jordan has since 2016 embarked on a process of issuing citizens over 18 with a new, secure 'smart' identity (ID) card (SIC), replacing the laminated civil ID card. The sign-up process for the SIC at Jordan's Civil Status and Passports Department is relatively easy, affordable and fast. It includes capturing facial, iris and fingerprint data, and takes less than 15 minutes. The SIC currently stores 18 data fields such as gender; the person's name in Arabic and English; place of birth; area of residence; and blood type. Other fields such as drivers licenses, health insurance, and 'keys' for the citizen's electronic signature (e-signature) are reserved for later implementation and anticipated general commercial usage. In addition to the new SIC,[86] a range of other government-issued ID documents are accepted in the financial sector for CIV purposes and for sign-up to the JoMoPay DFS switch.[87]

Exhibit 2: Jordan's eKYC System using A Smart Identity Card

For eID acquisition and eKYC use, the basic procedure starts with enrollment involving in-person capture as the case may be of a person's biographical details and biometric details by an authority and/or agency.[88] In some cases a private entity may capture the biographical and biometric details for eKYC purposes.[89] Users need to register their demographic and, in some cases, biometric data with the authority/agency. Enrollment centers are usually established for document authentication and capturing of biometric data. Initial implementations have involved capturing fingerprints and/or iris scans for registration and usage purposes. Where the entity is a state organ or its agent, captured information may be stored in a national population registry or national ID database (if such exists), which financial institutions and MNOs can use to verify the identity of their customers.

Even where there is no national ID, some biometric-based eIDs may serve as a *de facto* national ID because of their degree of acceptance across financial institutions and businesses.[90] In Nigeria for example, the Central Bank of Nigeria's Bank Verification Number (BVN) is a biometric-based card that is mandatory for all bank account holders.[91] India's Aadhaar eKYC system[92] – seen as the global eID archetype – has over 1.21 billion users who have signed up using biometric identifiers. The system however was dealt a huge blow in a September 2018 court ruling that banned its (mandatory) use in a swathe of activities, including SIM card registration and CIV for financial institutions.[93]

In Australia – where there is no national ID – the government's Digital Transformation Agency[94] is developing an eID called myGovID for access to, initially, end-to-end digital Tax File Number application process. Under the scheme, users will opt in and create a digital identity by giving 100 points of ID, and uploading a 'selfie' for checking against passport or driver license photos. Other providers will be also able to provide the service. The solution uses biometric matching to documents issued by trusted Australian third parties such as driver's license and passports. The credential is a device based authenticator app, paired with native authentication - such as a fingerprint - or password.

Similar eID systems are being developed, but where the biometric identifier is facial recognition. Facial recognition will be the centralized biometric authenticator that will be used across both government and private sector applications in the new Singapore national ID, called the National Digital Identity (NDI) program to be issues free for all citizens.[95] DLT

[86] Jordanian e-Government (2017) *Jordan Smart Card*, available at https://jordan.gov.jo/wps/portal/Home/SmartCard
[87] These include the legacy laminated card, passports issued to Jordanians and those from the West Bank and Gaza, refugee documents, military ID cards, and foreign passports with proper immigration stamps or visas. Each ID document usually contains a unique ID number.
[88] For example the UNCHR at refugee camps using its (independent) IrisGuard biometric capture system. UNHCR (2017) *Executive Committee of the High Commissioner's Programme*, available at http://www.unhcr.org/59ca231b7.pdf
[89] As occurs with the MNOs in Tanzania.
[90] MicroSave (2017) *Progress and Challenges with KYC and Digital ID,* available at https://bit.ly/2teQXAN
[91] See further 4.3 below.
[92] See 4.2 below.
[93] Economic Times (2018) *Payments companies asked to stop Aadhaar-based services*, available at http://www.ecoti.in/tfgiUb
[94] Digital Transformation Agency (2018) *Digital identity for people*, available at https://bit.ly/2EDQost
[95] AVISIAN (2018) *Singapore national ID to include facial recognition*, available at https://shar.es/a18G3l

(blockchain) type self-sovereign ID systems such as Civic[96] are also gaining traction using so-called zero-knowledge proofs.[97] Here, users sign up to the Civic platform with a 'selfie' picture and a copy of an ID – such as a driver's license - issued by a state or authority. In Thailand, the central bank changed its AML laws to allow a fintech company participating in its regulatory sandbox to take remote copies of IDs for CIV purposes.[98] In China, SIM cards can be obtained by foreigners at airports by simply holding up their passport to a video camera on a SIM-dispensing kiosk operated remotely by a MNO agent.

And while not usually acceptable for CIV purposes, so-called federated IDs using Facebook, Amazon or Google account logins are gaining traction for seamless identification for web services. It is not inconceivable that these 'techfin'[99] companies may obtain approval to use their IDs in some future CIV environment as a substitute for an ID issued by an authority. Public policy considerations may however limit their scope and use of any user data.[100]

Exhibit 3: Alternative IDs for use in eKYC Processes

eKYC though is a relatively new phenomenon, with some of the first implementations worldwide used for customer identification purposes during registration for or obtaining replacement mobile SIM cards.[101] For example, when a user requests a new SIM card, the service provider uses an authorized biometric reader, or a card reader authorized by a regulator or the ID agency to authenticate the information with the central database as means to fulfill CIV requirements. Usually, at the least, the capture device has a license number allowing it be used for that purpose. Costs for technology and new APIs for Iris capture using smartphones have allowed capture stations to proliferate.[102]

While implementations vary, most of the eKYC systems pivot around biometrics for customer sign-up and verification procedures and usually involve biometric fingerprint capture and/or an iris scan, or in case of Singapore's the National Digital Identity, facial recognition.[103] Few others also use facial recognition, a still-evolving technology. In most cases, at a minimum the registrant will get an eID which requires just their fingerprint or iris scan for identification, verification and authentication.[104] In some cases, the eID will be twinned with a smart ID card (SIC) containing at the very least, biographical data of the person, some or all of their fingerprints, and a compressed version of their headshot. While a picture of the holder and their ID number are printed and stored on the SIC, due to storage size limitations on most SICs, the high resolution iris image files are not stored.[105]

[96] See www.civic.com
[97] Venture Beat (2017) *What Zero-Knowledge Proofs Will Do For Blockchain,* available at https://bit.ly/2k4XLwk
[98] See Wechsler, M; Gurung, N & Perlman, L (2018) *The State of Regulatory Sandboxes in Developing Countries*, available from www.dfsobservatory.com
[99] These are technology companies who have branched out into financial services. For use of the term, see Zetzsche, D, Buckley, R. Arner, D *et al.* (2017) *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, available at https://ssrn.com/abstract=2959925
[100] SMH (2018) *Govpass on brink of becoming the next Australia Card debacle: report,* available at https://bit.ly/2AfqZ47
[101] For example in Bangladesh, where fingerprint registration is required to obtain a SIM card. See the Bangladesh Telecommunications Regulatory Commission on its biometric verification system linked to the national ID or foreigner passport, available at https://bit.ly/2PRO2rb
[102] An API was issued for Aadhaar-based iris capture in India.
[103] The Singapore government will provide software development kits to industries such as banking and finance, for connecting their services to NDI. AVISIAN (2018) Singapore national ID to include facial recognition, available at https://shar.es/a18G3l
[104] Some scholars differentiate between eID and what they term in the context of their work on a digital finance, 'digital identities.' Digital IDs may mean something else in another context. Arner *et al* say a legal identity they say is external and personal and summarizes who someone is, while a physical or behavioural identity is internal and interactive and defines who someone is. eID's would represent in large measure the former and have relatively static legal identifiers such as physical features, birth data, along with some biometrics. A 'digital ID' they say would have the eID features but may be more advanced and critical to the development of a digital finance ecosystem. It could possibly include dynamic or behavioural identity features such as the holder's status in the community, akin to the social identity scores being used in China. They recognize however that such systems – while technically feasible – may not be politically feasible in many countries.
[105] Iris images would exceed the 144kb available storage.

The more technologically advanced eKYC systems – such as Aadhaar in India and those in South Africa - will have a robust online component to either verify all the data (and the person presenting a SIC or fingerprint) on and in the SIC in real-time. The central database then will in real-time attest to the veracity of the SIC data and the identity of the person.

If there is no online component – possibly because of infrastructural, policy[106] and design issues, or temporary loss of connectivity - then use of a SIC with an approved card reader and corresponding screen, or a simple USB-based single fingerprint (digit) reader will give the local verifier a view of the data on the card and ability to visually confirm – with reasonable certainty - that the person presenting themselves is the person whose data is on the card.[107]

4. BENEFITS AND CHALLENGES WITH ELECTRONIC IDENTIFICATION AND EKYC

An eID's three security functions - identification, authentication, and electronic signature – are primarily used to detect identity fraud and ML/TF, but can also create a reliable online infrastructure not just limited to CIV but also for other CDD processes and for access to future e-Government (eGov) services, government-to-person payments, aid disbursements, and tax filings.[108] There are however still a number of challenges in eID and eKYC implementations.

4.1 Benefits of eKYC Use

4.1.1 Reduction of Fraud

India's Aadhaar has foreclosed on fraudulent access to subsidy rolls and financial accounts via multiple identities and opportunity to streamline the delivery mechanism of welfare programs, and support transparency and good governance.[109] The September 2018 court ruling restricting Aadhaar use may however significantly alter that utility.

4.1.2 Financial Inclusion

The new trend of using eIDs - especially biometric identifiers linked to national ID numbers - has supported digitization of previously time-consuming, costly and cumbersome CIV processes. This paperless verification process for new customers is the basis for eKYC and can promote efficient onboarding of customers through real-time or quicker verification of customer identity by DFSPs.[110] eIDs are hence replacing paper (analogue) ID cards and booklets in a number of jurisdictions. Provision of attested forms of state issued ID is critical for DFS and financial inclusion and can prevent incidents of de-risking by ventilating the identity of those with beneficial ownership of received funds. Loss of remittance income from de-risking actions can affect digital liquidity in DFS and damage financial inclusion efforts.

Aadhaar in India's almost universal adult coverage eases the ability to verify their identities and open accounts.[111] The 2018 'State of Aadhaar' report indicated that 84% of people used Aadhaar as proof of identity to open their most recent bank or DFS-type account.[112] It has also enhanced the coverage and, hence, usefulness of the Indian national credit bureau that has allowed more access to credit and financial products by Indian citizens.[113] A court ruling restricting Aadhaar use in September

---

[106] In Jordan for example DFSPs do not currently have real-time access to the central database housing biographical and biometric data, such that all identity verification is done locally and offline. Only some Jordanian banks have direct, real-time ability to verify a person based on the credentials presented to them.

[107] The picture and fingerprints stored on the SIC can be viewed and recognized/verified offline with an approved card reader, and online with the registration body using the approved reader. In Jordan, this device must be approved by the Ministry of ICT, even if used for verification on behalf of another agency or regulator. In India, the device must be approved by UIDAI.

[108] Gemalto (2017) *Gemalto to Supply New Digital Identity Solution for the Swedish Tax Agency,* available at https://bit.ly/2yyM2zH; Deloitte (2016) *Picture Perfect: A Blueprint for Digital Identity,* available at https://bit.ly/2aOblg1; UNHCR (2016) *UNHCR Cash Assistance*, available at https://bit.ly/2Mfowtq; GSMA (2013) *Mobile money: The Opportunity for India,* available at https://bit.ly/2ts5eub

[109] IMF (2018) *Financial Inclusion in Asia-Pacific*, available at https://bit.ly/2PWoPvh

[110] Barman, N & Saraswathy, M (2013) *e-KYC Set to Benefit Banking, Financial Services Sectors,* available at https://bit.ly/2MgIHr9; Development Asia (2017) *Using Digital Technology to Reach the Unbanked in Southeast Asia,* available at https://bit.ly/2yzyHqG

[111] Raman, A (2018) *India Moves Toward Universal Financial Inclusion*, available at https://bit.ly/2POahhF

[112] See the '*State of Aadhaar' report from the UIDAI*, available at https://bit.ly/2R6HPYi

[113] IMF (2018) *Financial Inclusion in Asia-Pacific*, available at https://bit.ly/2PWoPvh

2015 may however significantly alter its utility. Similarly, in Bangladesh, eKYC has facilitated improved monitoring of borrowers' credit quality since use of national identity card and authentication via eKYC is mandatory for access to credit.[114]

4.1.3 Access to Government Services

Digitization can reduce risks of fraud, identity theft and misplacement of documents, and reduce the overall cost of CIV processes.[115] Once functional and at a critical user mass, eIDs and eKYC processes can also be used for purposes other than just opening DFS and bank accounts, and mobile SIM card registration. India's Aadhaar has acted as the basis for development of eGov services and an integrated digital infrastructure for use by multiple state entities.[116] It can be used in village-level computer kiosks around India that help citizens access common e-governance services such as pensions and student scholarships.[117]

4.1.4 Gateway to KYC Utilities

When CIV is coupled with other CDD processes, implemented as sanctions screening,[118] transaction limit checks,[119] and velocity checks,[120] eKYC can also contribute to the development of what is known as a 'KYC Utility.'[121] These are usually centralized facilities owned by industry or government or in partnership that allow service providers and regulators to obtain and verify customer information in real-time, to monitor for fraudulent activities and to aggregate customer information for ML detection purposes.[122] While implementing a national KYC Utility infrastructure will share costs across all participants, it may however be costly and take time to implement and perfect.[123]

4.2 Challenges in eKYC Use

---

[114] *ibid.*

[115] Development Asia (2017) *Using Digital Technology to Reach the Unbanked in Southeast Asia,* available at https://bit.ly/2yzyHqG; Puttanna, S (2016) *Digital KYC: A Key to Transform*, available at https://bit.ly/2K6NpH5; Taylor, E (2018) *Digital Onboarding and KYC: Aligning the Interests of Consumers, Businesses and Regulators,* available at https://bit.ly/2K6LDFP

[116] Sharwood, S (2017) *India Makes Biometrics Mandatory for All e-gov Projects,* available at https://bit.ly/2qaeDqD; Security Identity Alliance (2014) *The Role of Trusted Digital Identities in Enabling the eGovernment 2020 Vision,* available at https://bit.ly/2MO2b7g; Edwards, M (2017) *Paving the Way for Digital Identities and Mobile eGov Access,* available at https://bit.ly/2mSsFva

[117] Huffington Post (2018) *UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm*, available at https://bit.ly/2CPdTgf

[118] Check sanctions, blacklists and geography of users to identify risks for the service providers authenticating the identity of the user and the regulators monitoring the financial sector.

[119] Limits could be monitored to ensure that the user is not exceeding them.

[120] Smurfing is a common phenomenon where financial transactions are broken down and executed in a specific pattern to avoid raising suspicion of money laundering. Frequency can thus be monitored and high frequency and/or identifiable patterns of financial transactions using DFS could trigger suspicious activity alerts.

[121] The concept of a 'KYC Utility' is commonly considered to be a central repository that aim to streamline the collection and exchange of data between member institutions, while maintaining appropriate privacy controls. While a KYC Utility may be commercially used for the purpose of CIV, the KYC Utility model can encompass the full range of CDD obligations and can extend benefits to both the private and public sector. A type of Utility has been established in South Africa. Powered by Thomson Reuters 'Org ID' as 'KYC-as-a-service,' three large national banks provide their customers with unique login keys to the Utility for provision of documents that would form part of a KYC by the major banks. The Utility undertakes KYC on the customer. The customer can choose which of these documents it wishes the Utility to share it with, and with whom. Org ID is also available in n the UK, Poland, and Malaysia. See Thomson Reuters (2016) *Strong Growth for KYC Managed Service Org ID*, available at https://tmsnrt.rs/2P7TybP; and also PwC (2015) *Share and Share Alike: Meeting Compliance Needs Together With A KYC Utility,* available at https://pwc.to/2IOl7Aa; CITI (2014) *Know Your Customer Utilities,* available at http://citi.us/2HtqUvy; Lyman, T & De Koker, L (2018) *KYC Utilities & Beyond: Solutions for AML/CFT Paradox?*, available at https://bit.ly/2OqOgso

[122] Perlman, L & Gurung, N (2018) *Use of Regtech by Central Banks and its Impact on Financial Inclusion,* available at dfsobservatory.com

[123] For more on the practicalities of a KYC Utility, see Lyman, T & de Koker, L (2018) *KYC Utilities & Beyond: Solutions for AML/CFT Paradox?*, available at https://bit.ly/2OqOgso

The availability of national IDs issued by a national agency/authority, usually the Interior Ministry or National Identification Authority,[124] and whether the identity documentation being used can be validated against a government registry, either at point of sale or at point of activation, has a significant bearing on the registration solution.[125] Other considerations apply relating to legal certainty of the eKYC solution(s) employed, security of customer data, privacy and data protection considerations, the transition period from analogue (physical) ID documents to eID solutions and the degree and duration of their continued validity.

4.2.1 Legal Certainty

Legal certainty is critical in embarking on eID and eKYC programs, especially if harmonization and integration of various identity databases is required as part of (creating) a national ID database. This process requires clear legal frameworks and delegation of responsibilities to the contributing authorities or agencies who control part or all of each component database. This has been the case for example in Nigeria, where use of the central bank–mandated biometric bank verification number (BVN) has been marked by legal challenges by the National Identity Management Commission (NIMC) who contested[126] the right of the central bank to register citizens using biometric information and to issue the BVN. The NIMC claimed sole rights to undertake biometric registrations and verifications. An agreement was reached[127] however to harmonize BVN database with that of the new National Identity Database (NIDB). The government has said that from 1 January 2019 that use of the new National ID number – and not the BVN – will be mandatory and that up to December 1 2018,[128] only qualified databases with biometric eKYC will be eligible for harmonization. The NIMC has said that only data captured by banks through BVN registration have met the standard required for use with the new NID. New data will be required to conform to the NIMC biometric standards for the NID.

There have also been legal issues and challenges around Aadhaar in India, with the project and the enabling legislation under review for constitutional validity by the Supreme Court with regards to aspects of privacy, personal autonomy, and surveillance state.[129] A September 2018 ruling by the Supreme Court confirmed the constitutional validity of Aadhaar and emphasized that it does not violate the right to privacy of individuals.[130] But while the Court allowed some government-facing uses such as tax filing, it prohibited the mandatory use of Aadhaar for bank CIV and registration for SIM cards.[131] Financial and telecommunications providers have now reverted to use of the physical Aadhaar card for basic, visual-only identification of the holder, since they now do not have the ability to undertake any additional electronic verification. Similarly, in Afghanistan, use of the e-tazkira eID/eKYC system was halted because of controversy over whether to include ethnic identity and opposition from ethnic leaders.

4.2.2 Capital and Operational Costs

Establishing eID and eKYC systems can be costly: India's Aadhaar system has since its establishment in 2009 cost some USD 1.5 billion up to September 2018, with annual costs – operational and capital – averaging some USD 42 million per year.[132] As suggested by the World Bank,[133] public-private partnerships (PPP) that will create revenue flows and ensure sustainability are important method for governments to reduce the initial financial burden of establishing and running an eID and eKYC system.

---

[124] This is entity responsible for developing a national ID system, issuing ID and attesting to true ownership when presented for authentication purposes to third parties and government services.

[125] GSMA (2016) *Mandatory Registration* of *Prepaid SIM Cards*. *Addressing Challenges Through Best Practice*, available at https://bit.ly/2rx7NKs

[126] Communications Week (2014) *NIMC, CBN at Loggerheads over BVN Scheme*, available at https://bit.ly/2PIiunb

[127] Pierre Biscaye, Sarah Coney, Eugenia Ho, Brian Hutchinson, Mia Neidhardt (2015) *Review of National Identity Programs*, available at https://bit.ly/2EFgs6B

[128] New Telegraph (2018) *Only BVN data useful for national database –NIMC*, available at https://bit.ly/2CZh98X

[129] Livemint (2018) *Aadhaar Legal Validity: SC Constitution Bench to Commence Hearing Today,* available at https://bit.ly/2KaTZ2t

[130] For Supreme Court of India judgment, see https://bit.ly/2OM50Gx*;* Livemint (2018) *Supreme Court Verdict on Aadhaar: Constitutionally valid, doesn't violate privacy,* available at https://bit.ly/2CKBDlT

[131] Economic Times (2018) *Payments companies asked to stop Aadhaar-based services*, available at http://www.ecoti.in/tfgiUb. For the Supreme Court of India judgment, see https://bit.ly/2OM50Gx*;* Livemint (2018) *Supreme Court Verdict on Aadhaar: Constitutionally valid, doesn't violate privacy,* available at https://bit.ly/2CKBDlT

[132] See UIDAI (2018) *Finance and Accounts*, available at https://uidai.gov.in/about-uidai/about-uidai/financials.html. The depreciation of the Indian Rupee versus the US Dollar masks the high local-currency cost.

[133] Dahan, M & Sudan, R (2015) *Digital IDs for Development: Access to Identity and Services for All. Transport and ICT connections,*, available at http://hdl.handle.net/10986/22297.

This however should not transfer as high registration costs for the public for eIDs and high costs for providers to access eKYC systems as it can quench critical use.

Aadhaar uses a PPP model,[134] where 'enrollment centres' are paid per successful registration.[135] Each enrollment centre requires at a minimum requirement licensed biometric scanners, a laptop, a printer, a web camera, a GPS dongle, reliable power supply, a document verifier, operators and a supervisor.[136] The cost to a merchant for buying a UIDAI-certified fingerprint reader is around USD 60. Enrollees are charged a fee for enrollment in some areas. One study suggested that Aadhaar enrollment costs overall would decrease to under USD 3 per enrollee if no physical card was issued.[137]

4.2.3 Design Elements

A lesson in the impact of design imperatives on usability and security of an eID/eKYC system can be drawn from constant and high-profile intrusions into India's Aadhaar system which, expert reports suggest, originated from a 2010 design decision to democratize enrollments by allowing private agencies to enroll users using official, standardized enrolment software called the Enrolment Client Multi-Platform.[138] This decision resulted in the placement of the enrollment software on every computer used for enrollment, rather than a cloud-based eKYC as a service solution used by MNOs in Tanzania for SIM card registration.[139]

Due to cost and logistical implications, decisions also need to be made many years in advance of launches of ID system upgrades, such as whether to undertake multimodal biometric capture; that is whether all or combinations of iris, face, palm, and fingerprint, or even voice - biometrics should be captured during enrollment. Some systems – such as that being developed in South Africa – are replacing manual enrollment processes with automatic systems that remove the need to manually notify users and to fill out and wet-sign forms for enrollment and use of eIDs. The design and type of eID companion card is also critical to eventual use, for example whether there is a smart chip embedded (and its memory capacity), whether digital signatures will be stored on the card, which biographical details will be printed on it, the actual size of the card and international and regional compatibility.[140]

4.2.4 System Continuity

The core of an eKYC CIV process is to be able to undertake real-time verification from a central database of a person. This requires persistent connection to the central server of the attestation body, be that a national ID authority or a central bank. Fallback mechanisms for when connectivity is down or where there is scarce internet connectivity is required.

4.2.4 Security of Systems and User Data

---

[134] Participants in the enrolment process include the UIDAI, registrars (state and central government organisations, banks, or private entities) enrolment agencies; Enrolment operators; and residents who are enrolled in the program. Some commentators indicate that a successful enrolment - that is, generation of Aadhaar number - will pay the operator between USD 0.54 and USD 0.82. Deductions for process errors during enrolment are between USD 2 and USD 6.80. See Venkatanarayanan, A (2018) *Aadhaar enrolment costs*, available at https://link.medium.com/6mLphTddbR.

[135] Economic Times (2017) *Government okays Rs 2,000 crore to set up Aadhaar units in post offices*, available at http://www.ecoti.in/W-PTqb

[136] Venkatanarayanan, A (2018) *Aadhaar enrolment costs*, available at https://link.medium.com/6mLphTddbR

[137] Pierre Biscaye, Sarah Coney, Eugenia Ho, Brian Hutchinson, Mia Neidhardt (2015) *Review of National Identity Programs*, available at https://bit.ly/2EFgs6B

[138] Huffington Post (2018) *UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm*, available at https://bit.ly/2CPdTgf

[139] The Tanzanian system captures text based information, images, ID documents and signature and uses facial and ID recognition technology built-in to improve quality of data. It is also optimized to work on the lowest end photo-capable smartphones.

[140] In many countries, the ID-1 card specification is used for ID/eID cards.

Given its size and the value of the information in it, the eponymous Aadhaar system in India has come under sustained attack[141] which has led to leaking of registrant details,[142] creation of multiple fake Aadhaar numbers,[143] as well as disabling of the enrollment software's GPS security feature. Another hack reduced the sensitivity of the enrolment software's iris-recognition system, making it easier to spoof the software with a photograph of a registered operator, rather than requiring the operator to be present in person, while another allows the bad actor to user bypass critical security features such as biometric authentication of enrolment operators to generate unauthorized Aadhaar numbers.[144]

As mentioned earlier, the hacks and spoofs originated from a 2010 design decision to democratize enrollments by allowing private agencies to enroll users using official, standardized enrolment software called the Enrolment Client Multi-Platform (ECMP).[145] The Aadhaar Android app has also been hacked.[146] Even providers have been seen to compromise eKYC systems: MNO and DFSP Airtel apparently undertook diversion of USD 25 million in gas subsidies for the poor to the Payments Bank accounts of its mobile phone subscribers.[147] Its Aadhaar 'master key' was temporarily revoked by UIDAI as a result. Vulnerabilities are constantly being fixed as they are identified, but to maintain user confidence in the system, UIDAI launched a Virtual ID (VID) number, a temporary, revocable 16-digit random number mapped with the Aadhaar number that can be used for the authentication in the same way the Aadhaar number is used.[148]

4.2.5 Privacy and Data Protection Considerations

Ensuring data protection and privacy when dealing with large volumes of eID and eKYC data is a major issue which is under discussion in many jurisdictions, including India following the hack of the Aadhaar database.[149] Similarly in Mexico, where the mandatory SIM registration program was marred by concerns on the privacy and security of the database. The program and database there was scrapped in 2012.[150]

There are also still many countries, especially developing nations, without comprehensive data protection laws.[151] In Asia, 14 nations[152] have comprehensive privacy laws and a few other countries such as China and Indonesia have enacted other laws and regulations that have impacted data protection.[153] In Africa, only 23 out of 55 countries have passed or drafted personal

---

[141] India Times (2018) *French Cyber Expert Cracks Official Aadhaar App In 1 Minute, Realizes UIDAI's Worst Nightmare,* available at https://bit.ly/2MfmEAX; The Tribune (2018) *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details,* available at https://bit.ly/2E4qEjK

[142] Huffington Post (2018) *UIDAI Aadhaar Hack: New Analysis Shows Hackers Changed Enrolment Software Code In 26 Places*, available at https://bit.ly/2PdgXst

[143] NewIndianXpress (2018) *26-year-old Bihari man created fake Aadhaar Cards for Bangladeshi nationals*, available at https://goo.gl/UDjm11

[144] Huffington Post (2018) *UIDAI Aadhaar Hack: New Analysis Shows Hackers Changed Enrolment Software Code In 26 Places*, available at https://bit.ly/2PdgXst

[145] Huffington Post (2018) *UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm*, available at https://bit.ly/2CPdTgf

[146] BT India (2018) *Aadhaar data: French hacker exposes flaws in its Android app, asks people not to use it*, available at https://bit.ly/2OEKGuR

[147] NDTV (2017) *Airtel Payments Bank To Return Rs 190 Crore Cooking Gas Subsidy*, available at https://bit.ly/2R75sjr

[148] Aadhaar holders can regenerate a VID multiple times. It is valid for a minimum of one day, there is no expiry period, and it is valid until the next generation of a VID. See Economic Times (2018) *What is VID?*, available at https://bit.ly/2R9K3q5

[149] India Times (2018) *French Cyber Expert Cracks Official Aadhaar App In 1 Minute, Realizes UIDAI's Worst Nightmare,* available at https://bit.ly/2MfmEAX; The Tribune (2018) *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details,* available at https://bit.ly/2E4qEjK

[150] Watts, D, Medine, D & De Koker, L (2018) *Customer Due Diligence and Data Protection: Striking a Balance,* available at https://bit.ly/2KKJAHk; GSMA (2016) *Mandatory Registration of Prepaid SIM Cards*, available at https://bit.ly/2rysm90

[151] DLA Piper (2018) *Data Protection Laws of the World,* available at https://bit.ly/2k0dA73; Deloitte (2017) *Building Trust Across Cultures,* available at https://bit.ly/2KsPcGh

[152] Australia, Hong Kong, India, Japan, Kazakhstan, Kyrgyzstan, Macao, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Taiwan, and Turkmenistan

[153] Rich, C (2017) *A Look at New Trends: Privacy Laws in East, Central, and South Asia and the Pacific,* available at https://bit.ly/2tFQdUK

privacy laws and only 9 of them have specific data protection authorities.[154] New technologies like DLTs/blockchain using for example zero-knowledge proofs[155] may allow secure encryption, storing, transfer and authentication of national identification data but regulatory provisions for data protection and privacy are also necessary to safeguard users and address concerns of privacy and data security for eKYC.[156] The digital locker concept is India is a reasonably elegant similar solution that empowers users to control use of their personal data, although there have been concerns about the privacy implications of allowing users to download their Aadhaar use history, which includes any update relating to name, date of birth, gender or address, or addition/deletion of mobile numbers or email addresses.[157] The concern is that the data may fall into the wrong hands given that Aadhaar has been compromised a number of times.[158]

Similar privacy concerns have been raised regarding the centralized GovPass eID/eKYC system in Australia, with one major report indicating that there are weak legislative protections, a lack of attempts at communicating the changes to the public, and the potential for the ID to "turbocharge" how private companies gather details about customers, all of which could mire the system in controversy.[159] The government though has said that the scheme will protect personal details with a design that forces agencies to verify identity through a hub that stops them from accessing the data used to cross-check information.

4.2.6 Regulatory and Business Coordination

The roll out of eID and the subsequent eKYC for DFS requires regulatory coordination. In some countries, CIV procedures for DFS are different for MNOs and financial institutions because usually SIM card registration is under the mandate of the telecommunications regulator[160] and any DFS registration is under the AML/CFT mandate and rules of the central bank,[161] and/or an FIU.[162] Because fiat money – rather than airtime value – is involved in the DFS wallet, ML/TF concerns relating back to FATF AML/CFT requirements are applicable, and Tier limits as part of a RBA are often set by the central bank and/or FIU.

In some cases, registrations have been largely successful, although there may be huge capital investments necessary to create a national database and remove duplicate identities to develop a single identification - as seen in Nigeria.[163]

Coordination failure amongst regulators to provide licenses for individual eKYC biometric capture devices, design APIs and integration into a national database often means that eKYC undertaken for SIM card provision is not usable for sign-up for DFS, possibly wasting an opportunity to leverage the same information across multiple platforms. In one extreme case, coordination failure between a national ID authority, the telecommunications regulator and the central bank resulted in millions of customer being cut off from access to their DFS accounts.[164] In Uganda in 2017 and 2018, lack of coordination amongst DFS-related regulators as well as technology failures led to expensive effects on the society and the economy, with DFS users

---

[154] Dahir, A (2018) *Africa isn't Ready to Protect its Citizens Personal Data Even as EU Champions Digital Privacy,* available at https://bit.ly/2rzHN0b

[155] Venture Beat (2017) *What zero-knowledge proofs will do for blockchain,* available at https://bit.ly/2k4XLwk

[156] World Economic Forum (2016) *A Blueprint for Digital Identity,* available at https://bit.ly/2aOblg1; Insurance Journal (2018) *Data Privacy Risks as Digital Identity Moves to Biometrics, Blockchain,* available at https://bit.ly/2Kb7qQ1

[157] NDTV (2018) *Aadhaar Update History Feature Now Available to Download*, available at https://bit.ly/2Jl2JUo

[158] Huffington Post (2018) *UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm*, available at https://bit.ly/2CPdTgf.

[159] See ASPI (2018) *Preventing another Australia Card fail*, available https://bit.ly/2NJfi9i

[160] In Tanzania in September 2017, 6 MNOs were together fined a record USD 5 million by the Tanzania Communication Regulatory Authority (TCRA) for registering new SIM cards for subscribers whose IDs were questionable, and others could not be traced in the database. The TCRA also indicated that there were other irregularities such as were failure to confirm customers' information, allowing registrations with other person's IDs and the mismatch of the customer's photos with the one on the ID.

[161] The Central Bank through its preferred CIV process for AML may specify which forms of ID are acceptable for initial registration of a DFS account. The degree of transactional ability will also be determined by the Central Bank based on the degree of identity verification determined through the authenticating documents the customer provides.

[162] The FIU may set policies for AML/CFT purposes, either as general principles or as specific guidelines. FIU policies may be implemented by repowering entities such as the CB and NTA, who may need to report back to the FIU as part of FATF-mandated National Risk Assessments.

[163] Tarpael, F (2017) *FG to Harmonize BVN, Others into National Identity Database*, available at https://bit.ly/2yxAufX

[164] See 4.5 below on Uganda.

unable to access their funds.[165] Coordination is hence needed not just for a legal framework to use national IDs but also for technical and financial feasibility for service providers to use a common database for eKYC.

Similarly, over-bearing - or uncoordinated - CIV requirements issued by some regulators as part of the mandate may unintentionally exclude vulnerable and socially disadvantaged consumers.

4.2.7 Transition Periods and Carve Outs

There may also be certain exceptions to eID and eKYC verification and monitoring systems during periods of harmonization of programs where there are multiple forms of identification issued by multiple authorities involved. It may take many years for eKYC infrastructure and systems to be nationally available and for physical IDs – such as ID booklets, family books and laminated cards - to expire or be declared invalid by national government at a date certain. Birth certificates, passports, health cards, voter cards, driver licenses, and even physical non-smart ID cards should all still be valid and be considered for KYC/eKYC purposes if possible while new eID and eKYC systems are rolled out.[166] Similarly, tourists who use their passports to obtain SIM cards also often cannot be verified in real-time, nor are they subject to restrictions on the number of mobile phone lines they may obtain. They may potentially give their mobile phone lines to others who are not able to obtain lines (for example, those on a security blacklist), or to citizens trying to circumvent the restriction on the use and number of mobile phone lines that can be registered in their name.[167]

4.2.7 Coordination of Regional Efforts

There are also some regional efforts to undertake digital IDs and CDD across borders as seen in the East African Community (EAC) - Kenya, Uganda and Rwanda – where the 'One Area Network' was launched to develop a uniform policy on SIM card registration.[168]

5. COUNTRY EKYC IMPLEMENTATIONS AND FINANCIAL INCLUSION

As noted above, various eKYC implementations around the world have a nexus between SIM card registration and DFS account provision. These types of eKYC systems are in place or planned in *inter alia* Bangladesh, Ghana,[169] India, Nigeria, Pakistan, Uganda, and Jordan, with varying degrees of success. Some eKYC implementations revolve around the use of a single national eID, while other eIDs may be specific to a sector.

Country	First Operational	DFS Use	Notable Features & Challenges
Bangladesh	2015	In progress	eID is mandated by the Bangladesh Telecommunication Regulatory Commission for SIM card registration and re-registration. The Bangladesh Bank is also developing an eKYC system for financial services.
Ghana	2017	Yes	Ghana Card is the national eID which has been recently updated to a 128kb SIC with tactile elements for the blind, iris-capture capabilities and all 10 fingerprints of an applicant. The new SIC will provide organizations with data sharing, personal information verification, online identity validation and biometric verification services.

[165] New Vision (2017) *Telecom firms given 72 hours to deactivate SIM card*s, available at https://shar.es/1Pemkq; Article 19 (2017) *Uganda: SIM Card Registration Requirements Must Respect Fundamental Rights,* available at https://bit.ly/2K93MTJ

[166] In Ghana for example, although 98% of Ghanaians have at least one form of ID, banks and DFSPs need to have processes in place for processing nine separate ID databases in use across the various government agencies. BFA (2017) BTCA Ghana Country Diagnostic, available at https://bit.ly/2ysfBka; and AKROFI–LARBI, R (2015) *Challenges of National Identification in Ghana*, available at https://bit.ly/2Ja03FH

[167] In Jordan, the planned TRC SIM card biodata enrollment will reportedly capture the fingerprints of foreigners using passports for SIM card registration may provide greater security.

[168] Standard Kenya (2015) *EAC Banks On Regional SIM Card Law to Curb Insecurity*, available at https://bit.ly/2rCflui

[169] Biometric IDs are issued by the National Identification Authority. Ghana began re-registration of SIM cards in November 2017. Modern Ghana (2017) *Ghana to Witness Massive Re-registration of SIM Cards from November*, available at https://bit.ly/2rx7NKs

India	2010	Yes	Aadhaar system collects biometric and demographic data of residents, which is stored in a centralized database. Using the eKYC service, residents can authorize service providers to access their demographic data and photograph from the database using biometrics or password. There have however also been multiple security breaches of the Aadhaar system, raising questions of data privacy and protection.
Jordan	2016	Yes	Department of Civil Status and Ministry of Information and Telecommunication Technology introduced national eID along with a SIC containing biographical data, fingerprints and iris scans (except in the SIC). In 2018, the Telecommunication Regulatory Commission also mandated the collection of biometric data for SIM registration.
Malawi	2017	Yes	Within 180 days, around 9.1 million citizens out of 16 million were registered for the national eID, while 3.6 million children were registered alongside their parents. The total cost of the project was around USD 52 million.
Pakistan	2015	Yes	The Telecommunication Authority mandated the verification of all SIM card owners using biometric information linked to their NIC number. SIM registration was later allowed to satisfy KYC requirements for mobile money account set up, making it easier for people to access mobile money services.
South Africa	2016	Yes	SIC with a person's photograph, full name, date and place of birth, fingerprint and unique ID number replaced bar-coded identity books. The government in 2018 launched its Automated Biometric Identification System project that integrates all systems and offer a single source for biometric authentication for citizens.
Uganda	2017	Yes	UCC has made multiple attempts to require verification of all SIM cards using proper identification documents but it has been affected by conflicts between MNOs, the UCC and the government over deadlines for registration and availability of required ID documents. UCC, in different occasions, banned the sale of new and replacement SIM cards until the national ID and database was fully integrated into the CIV processes for SIM registration and also switched off unregistered SIM cards. While both actions were lifted, they prevented users from accessing their DFS accounts for that period.
UNHCR	2015	Yes	UNHCR, as its own eKYC system, uses a combination of iris scans,[170] document (passport, national ID, military cards or family books) authentication and interviews. The documents are checked for authenticity and interviews are conducted to capture biographical info of family members on the database. The iris data of adults in a family is also captured and stored. If there are any doubts or suspicions regarding the identity of the individuals/family, further investigation is conducted. Otherwise, they are given refugee/asylum status and they can use UNCHR financial services using their biometrics.

Exhibit 4: Selected eID and EKYC implementations used for CIV for financial services

5.1 Bangladesh

The Bangladesh Telecommunications Regulatory Commission mandated biometric identification for new and existing SIM card holders.[171] Mobile phone providers hence required biometric verification devices that were linked to the National Identity

[170] This uses the UNHCR's IrisGaurd iris capture system.

[171] InterMedia (2017) *Bangladesh, Wave 4 Report, FII Tracker Survey,* available at https://bit.ly/2y2Wvmv; Bdnews24.com (2016) *Deadline for Biometric Re-registration of SIM Cards Extended by a Month,* available at https://bit.ly/2thSdmy

Card (NIC) database of the Election Commission.[172] This initiative is expected to have increased the percentage of adults who own a SIM card by nearly 20% and thus those with mobile money accounts by 7% since you need a SIM card in your own name to get a DFS account. [173] Along with a SIM card number, customers must also submit either a copy of their National ID Card, citizenship certificate, driver's license, or passport to obtain a DFS account.[174]

These requirements can be automatically fulfilled in cases where DFS is provided by MNOs using the SIM registration data-providing opportunities for MNOs like Banglalink to easily on-board customers for DFS.[175] The Bangladesh Bank is also expected to introduce eKYC system for both banks and DFS.[176] Using eKYC, users can open accounts but will only be allowed to perform limited-scale agent banking and DFS transactions.[177] Bangladesh Bank is also planning on introducing eKYC,[178] allowing enrollees to operate limited-scale transactions through the agent banking network and DFSPs,[179] and then later, through banks. Current CIV is using the national identity card linked to the NIDB.

5.2 Ghana

Ghana has had a national identification program since the 1970s, and augmented this with a national eID card – the Ghana Card – which is provided to all citizens and resident non-Ghanaians. The Automated Fingerprint Identification System (AFIS) is the core platform technology for the NIS. A biometric-based unique ID system was started in 2006, but reportedly had modest success[180] and initially did not conform to international standards issued by ISO and the International Civil Aviation Organisation.

A revamped National ID launched in September 2017[181] is a 128kb SIC with tactile elements for the blind, and iris-capture capabilities as well as now taking all 10 fingerprints of an applicant. The storage capacity of the SIC will enable other participants to run their applications using SIC. The government plans to replace all the sectorial ID cards in circulation, with the Ghana Card ultimately becoming the only card that can be used in transactions where an ID is required. It will provide organizations with data sharing, personal information verification, online identity validation and biometric verification services. The services are regulated by National Identification Authority under the National Identity Register Act.[182]

5.3 India

Without formal ID, many Indians struggled to open a bank account and in response, the government launched Aadhaar in September 2010,[183] now considered the world's largest national identification number project and operated by the Unique Identification Authority of India (UIDAI). Aadhaar uses biometric capture devices to collect biometric and demographic data of residents, which is stored in a centralized database. Each enrollee is provided with a 12-digit unique 'Aadhaar number.'[184] Aadhaar is not proof of Indian citizenship, the person can simply be a resident. The UIDAI also provides eKYC service through which residents can authorize service providers to access their demographic data and photograph from the UIDAI database using biometrics or password.[185] As a privacy and anti-fraud mechanism, Aadhaar registrants can also check online who has used their data.[186]

---

[172] Mayhew, S (2015) *Biometrics Registration for SIM Cards in Bangladesh Starts Wednesday,* available at https://bit.ly/2trT2J3

[173] Those who shared or rented a SIM card were forced to register their own. FII (2017) *Financial Inclusion in Bangladesh Receives a Mobile Money Boost: Insights from the 2016 FII Data,* available at https://bit.ly/2ohdBWL

[174] USAID (2015) *Mobile Money Tipsheet,* available at

[175] Islam, M (2016) *Banglalink Keen to Expand Mobile Financial Service,* available at https://bit.ly/2K07Jhl

[176] Uddin, Z (2018) *Electronic KYC by June,* available at https://bit.ly/2lqy6OE

[177] *ibid.*

[178] *ibid.*

[179] Enrollees will be able to transact up to Tk 20,000 per month through a DFSP and Tk 1 lakh through agents.

[180] BTCA (2017) *Building an Inclusive Digital Payments Ecosystem: The Way Forward*, available at https://bit.ly/2AmwrSw

[181] Modern Ghana (2017) *Ghana Launches New National ID Card*, available at https://bit.ly/2ECOus7

[182] NIA (2008) *National Identity Register Act of 2008*, available at https://bit.ly/2CvL8V8

[183] ITU (2017) *Aadhaar: India's route to digital financial inclusion*, available at https://news.itu.int/SDPSP; Your Story (2017*) History of Aadhaar: How Nandan's core team came together,* available at https://bit.ly/2Eu98KE

[184] For more information on Aadhaar and UIDAI, see https://www.uidai.gov.in

[185] IndiaStack (2018) *About eKYC API,* available at http://indiastack.org/eKYC/

[186] A history feature provided by UIDAI allow Aadhaar users to download details of all the updates they have made to their Aadhaar data, such as change of address. Another allows users to download details of where and when their Aadhaar number

In 2013, Reserve Bank of India announced that the eKYC from UIDAI is sufficient to open accounts in financial institutions.[187] The government had also made it mandatory to verify and link all financial institution accounts and mobile SIMs to Aadhaar.[188] Aadhaar's eKYC processes are however just part of a larger digital infrastructure, the India Stack, which includes eSign, online electronic signature service, Digilocker, digitally store and share important documents, and Unified Payment Interface, collection of payments, fees and charges electronically by financial service providers.[189] As noted above, there have been legal issues and challenges around Aadhaar. The project and the Act were under review for constitutional validity by the Supreme Court with regards to aspects of privacy, personal autonomy, and surveillance state.[190] The Supreme Court has now confirmed the constitutional validity of Aadhaar and emphasized that it does not violate the right to privacy of individuals.[191] While Aadhaar is still allowed to be mandatory for filing income tax and obtaining a Permanent Account Number (PAN), the Court banned the use of Aadhaar for bank CIV processes and for registering for a SIM card.[192] The system has also suffered several leakages of user data through hacking.[193]

5.4 Jordan

In 2016, the Department of Civil Status and Ministry of Information and Telecommunication Technology introduced national eID containing biographical data and well as iris scan and fingerprints, with future plans to include health insurance, pension and voting activities.[194] A companion SIC is also issued that includes all data except iris data. In January 2018, the Telecommunication Regulatory Commission also mandated the gathering of biometric data for SIM card registration.[195] The older laminated national ID cards will still be valid for a number of years until each card expires, after which the holder must enroll for the eID and SIC.

5.5 Malawi

Up until a biometric ID program was launched in 2017, Malawi had one of the lowest number of persons with a legal form of identity.[196] With donor assistance,[197] Malawi's National eID project was launched in 2017, registering citizens aged 16 years

---

was used for authentication purposes. India Today (2018) *What is Aadhaar history, why it is important and why you should or should not download it from UIDAI site*, available at https://bit.ly/2JcY2IE

[187] Riley, T & Kulathunga, A (2017) *Bringing E-money to the Poor,* available at https://bit.ly/2K9d0iT

[188] NDTV (2018) *Now, Link Mobile SIM with Aadhaar Card from Home Via IVR System,* available at https://bit.ly/2K0NJew; The Economic Times (2018) *Now You Can Check if Your Bank Account is Linked to Aadhaar,* available at https://bit.ly/2Ie1bpx

[189] For more information on IndiaStack, see http://indiastack.org/

[190] Livemint (2018) *Aadhaar Legal Validity: SC Constitution Bench to Commence Hearing Today,* available at https://bit.ly/2KaTZ2t

[191] For Supreme Court of India judgment, see https://bit.ly/2OM50Gx*;* Livemint (2018) *Supreme Court Verdict on Aadhaar: Constitutionally valid, doesn't violate privacy,* available at https://bit.ly/2CKBDlT

[192] Economic Times (2018) Payments companies asked to stop Aadhaar-based services, available at http://www.ecoti.in/tfgiUb. For the Supreme Court of India judgment, see https://bit.ly/2OM50Gx*;* Livemint (2018) *Supreme Court Verdict on Aadhaar: Constitutionally valid, doesn't violate privacy,* available at https://bit.ly/2CKBDlT

[193] *See* Section 4.2.4. Huffington Post (2018) *UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm*, available at https://bit.ly/2CPdTgf. One hack reduces the sensitivity of the enrolment software's iris-recognition system, making it easier to spoof the software with a photograph of a registered operator, rather than requiring the operator to be present in person.

[194] The Hasemite Kingdom of Jordan (2018) *Jordan Smart Card,* available at https://bit.ly/2thfXY2.

[195] Privacy International (2018) *State of Privacy Jordan,* available at https://bit.ly/2Ceqzgr

[196] The Malawi National Registration Act went into effect in August 2015, requiring all Malawians 16 years of age and older be included in a national registry and be issued an ID card. The Act also created the National Registration Bureau to manage both civil registration and registration for the ID program. Up to the start of the registration program, Malawi was the only country in the Southern African Development Community and in the Common Market for Southern and Eastern Africa that did not have a functional national registry and ID system. Malawi had an estimated 2 to 3 % coverage for birth registration, while national ID registrations totaled around 40,000-50,000 people out of an estimated adult population of some 9 million. See UN Malawi (2018) *Malawi's National ID Project Praised at Africa's Largest Forum on Digital Identity*, available at https://bit.ly/2J3Pxjb; and Malik, K (2018) *Malawi's Journey Towards Transformation: Lessons from its National ID Project*, available at https://bit.ly/2yNXMLG.

[197] Its National biometric ID project is being implemented by the National Registration Bureau with technical support from UNDP and financial assistance from EU, UK Government, Royal Norwegian Embassy, Irish Aid, and USAID. UN Malawi (2018) *Malawi's National ID Project Praised at Africa's Largest Forum on Digital Identity*, available at https://bit.ly/2J3Pxjb/

and above. Remarkably, within a designated 180 days period, some 9.1 million citizens out of 16 million were registered, while 3.6 million children were registered alongside their parents.[198] The total cost of the project was around USD 52 million.[199] While the majority of the population is biometrically registered, paper-based identity documents – passports and driver's licenses for example - will still be accepted for DFS sign-ups and for other commercial and government services.[200] All District Commissioners' Offices are designated to undertake continuous registration to cater for those that missed the mass registration campaign and those turning 16 years old.

5.6 Nigeria

Several government agencies undertook biometric data capture following regulatory requirements from *inter alia* the Nigerian Communications Commission (NCC); the Independent National Electoral Commission; the Federal Road Safety Corp; and the Central Bank's mandated use of bank verification numbers (BVN) for financial transactions.

The NCC made biometric registration for all SIM cards compulsory.[201] Based on the SIM card registration data, customers can fulfil Tier 1 KYC for a DFS account with limited transaction limit.[202] Higher transaction limits can be obtained if Tier 2 and Tier 3 KYC requirements are fulfilled, but which require more documents and verification.[203] Other biometric databases and identity verification schemes also exist in Nigeria. The Nigerian National Identity Management Commission provides eID cards that combine biometric identification and a prepaid payment card.[204] The Central Bank of Nigeria provides BVN - unique identification numbers associated with user's biometrics - for use in conducting banking transactions.[205] BVNs are added to a watch-list if customer is involved in confirmed fraudulent activities.[206]

There are plans to avoid duplication of biometric-based identity systems of these multiple databases by enrolment of Nigerians and legal residents into the NIDB to develop a single biometric identity.[207] It is believed that harmonization of all private and government agency databases could save the country about USD 110 million in operational costs by the different government agencies for their stand-alone data collection and evaluation.[208]

5.7 Pakistan

The Telecommunication Authority mandated the verification of all SIM card owners using biometric information linked to their NIC number in 2015.[209] Since the SIM registration requirement provided customers with an eID based on their biometric

---

[198] Previous reports indicated that the introduction of biometric identification substantially increased repayment rates amongst Malawian farmers with the highest risk of default. See IPA (2017) *Access to Credit and the Scale-Up of Biometric Technology in Malawi*, available at https://shar.es/a1KM1P

[199] The Malawian government contributed 40% of the total cost, and also contributed to security and transportation. The program include a points-based approach towards determining citizenship and the rapid development of a digitally skilled workforce to carry out mass registration. See Malik, K (2018) *Malawi's Journey Towards Transformation: Lessons from its National ID Project*, available at https://bit.ly/2yNXMLG.

[200] BiometricUpdate (2018) *Malawi pushing ahead on biometrics-based voter registration plan*, available at https://bit.ly/2yXOE71

[201] Balancing Act (2013) *Bio-key Biometric Tech Implemented for Nigerian SIM Registration,* available at https://bit.ly/2IdDu0H

[202] Helix (2014) *Agent Network Accelerator Survey: Nigeria Country Report 2014,* available at https://bit.ly/29foluO; Central Bank of Nigeria (2013) *Introduction of Three-tiered Know Your Customer (KYC) Requirements,* available at https://bit.ly/2KafpJU

[203] *ibid.*

[204] BBC (2014) *Nigeria Launches National Electronic ID Cards,* available at https://bbc.in/2IbsiBQ; MasterCard (2013) *Nigeria National ID Card (NID),* available at https://bit.ly/2MdfehK

[205] Esoimeme, E (2015) *A Critical Analysis of the Bank Verification Number Project Introduced by the Central Bank of Nigeria*, available at https://ssrn.com/abstract=2544934

[206] Central Bank of Nigeria (2017) *Bank Verification Number (BVN) Enrollment for Customers,* available at https://bit.ly/2HPgfip; Online Integrated Solutions (2018) *BVN Enrolment*, available at https://oisservices.com/bvn.php; Azeez, K (2018) *80 To 90% Bank Fraud Caused by Customers – NIBSS Boss*, available at https://bit.ly/2IMRejB

[207] Tarpael, F (2017) *FG to Harmonize BVN, Others into National Identity Database*, available at https://bit.ly/2yxAufX

[208] All Africa (2018) *NIMC's Unrealistic 2019 Deadline*, available at https://allafrica.com/stories/201809250414.html

[209] Every SIM owner was required to visit an operator outlet where their MSISDN and Computerized National Identity Card were confirmed or updated in the existing ownership database and fingerprints were matched with the National Database and

data and government-issued ID, Telenor, a mobile operator in Pakistan that provides DFS (Easypaisa), petitioned the State Bank of Pakistan to allow SIM registration to satisfy KYC requirements for mobile money account set up, making it easier for people to access mobile money services.[210] Further, the introduction of Biometric Money Transfer facility by Easypaisa has allowed retailers to use biometric verification to transfer and receive funds while ensuring their NIC is not expired or blocked.[211]

5.8 South Africa

South Africa's Department of Home Affairs launched a 'Smart ID Card' in 2016 to replace bar-coded identity books which are issued to South African citizens or permanent residence permit holders who are 15 years and six months or older. The ID books however are still valid. The new SIC includes a person's photograph, their full name, date and place of birth, and their unique ID number. Fingerprint data is also taken and printed along with biographical details and a colour photograph, on the SIC. The government also in 2018 launched its Automated Biometric Identification System project to integrate all systems, inside and outside the government, to offer a single source for biometric authentication for citizens. Banks for example will be able to verify client identification faster and police services will be able to match fingerprints.[212] The new system will add multi-modal components to allow iris and palm-print capabilities. The SIC can be applied for at banks and online.[213]

5.9 Uganda

The Uganda Communications Commission (UCC) has made multiple attempts to require verification of all SIM cards using proper identification documents but it has been affected by conflicts between MNOs, the UCC and the government over deadlines for registration and availability of required ID documents.[214] UCC banned the sale of new and replacement SIM cards until an application program interface (API) into the National Identification Registration Authority ID database was developed and integrated, and until MNO agents – who sell at places licensed by a city authority - could employ and use biometric readers to undertake real time online verification of customers' information with the database.[215]

The ban lasted for 2 months and was lifted, with some remaining restrictions in May 2018.[216] This followed the UCC ordering MNOs in 2017 to switch-off, then later switch back on following an outcry, some 2 million unregistered SIM cards.[217] In both cases, the effect was manifest on DFS: no access the mobile networks led to no access to DFS accounts.[218] Switch-off of unregistered SIMs involves barring all incoming and outgoing calls, barring data services, enable only mobile money cash-out but no cash in or receipt of funds, calls only for emergency services and calls to customer care. Unused DFS balances are retained in accordance to mobile money regulations as stipulated by Bank of Uganda.[219] The issue still percolates as issuance of national IDs can take up to month and requires often unavailable identification documents. It also highlights concerns that, despite ostensibly applying RBAs for financial inclusion imperatives recommended by the FATF, there are other contextual issues that that restrict SDD and national consideration – especially in relation to security matters – may override the suggested RBA though.[220]

5.10 UNHCR

The UN High Commission for Refugees (UNHCR) has a large presence in a number of countries with large refugee populations, where it staffs enrollment centers for provision of aid to refugees. In Jordan for example, it serves refugees from

---

Registration Authority. Gidvani, L (2015) *The Promise of Biometric KYC and Remote Account Opening for Branchless Banking in Pakistan,* available at https://bit.ly/2rFPhiP

[210] Matthew, W (2016) *Digital Identity: A Prerequisite for Financial Inclusion?,* available at https://bit.ly/2IbavdW

[211] The News International (2016) *Easypaisa Launches Biometric Facility,* available at https://bit.ly/2KbxLgV

[212] Biometric Update (2018) *South Africa to launch ABIS, add face and iris to national identity system*, available at https://bit.ly/2EAz6wh

[213] Businesstech SA (2016) *Apply for your Smart ID card online from Thursday*, available at https://bit.ly/2NTJFde

[214] New Vision (2017) *Telecom firms given 72 hours to deactivate SIM card*s, available at https://shar.es/1Pemkq; Article 19 (2017) *Uganda: SIM Card Registration Requirements Must Respect Fundamental Rights,* available at https://bit.ly/2K93MTJ

[215] New Vision (2018) *UCC Lifts Ban on Sale And Replacement Of SIM Cards*, available at https://bit.ly/2rzdwiT

[216] EDGE (2017) *UCC Directs Telecoms to Switch Off Unverified SIM Cards*, available at https://bit.ly/2whzolo

[217] New Vision (2017) *Unverified SIM Cards to be Switched Off Next Week,* available at https://bit.ly/2K8UIOs; Daily Monitor (2017) *UCC Orders Telcom Companies to Re-connect Unregistered SIM Cards,* available at https://bit.ly/2qGXbG7

[218] Kyatusiimire, S (2017) *UCC Issues SIM Card Switch-off Guideline; Mobile Money Transactions Affected,* available at https://bit.ly/2tueNb6

[219] EDGE (2017) *UCC Directs Telecoms to Switch Off Unverified SIM Cards*, available at https://bit.ly/2whzolo

[220] The 2018 ban came after kidnappers were found to have used unregistered SIMs. New Vision (2018*) UCC lifts ban on sale and replacement of SIM cards*, available at https://bit.ly/2rzdwiT

inter alia Syria, Sudan, and Yemen who register with the UNHCR to obtain refugee status and associated UNHCR-issued identity documents. This refugee enrollment process as part of UNHCR's own eKYC system uses a combination of iris scans,[221] document authentication and interviews. Documents may *inter alia* be passports, national ID documents, military ID cards, or family books.[222] UNHCR staff are trained in assessing the authenticity of documents. In the course of the interview of a family, biographical information of family members are captured on the UNHCR's proGres database application.[223] The iris data of adults in a family is also captured and stored on the UNHCR EyeCloud database.[224]

If initial interviews and/or document inspection trigger a need for further investigation, a further level of assessment is done by UNHCR staff and if there are further concerns, the case is escalated to the UNCHR's legal case officers. If the assessments provide comfort to UNHCR personnel that the refugees do not pose a threat or are not military operatives, a family or individual is registered as a refugee/asylum seeker/person of concern by the UNHCR and, as proof thereof, provided with an A4-sized identity document with several security features. To access financial services, the registered individuals can use UNHCR or associated financial institutions to draw cash by simply walking up to an ATM equipped with an iris scanner linked to the UNHCR iris database.[225]

6. CONCLUSIONS

Appropriate financial inclusion regulations, policies and strategies, identity number and mobile phones together are very powerful, empowering tools for the poor.[226] The CIV process for mobile SIM card registration has been largely digitized by the use of eIDs, especially those that contain biometric data. The new eKYC procedure for SIM card registration is enough to obtain a basic DFS account with limited transaction and storage capabilities in many jurisdictions such as Bangladesh, Pakistan, Nigeria and Uganda. Since DFS is considered an effective and popular mean of expanding financial services to remote and underserved populations, the use of eKYC for both SIM card registration and DFS account provision can promote financial inclusion.

Implementation of eKYC procedures however not only requires regulatory provisions for SIM card registration to complete CDD for DFS, even if it is just SDD, and complete roll out of national IDs, but also technological capacity for verification of documentations by DFSPs, regulatory and technological provisions for data privacy and protection and regulatory coordination for strategic adoption as the process involves input from multiple regulatory entities. Implementing a fully-fledged eKYC system also requires large capital but beyond the initial costs incurred, countries must be able to further bear the ongoing costs associated with data management, security, and continual enrollment.

eID and eKYC can however provide a starting point for digitization of other CDD processes, not just limited to CIV. Without the necessary enabling environment however, the use of eKYC will rather limit user's access to financial services and put them at risk, rather than promoting financial inclusion.

---

[221] This uses the UNHCR's IrisGaurd iris capture system.

[222] In some cases and despite their controversial provenance, even ISIS-issued documents are accepted by the UNHCR in Jordan as proof of identity.

[223] UNHCR (2018) *Registration,* http://www.unhcr.org/en-us/registration.html

[224] UNHCR (2015) *UNHCR Jordan Cash Assistance Programme*, available at https://bit.ly/2J9E2a5, and UNHCR (2017) *The Common Cash Facility*, available at www.unhcr.org/596331dd7.pdf

[225] UNHCR (2018) *Registration,* http://www.unhcr.org/en-us/registration.html

[226] Paraphrase of remarks by R.S. Sharma, Chairman of India's Telecommunications Regulatory Authority (TRAI), now DCAA in ITU (2017) *Aadhaar: India's route to digital financial inclusion*, available at https://news.itu.int/SDPSP