Technical Assistance Consultant's Report

Project Number: 49386-001
November 2018

Financial Inclusion Framework Strengthening - Digital National Identification for Financial Inclusion: Final Report

Prepared by Bankable Frontier Associates, LLC (BFA)

For ADB

Table of Contents

Acknowledgments

Under ADB Technical Assistance, Financial Inclusion Framework Strengthening for the Philippines, this report was prepared by Bankable Frontiers Associates LLC (BFA)* at the request of the Bangko Sentral ng Pilipinas (BSP).[1] The TA and this report support important government initiatives reflected in the Inclusive Finance Development Program for the Philippines.[2] The program aims to improve access to financial services across the Philippines, including for small businesses, farmers, women and low-income households. The program is helping government strengthen the policy and institutional environment for expanding financial services and to invest in support networks and infrastructure such as the national retail payment system and the new national identification system. In addition, the program is supporting innovative solutions to strengthen the capacity of financial service providers to expand financial services particularly for micro, small, and medium enterprises in rural areas and in the agriculture sector.

On behalf of the ADB, BFA wishes to thank Pia Roman, Managing Director, Inclusive Finance Advocacy Office (IFAO), Bangko Sentral ng Pilipinas (BSP) and Kelly Hattel, Senior Financial Sector Specialist, Asian Development Bank (ADB) for the invaluable support, guidance and insights throughout the project. BFA also thanks Ellen Joyce Suficiencia and Cesar Augusto Villanueva Jr. of IFAO for coordinating stakeholder interviews and supporting us throughout the course of the project. Thanks is also extended to the financial service providers who agreed to be interviewed. The team appreciates their willingness and openness to share their experiences and expectations.

This report was written by Rajesh Bansal, Rakesh Ranjan, Jeremiah Grossman, and Priyanka Kapoor of BFA. The report is based on desk research findings and stakeholder interviews conducted during in-country visits by BFA's team of consultants.

---

* BFA is a global consulting firm specializing in financial services for people on low incomes. BFA's approach is to seek out, create and implement financial solutions to help people manage challenges and seize opportunities. BFA partners with cutting-edge organizations that touch the lives of low-income consumers such as financial institutions, fintech companies, and information providers. In creating solutions, BFA integrates a deep expertise in customer insights, business strategy, new technology, and growth-enabling policy and regulation. Founded in 2006, BFA's clients include donors, investors, financial institutions, policymakers, insurers, and payment service providers. BFA has offices in Boston, New York, Nairobi, Medellin, and New Delhi.

Abbreviations

4Ps	Pantawid Pamilyang Pilipino Program
AML	Anti-money Laundering
ATMs	Automated Teller Machines
BAP	Bankers Association of Philippines
BSFIs	BSP-Supervised Financial Institutions
BSP	Bangko Sentral ng Pilipinas
CBA	Cost-Benefit Analysis
CBS	Core Banking System
CCT	Conditional Cash Transfers
CDD	Customer Due Diligence
CRN	Common Reference Number
CRVS	Civil Registration and Vital Statistics
DPA	Data Privacy Act of 2012
DSWD	Department of Social Welfare and Development
e-Signatures	Electronic Signatures
ECA	Electronic Commerce Act of 2000
EFT	Electronic Fund Transfer
e-KYC	Electronic KYC
FATF	Financial Action Task Force
FSPs	Financial Service Providers
FXDs	Forex Dealers
G2P	Government-to-Person
GDP	Gross Domestic Product
GNI	Gross National Income
GSIS	Government Service Insurance System
ICT	Information & Communication Technology
ID	Identity
ID4D	Identification for Development
IRR	Implementing Rules and Regulations
KYC	Know Your Customer
MC	Money Changer
MFI	Microfinance Institution
MIS	Management Information System
MRZ	Machine Readable Zone
NADRA	National Database and Registration Authority
NBFIs	Non-Bank Financial Institutions
NGOs	Non-governmental Organizations
NPV	Net Present Value
NRPS	National Retail Payment System
NSFI	National Strategy for Financial Inclusion
NSSLAs	Non-Stock Savings and Loan Associations
OFW	Overseas Filipino Workers
OTP	One Time Password
P2P	Person-to-Person
PHP	Philippines Peso
PII	Personally Identifiable Information
PMPG	Payments Market Practice Group
POS	Point-of-Sale
PSMB	Payment System Management Body
PSA	Philippines Statistics Authority
PSN	PhilSys Number
PVC	Polyvinyl Chloride
REE	Rules on Electronic Evidence
RIRR	Revised Implementing Rules and Regulations
ROI	Return-on-Investment
RTC	Remittance and Transfer Company
SPI	Sensitive personal information
SSS	Social Security Systems
TF	Terrorism Financing

Executive Summary

The Philippines is considered a pioneer in mobile financial services, but access to formal financial services remains sparse. According to Bangko Sentral ng Pilipinas' (BSP's) Financial Inclusion Survey, 2017, only 22.6 percent of the adult population has a formal account and only a small percentage of payments are made electronically. Despite extensive smartphone usage, 46 percent of account holders who have access to the internet are still ambivalent about e-payments.[3]

As part of a broader effort to create an enabling financial ecosystem that utilizes digital technology as a catalyst for financial inclusion, the government of the Philippines has decided to establish "PhilSys" as a single, digital, national identification (ID) system. A digital national ID system has the potential to support an entire digital financial ecosystem and deliver a wide array of benefits including lower barriers to entry for lower-income consumers and innovative service providers.

It is also worth considering that rolling out and implementing such a system will generate significant issuance and service delivery infrastructure costs. However, comparing the cost and benefits of the digital national ID system, we found that net benefits are high with a net present value (NPV) of US$517 million, making it an attractive proposition for financial institutions to adopt digital national ID as a preferred identification document.

Role of PhilSys in furthering financial inclusion

By enabling unique, traceable identities, digital national IDs can facilitate compliance with anti-money laundering (AML) laws, ensure robust credit reference checks and scoring, and lower costs for social cash transfer programs. Most importantly, a digital national ID would allow accurate identification of social welfare beneficiaries, ensuring efficient delivery of public services and mitigating fraudulent transactions in conditional and unconditional cash transfer (CCT/UCT) programs.

A digital national ID simplifies public and private transactions by allowing service providers – like governments, banks, telecommunications companies, and other private sector users – to complete know-your-customer (KYC) requirements for their constituents digitally (e-KYC). e-KYC can reduce customer onboarding costs by up to 80 percent, making customer acquisition, especially among the lower-income segments, a more viable business proposition for financial services providers (FSPs).

Finally, without digital ID platforms, innovators in the provider space have had to rely on pseudo-digital channels (e.g., photographing physical ID documents) and KYC processes of established FSPs that decentralize a critical piece of their product/service offerings. A digital ID can provide the market architecture that technology-driven providers need to succeed.

PhilSys design features that maximize financial inclusion

However, to achieve a digital finance ecosystem that supports the diverse needs of all users in a manner that is secure, sustainable, convenient and affordable, care must be taken in the design of the PhilSys information technology (IT) platform and the PhilID - a non-transferable card to be issued to all citizens and resident aliens registered under the PhilSys. The PhilID shall serve as the physical medium to convey essential information about the cardholder's identity. All the information appearing in the PhilID should match with the registered information in the PhilSys. Since the PhilID is intended to serve as the official, government-issued identification document for the cardholder in dealing with all national government agencies and private sector entities, we suggest:

- In addition to the Quick Response (QR) code, the PhilID cards should contain a machine-readable zone as well as physical security features such as micro-lettering, optically-variable ink, and latent images to facilitate reading by FSPs electronically and to prevent counterfeiting.
- The enrolment process should feature strict monitoring procedures to verify documents and to capture high-quality biometrics.
- The PhilSys system should offer multiple modes of authentication based on one or more of: something you have (e.g., PhilID card), something you know (e.g., PIN or password), and something you are (e.g., biometrics). Additionally, the system could offer a one-time password (OTP) authentication to provide additional consent.
- Since smartphones are in wide use, PhilSys could offer a downloadable profile to be stored in the smartphone and shared digitally to verify identity.
- The authentication system must provide open application programming interface (API) architecture to develop an ecosystem in which national ID and authentication services are widely used.
- Data privacy must be paramount to ensure that no demographic or biometric data is shared with a third party unless consent is obtained from the owner.

Areas for further attention

It is important to note that simply establishing a unified, digital proof of identification for all citizens will not be sufficient to overcome other barriers to sustainable financial inclusion in the Philippines, therefore attention should be given to ensure that National Retail Payment System (NRPS) promotes the use of PhilISys whereby individuals are identified uniquely by their PhilID, demographic data and/or biometric data and that their financial addresses are linked to their ID. Similarly, e-money service providers should also be advised to authenticate using the PhilSys platform. Using PhilID across all e-money and bank accounts will slowly lead to the creation of individual financial profiles, which can then be used to design and roll-out new financial products and services.

And finally, a broader set of issues that should be resolved to promote widespread adoption, such as high transaction fees, network connectivity, skewed financial services access in rural areas, low adoption of technology by rural banks, insufficient credit history, low fintech activity, and little financial and digital literacy. Adopting a digital ID platform can, at best, trigger a cascade-effect regarding technology adoption, awareness, and competitive pricing, but a systemic approach is needed to achieve the ambitious goal of providing access to affordable and client-centered financial services.

Introduction

"ID technologies sit at the interface between the power and prerogatives of institutions, and the rights and needs of individuals. They can help create a basis of trust and inclusion that strengthens democracies and free market economies." -- (USAID).[4]

> Identification (ID) systems offer a means to developing nations to accelerate their economic and social development. There may be no single factor that affects a person's ability to share in the gains of global development as much as having an official identity.[5]

A national ID attempts to bring all citizens under one fold by unlocking access to a host of formal services for the financially excluded and the most vulnerable members of the society. Social services like healthcare and education, electoral rights, business registration, school enrolment, and safety net programs to financial services like account ownership, loan application, savings, transactions, payments, and insurances, etc. could all be accessed using a national ID.

Financial inclusion has been recognized as a significant policy objective by countries aiming to achieve inclusive and sustainable economic growth, financial stability, and poverty alleviation. By helping low-income populations gain access to formal financial systems, it allows them not only to accumulate savings and insurance to protect them during unforeseen financial risks and shocks but also to expand their businesses through credit.

However, despite consistent efforts, most countries are still struggling to achieve sustainable inclusion. Policymakers, financial institutions, and researchers have continuously explored the reasons why financial inclusion schemes have not been beneficial. They have tried to identify environmental factors that have so far hindered the growth of both 'd*emand-side pull*' and 's*upply-side push*'; supply-side barriers consist of high transaction costs, information asymmetry, and inadequate regulatory frameworks that impede the quantity and quality of financial products and services that are accessible by the poor. Demand-side barriers constitute a range of factors that have effectively excluded individuals, especially the poor, from accessing financial services — socio-economic and cultural elements, challenges posed by the lack of formal identification systems, and low levels of financial literacy in addition to the absence of appropriate consumer protection mechanisms. Other factors that drive exclusion of the poor from financial services are a lack of awareness of available services and the inappropriateness of certain products about the needs of the low-income consumers and the risks of dealing with poor customers.

While all of the above aspects have hindered the development of an effective financial ecosystem, lack of a valid Identification document has emerged as one of the most significant barriers in bringing the unserved and underserved population to formal financial systems. In recent years, several developing countries have realized that

effective ID systems can contribute significantly to improvements in their citizens' social and economic conditions. An ID system that can uniquely identify beneficiaries and consumers enables delivery of services or transfer of benefits transparently by preventing leakages in government spending and aiding financial inclusion.

It has been observed that most of the successful ID implementations are not just paper-based Identity schemes but are digital Identities that can be electronically verified either online or offline. Digital IDs offer a unique opportunity to service providers like governments, banks, telecom companies, and other private sector users to complete KYC requirements for their constituents digitally (termed e-KYC in this paper[6]). Such ID systems usually capture biometric information (e.g., fingerprints, iris, face) and demographic information (e.g., name, gender, date of birth, etc.) to eliminate duplicates more effectively.[7]

The purpose of this study is to analyze how the implementation of a digital national ID system in the Philippines can help accelerate access to finance in the country. References have been drawn from World Bank's "ID4D" principles, India's Aadhaar, and Pakistan's NADRA programs that have effectively supported financial inclusion initiatives in their respective countries. This report explores the existing state of financial inclusion in the Philippines, determines barriers to achieving sustainable financial inclusion, and suggests recommendations to use the digital national ID to improve financial inclusion as a critical, strategic poverty reduction measure through increased access to financial services and strengthening of the social protection system.

1 Financial Inclusion in the Philippines – A Review

Financial inclusion aims at drawing the unbanked population into the formal financial system so that it has the opportunity to access financial services, including savings, payments, and transfers to credit and insurance.[8] Theoretical and empirical studies suggest that financial systems serving the low-income segment of society promote pro-poor growth.[9] Financial inclusion is therefore considered an important element that can contribute to broad-based development and inclusive growth. While most developing countries have increasingly focused their financial sector development towards inclusive financial systems, the Philippines emerged as one of Asia's leaders in financial inclusion in *The 2017 Brookings Financial and Digital Inclusion Project Report* due to policies supportive of wider banking access.[10]

Since the year 2000, the BSP has been pursuing an active agenda for nurturing an enabling environment for the delivery of financial products specifically for the low-income and vulnerable sectors of society. Among others, the goal was to mainstream microfinance as a banking activity and enable market-based solutions to address frictions and promote financial inclusion more sustainably. This approach has allowed 163 banks — mostly rural banks in the countryside — to serve more than 1.7 million micro-entrepreneurs. Beyond credit, the microfinance regulations have also enabled delivery of other financial products, such as microdeposits and microinsurance.[11]

1.1 Country Context

The Philippines is an island country in Southeast Asia, located between Taiwan and Borneo. It is an archipelago comprising some 7,641 islands and islets in the western Pacific Ocean. The capital city of the country is Manila, but nearby Quezon City is the most populous city. Both the cities are part of the National Capital Region (Metro Manila) located on Luzon, the country's largest island. Mindanao, the second-largest island, is in the southeast.[12]

The country has a population of 101 million and a land area of 300,000 km^2. The adult literacy rate is very high at 96.5 percent (2013). In 2017, it was one of the fastest-growing economies in the East Asia region ranking third after Vietnam and China although growth in gross domestic product (GDP) slowed in 2017 to 6.7 percent year-on-year from 6.9 percent in 2016[13]. The Philippines is a lower-middle-income country with a gross national income (GNI) per capita of US$3,580 in 2016[13]. It has a very strong base of overseas working population at 10.2 million (2013). By 2017, these workers were sending around US$28 billion back to the Philippines each year[14]. The country has a very high telecom adoption rate. The proportion of the population with SIM cards stood at a staggering 113 percent, while the adoption rate for smartphones was also high at 59 percent.[15]

1.2 The Philippines Financial System

The Philippines' economic narrative has been one of robust and resilient growth. With the real GDP growing by 6.7 percent in 2017 and the economy expanding by more than 6 percent annually over the past five years, the country now stands on a solid foundation to support inclusive growth and nurture an enabling environment that promotes greater access to financial products and services. The banking system continued its robust performance and contributed positively to the economy's growth in 2017 on the back of sound fundamentals, underpinned by sufficient provisioning and adequate capital and liquidity buffers to ward off unexpected external shocks.[16]

The country's financial sector is diverse, including universal banks, commercial banks, thrift banks, rural banks, cooperative banks, microfinance institutions (MFIs), and pawn shops. As of 2017, rural and cooperative banks comprised 83.3 percent (489) of the total number of banks, followed by thrift banks (55 or 9.4 percent), universal banks (21 or 3.5 percent), and commercial banks (22 or 3.7 percent).[17]

The Philippines also has a large number of pawn shops operating in the country that provide both domestic and overseas remittances services. According to the Financial Inclusion Survey, 2017, remittance agents - especially pawn shops - are overwhelmingly used by Filipino adults. Some 93 percent of senders and 83 percent of receivers used them during the first six months of 2017. Pawn shops are also popular in the country owing to their vast network, accessibility, convenience to the users and aggressive pricing strategy. A few of the large pawn shops agencies have an enormous network of more than 1,000 branches.

Mobile money providers have also established a robust agent network in the country, providing access to formal financial services for unserved and underserved segments.

While the 43 universal and commercial banks (with a total physical outreach of 6,483[18] branches) deploy core banking solutions (CBSs), the branch network of commercial and thrift banks is still relatively limited in the Philippines, causing most of the financially-included Filipinos to use the services of microfinance and cooperative banks. The MFIs have better rural reach, but limited access to the latest tools and technology. Both the thrift banks, serving the rural and urban population with 2,417[19] branches, and the rural and cooperative banks, predominantly serving the rural areas with 2,893[20] branches, mainly rely on stand-alone Management Information Systems (MIS) and use manual processes.

An overview of the current industry profile of the Philippines' banking system illustrates growth of 5.5 percent in the number of banks (head office, branches, and other offices), and an increase of 6.3 percent in the number of automated teller machines (ATMs) across the country in the past year. Microfinance non-governmental organizations (NGOs) and credit cooperatives reported a growth of 26.1 percent and 6.3 percent, respectively, in 2017.

Table 1 depicts the current status of banking access points in the country, as of third quarter (Q4) 2017[21] and table 2 illustrates the access status of other financial service access points as of Q4, 2017[22].

Table 1: Banks and automated teller machine access points

Other Financial Service access points		2016 Q4	2017 Q4
Banks (head office, branches, and other offices)		11,129	11,744
	Universal & Commercial Banks	6,188	6,434
	Thrift Banks	2,176	2,417
	Rural & Cooperative Banks	2,765	2,893
ATMs		19,081	20,276
	On-site ATMs	10,721	11,278
	Off-site ATMs	8,360	8,998

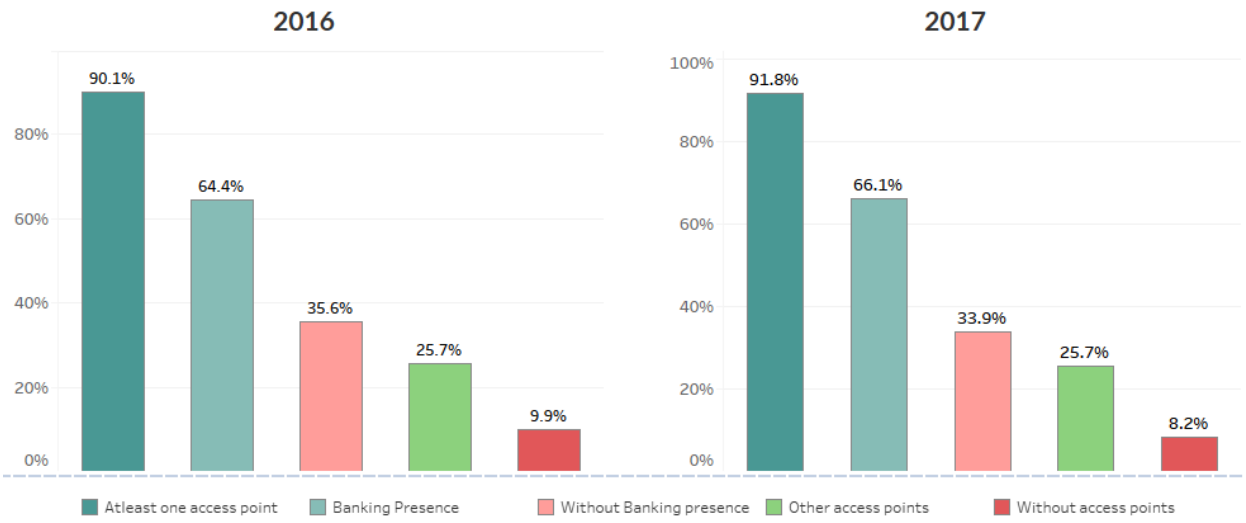
Table 2: Other financial service access points

Other Financial Service access points		2016 Q4	2017 Q4
Savings, credit & other services	NSSLAs (Non-stock Savings and Loan Associations)	199	197
	Credit Cooperatives	3,446	3,664
	Microfinance NGOs	2,065	2,603
Credit & other services	Pawnshops	16,698	16,582
	Other NBFIs	181	218
Payment & money transfer services	FX Dealers/Money Changers (FXDs/MCs)	1,940	1,965
	Remittance and Transfer Companies (RTCs)	5,356	5,298
	FXDs/MCs/RTCs	4,732	4,434
	E-Money Agents	26,028	48,295
	Point-of-sale (POS) terminals	152,203	181,748

The other formal financial channels play a significant role in providing access to regions where there is either limited or no banking access point. Out of a total of 1,489 municipalities, 33.9 percent do not have a banking presence. Of these unbanked municipalities, 25.7 percent are served by more than 50,000 other financial service access points, making 91.8 percent of the total number of cities and municipalities covered by at least one access point.

Figure 1[23] depicts an overall access situation in the Philippines in 2017 in comparison to the previous year, signifying a 1.7 percent growth in the overall banking presence and a reduction of 1.6 percent in the total number of municipalities without an access point.

Figure 1: Overall access situation



1.3 Current State of Financial Inclusion in the Philippines; A Long Road Still Ahead

According to a World Bank report,[24] approximately 25 percent of people in the Philippines live below the poverty line. Millions of other Filipinos are still highly vulnerable to climate events, financial crises, and price shocks, even though their incomes are just above the poverty line. However, in the last few years, the Philippines has made modest economic progress thanks to strong policy fundamentals and large inward remittances from abroad. Nonetheless, despite good economic growth, poverty levels have not declined commensurately.

Figure 2: Snapshot of financial inclusion

BSP has been at the forefront of designing policies and frameworks in accordance with the Philippines Development Plan to promote financial inclusion, but despite its commitment and an enabling regulatory framework for 'affordable' and 'secure' financial services to the public, large-scale access to financial products and services remains a challenge. Around 65 percent[25] of the adult population in the Philippines does not have access to formal financial services, 1 percent of 2.5 billion transactions worth PHP3.7 trillion[26] takes place electronically, and it takes a minimum of 21 minutes and an average of PHP43[27] to get to the nearest financial services touchpoint. The situation calls for immediate attention to identify barriers that have thus far prevented expansion of financial inclusion measures.

As per the 2017 BSP survey (see table 3), only about 22.6 percent of the adult population is reported to have had a formal account. About 48 percent of the adult population in the Philippines saved while 68 percent out of those who saved kept their savings at home; 40 percent who had outstanding loans obtained loans from informal resources and 10 percent of the local municipalities had no access to an outlet of a bank or any other financial service provider. Moreover, while the Philippines is considered a pioneer in mobile financial services, only a small percentage of payments take place electronically. Despite extensive smartphone usage, 46 percent of account holders who have access to the internet are still ambivalent about e-payments.[28]

Table 3: Financial services usage in 2017, as a percentage of the total adult population

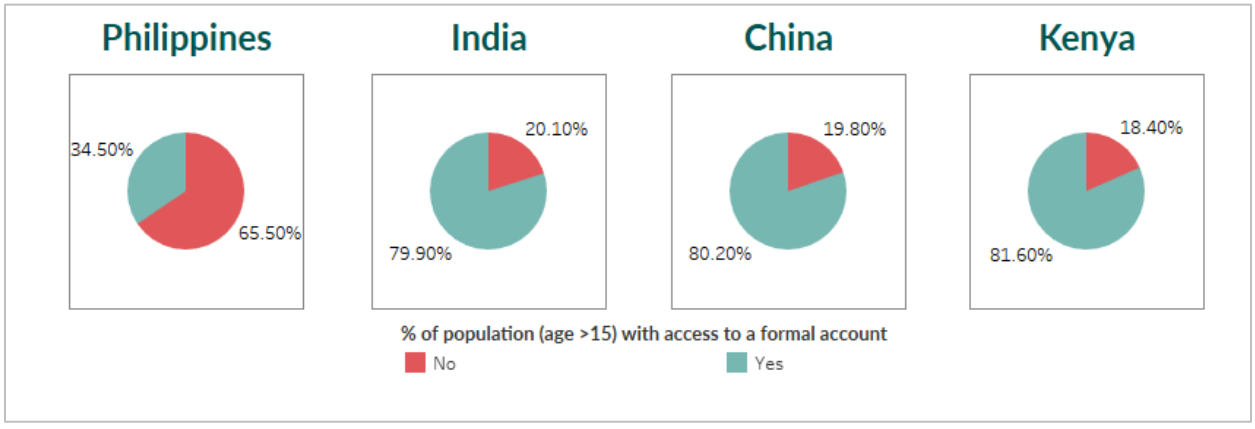





Financial Service	% of Total Adult Population	Bank	Microfinance NGO	Cooperative	e-money	NSSLA	Informal methods
Account Opening	22.6%	11.5%	8.1%	2.9%	1.3%	0.3%	NA
Savings	48%	9.0%	7.0%	3.0%	NA	0.30%	36.7%
Loans	22.3%	0.6%	7.6%	1.3%	NA	NA	8.9%

When compared to other developing economies, the number of adults participating in formal financial systems in the Philippines is extremely low. Figure 3[29] summarizes the findings from four developing countries (the Philippines, India, China, and Kenya) and compares the total number of citizens (under age 15) having access to a formal account.

Figure 3: Formal account ownership (% age >15)



1.4 Initiatives to Promote Financial Inclusion

Owing to its commitment to broadening financial inclusion and its enabling regulatory framework, the *2017 Brookings Financial and Digital Inclusion Project Report*[30] showed the Philippines to be the world's fourth-best in providing an enabling environment for access to 'affordable' and 'secure' financial services to the public. In 2015, the Philippines government had issued a National Strategy for Financial Inclusion (NSFI) [31]. The Strategy identifies four critical areas for promoting financial inclusion, namely: (i) policy and regulation; (ii) financial education and consumer protection; (iii) advocacy programs; and (iv) data and measurement. These key areas aim to govern the strategies that will serve as a framework for crafting evidence-based regulations, designing and implementing programs, and monitoring progress relevant to financial inclusion.

Continuing its efforts to improve financial inclusion, education, and regulation, BSP now aims to create an enabling financial ecosystem that utilizes digital technology as a catalyst for financial inclusion. Digital technology with its ability to reduce transactional costs has the massive potential of serving the mostly untapped low-income market and support the needs of all classes of customers in a sustainable, convenient, and affordable manner. In order to promote financial inclusion, BSP strongly believes in developing an ecosystem that includes:

- An efficient retail payment system.
- An expansive network of low-cost touch points to onboard new clients and facilitate digitization and disbursement of cash and other financial services.
- Democratized access to transaction accounts wherein every individual can open a bank account and use digital financial products.

BSP believes the above principles are best underpinned by strong Identity and KYC infrastructure, adequate digital literacy, comprehensive telecom infrastructure, supportive regulations, and good market conduct to deepen public trust in financial products, particularly those offered through digital channels. BSP's goal is to develop a digital finance ecosystem that supports the diverse needs of all users in a manner that is secure, sustainable, convenient, and affordable.

1.5 Barriers to Financial Inclusion

Through in-country visits and desk research, BFA has identified various barriers to the expansion of financial inclusion in the country. These barriers, as listed in table 4, impact all or most of the stakeholders— citizens, financial service providers (FSPs), merchants, and the government — adversely in varying degrees. These are both on the supply-side and demand-side.

Table 4: Barrier to expansion of financial inclusion in the Philippines

	Barriers	Description
1.	Lack of a reliable digital identity	One of the key requirements for financial inclusion is to identify customers for ensuring compliance with the money laundering rules and regulations. Although the Philippines has utilized a risk-based approach, providers have expressed the lack of a reliable identity system as one of the critical barriers for serving low-income consumers. The existing identification documents not only lack universality but are also paper-based.
2.	Skewed access to financial services through banks, MFIs, and other financial institutions across provinces	Surveys have revealed that the more prosperous regions have the highest level of access to financial services. Ninety-one percent of total domestic deposits and 96 percent of total domestic loans come only from the National Capital Region and Makati City. On the other hand, poor provinces, especially Visayas and Mindanao (17 percent of the population), received only 0.9 percent of loan transactions and 2.5 percent of domestic deposits.
3.	High transaction cost at banks and other financial institutions	Banks and other formal financial institutions levy charges that are perceived to be high by some stakeholders. This is at least partly why cash is still the predominant method of payment for personal transactions such as utility bills and loan payments (60 percent by value is in cash).
4.	Poor network coverage in most provinces	Network coverage is a significant concern given that many provinces do not have a reliable internet or mobile connections. Given that most of the digital financial channels and products require data connectivity, lack of network only discourages their use.
5.	Lack of a thriving fintech sector	A flourishing fintech sector will play an essential role in bringing tech-enabled solutions to the unbanked and underserved population in low-access provinces at much lower costs. In other parts of the world, the fintech sector has played a significant role in rolling out innovative, low-cost solutions for mobile money, digital lending, regulatory tech, insurance tech, microfinance, remittances, etc. Fintech start-ups in the Philippines mainly focus. on mobile payments and alternative finance, with 26 and 17 players, respectively. Currently, there are 60 fintech start-ups in the Philippines. This number is quite low when compared to other developing countries like India and Indonesia; India, with 13 times the population of the Philippines, is reported to currently have 1,500[32] fintech companies while Indonesia, with 2.5 times the population, has 167.[33] Transaction value in the fintech market in the Philippines was estimated at US$5.5 million in 2017, which is significantly low in comparison to USD$22 billion in Indonesia [33] and US$ 52 billion in India[34] in 2017-18.

	Barriers	Description
		However, the fintech market in the Philippines is expected to grow annually at a rate of 19 percent to US$11.0 million by 2021 therefore; it can be inferred that there is enormous potential for further growth of the fintech industry in the country.[35]
6.	Low levels of technology adoption by thrift and rural banks	Thrift and rural banks are at the forefront of providing financial services to people in rural areas and small towns in the Philippines. However, the level of technology adoption is still low, leading to higher operational costs.
7.	Inadequate credit scoring framework	While Credit Information Corporation (CIC) can gather credit data from various types of financial institutions, including banks, a core issue is the lack of credit information due to delays in the full operationalization of CIC. Secondly, the lack of a unique identity across credit sources is a significant bottleneck in building a comprehensive credit registry
8.	Low financial and digital literacy	Financial literacy is one of the crucial ingredients for the unbanked and underserved populations to given them access to formal financial services. As a result of the digital transformation globally, the trend to deliver financial services through digital channels is on the rise. As a result, it has been observed that some services are now available through websites, mobile apps, unstructured supplementary service data (USSD), and even social media. It, therefore, becomes essential to improve digital literacy of people to leverage those services that are generally low cost and constantly available.
9.	Few strategic and technology partnerships between large commercial banks and community-based institutions	Large commercial banks possess IT infrastructure and expertise. Therefore, it is recommended that smaller banks that do not have necessary IT capability forge alliances to build common platforms for conducting transactions and continuously updating users' financial profile, identified using a common identity. As an example of successful partnerships in the Philippines, BPI, a large commercial bank with enterprise IT capabilities, is supporting its smaller subsidiaries like BanKO in offering its IT infrastructure for business. Similarly, in Vietnam, CEP, a non-profit microfinance institution, recently entered into a comprehensive cooperation agreement with Saigon Bank to help provide the CEP's customers with convenient and cost-effective services from Saigon Bank.

2 Identity Systems in the Philippines

UN Sustainable Development Goal 16.9 aims for "legal entity for all, including birth registration". An identity is an essential tool that is needed for every individual to assert their existence, be it for voting, obtaining access to government and private services, or for access to financial services. Development organizations are increasingly realizing the importance of an identity system in all countries and are focusing on enabling Identity systems. Globally, 1.5 billion people in the developing world lack any form of officially-recognized identification, either paper or electronic. Countries that have a robust birth registration system find it easier to progress to a national identity system – a *foundational identity* issued by governments to citizens and authorized aliens. This identity is different from any *functional identity* system, e.g. a voter's ID card, etc. that is issued for a specific purpose of voting.

The national ID can be either digital or physical in terms of data collection, storage, and the form of the ID itself (e.g., smart cards, etc.) The World Bank defines digital identity as a "collection of electronically-captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions".

New digital technologies are enabling more countries to adopt digital national ID systems, end-to-end. The data is captured and stored digitally and an individual's can be verified digitally. In some cases, captured data include biometrics (e.g., Aadhaar in India). Some countries that are adopting biometrics have had weak birth registration systems and the use of biometrics helps ensure uniqueness and the establishment of a robust identity system.

Digital national IDs not only help in digitizing the KYC process but also improve the robustness of the anti-money laundering (AML) regime in any country. The US Agency for International Development (USAID) has stated: "By leveraging the digital footprints of a connected population, digital ID opens new routes to inclusion for people who lack formal documentation."[36] With this understanding in mind, the Philippines has decided to develop an integrated digital national ID system.

Box 1: Components of the Philippines identification system

- PhilSys Number (PSN)
- Full Name
- Sex
- Blood Type
- Marital Status (Optional)
- Place of Birth
- Date of Birth
- Address
- Filipino or Resident Alien
- Mobile Number (Optional)
- Email Id (Optional)
- Front Facing Photograph
- Full set of Fingerprints
- Iris Scan
- Other Identifiable Feature as Determined in Implementing Rules and Regulations

The Philippine Identification System or PhilSys is to be established as a single national identification system for all citizens and resident aliens, eliminating the need for other forms of identification when accessing public and private services. PhilSys aims "to promote seamless delivery of service, to improve the efficiency, transparency, and targeted delivery of public

and social services, to enhance administrative governance, to reduce corruption and curtail bureaucratic red tape, to advert fraudulent transactions and misrepresentations, to strengthen financial inclusion, and to promote ease of doing business."[37] To achieve this, PhilSys aims to deploy a resilient digital system that can ensure the security of collected data. The government also recognizes the private sector's role in the growth and development of the country and seeks to provide all 'appropriate incentives to mobilize private resources' to scale the adoption and usage of PhilSys.

2.1 Philippine Identification System

For almost two decades, the attempts by the Philippines government to establish an integrated national ID system had faced opposition on the basis of constitutional and data privacy concerns. However, the Senate and the House of Representatives in the Philippines Congress passed the Senate Bill No. 1738 known as the "Philippines Identification System Act of 2018"[38] in March 2018, which was approved and signed into Law by the President of the Philippines, His Excellency President Rodrigo Roa Duterte, on August 6, 2018, and became Republic Act No. 11055[39]. The Act seeks to establish the Philippines National Identification System as a means to provide a valid proof of identity for all citizens and resident aliens. PhilSys seeks to harmonize, integrate and interconnect 'countless and redundant' government ID cards with a biometric-based national identification system which would eventually help in simplifying all public and private transactions.

The new Act permits the establishment of an "PhilSys Identity Platform" that will be administered by the Philippines Statistics Authority (PSA) to enroll Filipinos and resident aliens, and authenticate them for conducting public and private transactions. It is also recommended in the Act that every 10 years Filipinos and resident aliens enrolled under the program renew their registration to ensure continued accuracy. Box 1 lists all the components/data elements of the PhilSys.

2.2 Existing Unified Multi-Purpose Identification (UMID) Scheme

At this stage, it is important to review the existing identity system prevalent in the Philippines for its coverage and effectiveness.

For nearly two decades, the Philippines government has made attempts to establish a national ID System, but every time these efforts have faced resistance on the grounds of privacy and constitutional validity. In 1996, Administrative Order No. 308 was issued, adopting a National Computerized Identification System. The order was declared unconstitutional by the Supreme Court on the basis that legislative approval was required. In 2005, Executive Order No. 420 (EO420) was issued, requiring all government agencies and government-owned and controlled corporations to harmonize their ID systems. This order was also challenged on the grounds of privacy but was upheld by the courts as it

applied only to government agencies that issue ID cards as part of their functions, and its issuance was within presidential authority.

The 2005 order gave rise to UMID card, which is issued to the members of SSS (Social Security Systems), Government Service Insurance System (GSIS), PhilHealth and the Home Development Mutual Fund (PagIBIG fund). Since its launch in 2010, the government has issued approximately 10 million UMID cards within a population of 100 million. Through UMID enrolment, a beneficiary obtains a 12-digit Common Reference Number (CRN) that is shared with the service provider as a unique ID. This number is then used for printing service-specific UMID cards. UMID, in its present form, is more of a functional ID whereby identification is dependent on the presentation of the card to obtain specific government services.[40]

Has UMID solved the ID challenge?

The scope of this document excludes description of UMID card enrolment. However, the weaknesses of the card in the context of the promotion of financial inclusion are presented in table 5. These weaknesses should be treated as lessons learned for the design of the new PhilSys ID. The *Identity for Development in Asia and the Pacific* report published by the Asian Development Bank in 2016, identifies the key challenges of the current UMID system.

Table 5: UMID card drawbacks in promoting financial inclusion

	Gap	Description
1.	Lack of universality	The card is issued to a limited set of beneficiaries obtaining specific government services. This lack of universality is one of the primary reasons why less than 10 million people have been enrolled since 2010. In the present form, UMID excludes minors, the unemployed, people working abroad, and resident non-Filipinos.[41]
2.	Functional ID and not foundational ID	UMID card is used to obtain specific government services with limited use across different schemes and services.
3.	Not linked to Civil Registration and Vital Statistics (CRVS)	UMID does not check the validity of enrolment data with CRVS. Therefore, there is the possibility of a loss of integrity of data through discrepancies between data of the same person in CRVS and the agency database issuing the UMID. Also, there is no means to automatically update the status of an UMID card holder for life events like marriage, death, etc.
4.	Data security	During enrolment and until the time the UMID card is issued, individuals' data passes through systems of multiple agencies in an unsecured format.

	Gap	Description
5.	Limited biometrics data	Biometric data of only four fingers is captured for identification and de-duplication. This reduces the effectiveness of de-duplication in large population size like the Philippines.
6.	A limited number of enrolment agencies	At present, only three agencies act as enrolment agencies — SSS, GSIS, and PhilHealth, which limits coverage.
7.	Offline authentication only	While central registry of CRN maintained by PSA has provisions for online authentication, the feature is however not used currently. UMID cards contain an electronic chip that stores both demographic and biometric data that can be verified locally. However, physical verification of the UMID card is the most widely used method. Although the offline mode works, the authenticity of the card and information stored on it cannot be guaranteed.
8.	No single source of truth	Agencies issuing UMID card can take data update request without ensuring that the same update has been applied to central PSA registry

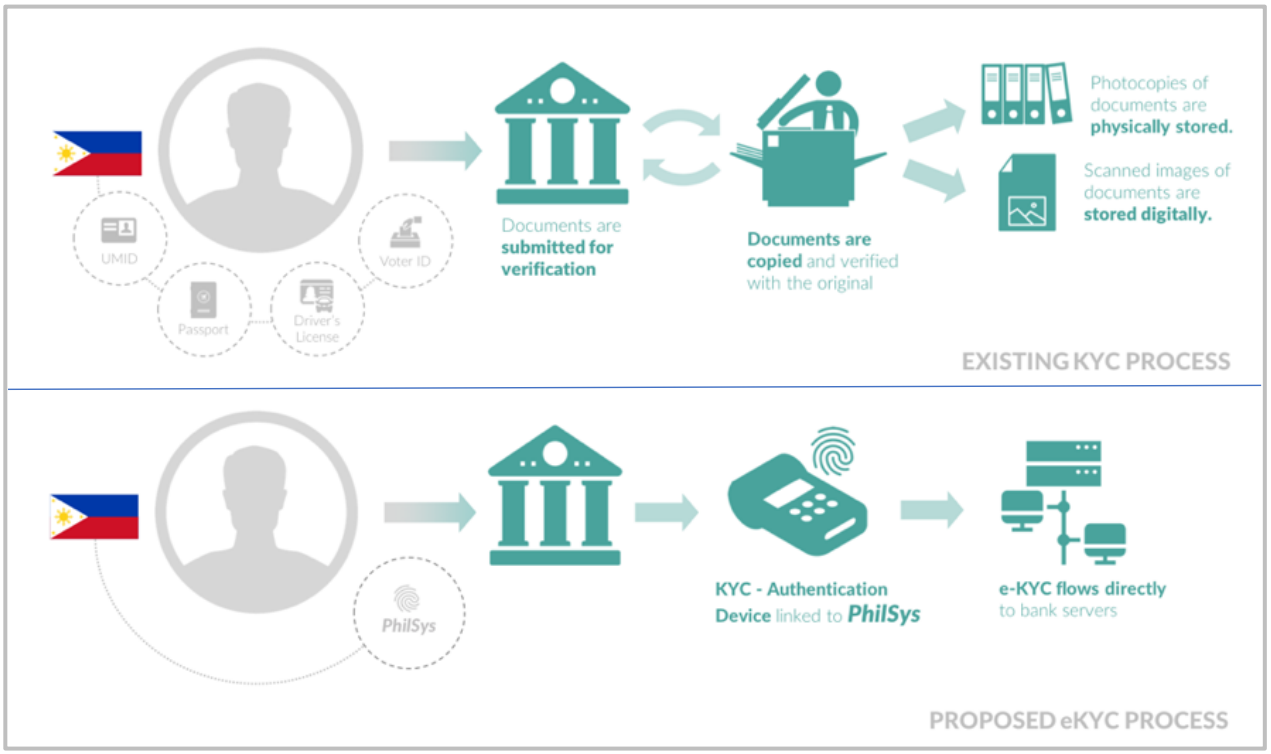
3 Digital ID – A Critical Success Factor for Financial Inclusion

Digital ID can help increase financial deepening in any country by improving access to payments, savings, credit, insurance, and investment products in ways outlined in the following subsections.

3.1 Reduced Cost of Customer KYC (CDD— Customer Due Diligence)

Digital ID has the potential to reduce customer onboarding costs by as much as 80 percent, making customer acquisition a more viable business proposition for FSPs. For example, in countries like India, which have a near-universal biometric-based ID (termed Aadhaar), it has been estimated by the GSMA that the Aadhaar-enabled e-KYC platform reduces the cost of KYC processes from INR40 (60 US cents) per customer to INR5 (7 US cents). This significantly lowers the overall cost of customer acquisition.[42] In other geographies including the Philippines, the cost of customer onboarding is in the range of US$5-10 each, which is a disincentive for FSPs to offer payments, savings, or other products such as micro-insurance or micro-investment for low-income customers. Due diligence of low-cost customers, enabled by digital ID, makes it possible to offer sachet-sized products to suit low-income consumers. PhilSys thus provides an opportunity to the FSPs to acquire customers at a much lower cost.

Figure 4: Comparison of existing paper-based KYC and e-KYC Processes



3.2 Robust Anti-Money Laundering Framework

In addition to lowering costs for the providers, a digital ID has the potential to improve AML compliance as the digital ID would be a unique identifier across the financial sector. It would be easier to identify incidents of fraud as individuals would be uniquely identifiable and traceable. This could enable a more robust AML framework in the country without leading to exclusion. A foundational digital ID, then, would be the right balance between robust AML and universal inclusion. A Financial Action Task Force (FATF) guidance note of 2013 (updated 2017) mentions India's Aadhaar system as the 'identity infrastructure' that would help further financial inclusion while strengthening AML/CFT implementation.[43]

3.3 Cheaper, Easier and De-risked Completion of Transactions

In addition to one-time customer onboarding, a digital ID has the potential to be used as a factor of authentication by FSPs, even replacing transaction tokens. For example, instead of issuing magnetic stripe (magstripe) or chip-based cards (expensive for both the provider and the outlet), FSPs could leverage the authentication services of a digital ID. For example, millions of people in India transact on their bank account by using just their Aadhaar number and fingerprints or iris scan at an agent location. This has helped banks in India yield significant savings for issuance of cards, token management (re-

issuance of lost or mutilated cards), and PIN management. From the consumer perspective, it has also empowered illiterate populations to operate their accounts. For example, ease at agent location without any risk of revealing their PIN, hence offering better consumer protection.[44] This functionality can also bring value to the marginalized populations that lack mobile devices by facilitating transactions at agent locations as all one requires is their biometric.

3.4 Robust Credit Assessment

In many geographies, the credit assessments are not trusted due to information that is incomplete, unreliable, or completely absent. The providers then use various "fuzzy" matching techniques to remove duplicates from their databases. For example, if an individual has defaulted on a loan obtained from Bank A using the tax ID and another loan from Bank B using a driver's license (with some other demographic data such as a different year of birth), the credit bureau would not be able to detect whether it is indeed the same person who has defaulted on the two loans. However, the insertion of a robust, unique identifier such as the digital ID in the credit portfolios of banks would ensure that the credit bureau would be able to detect that it is indeed the same individual who has defaulted. This would significantly enhance trust in the credit reference checks.

3.5 Effective Social Cash Transfer Programs

In some countries, including the Philippines, social transfer payments are made in cash, which entails high risk and is administratively expensive. The presence of a universal digital ID can enable digital account opening for program beneficiaries, which would be faster and cheaper, especially in reaching those in remote areas. Once accounts have been opened, direct transfers can be made into the beneficiaries' accounts, thereby reducing risk and administrative costs, while also enabling access to formal financial services. Additionally, a digital ID would provide increased accuracy compared to what is achievable using a physical identity and allow FSPs to streamline and automate many processes. For example, digital verification of beneficiaries in programs such as the Pantawid Pamilyang Pilipino Program (4Ps) in the Philippines would help reduce administrative costs and eliminate "ghosts" or duplicate beneficiaries. For example, the Philippines' Commission on Audit[45] observed in its 2017 report that PHP5.39 billion (US$100 million) was unclaimed in Land Bank accounts for over-the-counter beneficiaries of the 4Ps. This could have been reduced if there was a mechanism to authenticate the program beneficiaries using either one or both of PSN and biometrics at the time of disbursement through Land Bank. The unclaimed amount could have been repatriated to the account of the Department of Social Welfare and Development (DSWD) at the end of each cycle.

3.6 Innovative Digital Financial Offerings

Digital IDs affords financial innovators the ability to deliver end-to-end digital offerings. According to the World Economic Forum (2016), the process of identifying customers is

one of the critical barriers to deploying pure digital products. Without digital ID platforms, innovators have had to rely on pseudo-digital channels (e.g., photographing physical ID documents) or on KYC processes of established FSPs, thereby decentralizing a critical piece of the product/service offering. For example, it is now possible to start a mutual fund investment in India with just digital verification of ID using Aadhaar, thus enabling millions of small investors to diversify their investment portfolio. Another pertinent example is from Kenya where the Central Bank of Kenya was able to offer m-Akiba bonds (government securities issued through mobile money) for active retail participation in units of about US$30. Similarly, digital ID infrastructure such as PhilSys could enable online verification of identity, thereby laying the foundations of innovation in the payments, credit, insurance, and securities markets.

4 Harnessing the Potential of PhilSys in Promoting Financial Inclusion

4.1 Breaking the Barriers to Financial Inclusion

PhilSys, with its potential to make account opening, transaction authentication, and validation highly efficient and cost-effective, would result in not just greater access to financial services but will also reduce the underlying costs for all the associated entities. This in turn would result in higher usage of all financial services. Using a unified system to accurately and digitally identify individuals, PhilSys has the potential to improve the coverage and robustness of the credit assessment system of bureaus, financial institutions, and fintech companies. Most importantly, it would allow accurate identification of social welfare beneficiaries and ensure efficient delivery of public services and would also help in mitigating fraudulent transactions in conditional and unconditional cash transfers (CCT/UCT).

In this section, we will explore how PhilSys can play a crucial role in overcoming the barriers to financial inclusion as discussed in section 2.5. It is, however, paramount to recognize that the rollout of PhilSys cannot mitigate some of the challenges without the implementation of accompanying legal and regulatory changes.

Table 6: Role of PhilSys in overcoming the barriers to Financial Inclusion

	Barriers	Description
1.	Lack of digital identity and the platform	PhilSys is a step towards creating a digital identity platform that will assume the form of a foundational ID. This could be used for multiple purposes ranging from establishing ones' identity to the delivery of services by both private and public sector institutions.
2.	Skewed access to financial services through banks, MFIs, and other financial institutions across provinces	One of the key reasons for unequal access to financial services is lack of a valid identity to allow targeted delivery of financial products and services. Assuming unbanked and underserved people in rural areas are issued a verifiable digital ID, it will become simpler for financial institutions to uniquely identify their beneficiaries/consumers, create and maintain their financial risk profiles, allow risk-free online remittances so on across the provinces.
3.	High transaction cost at banks and other MFIs	As PhilSys is proposed to be a digital ID, it has the potential to substantially reduce KYC costs for the FSPs by facilitating paperless and remote onboarding of customers. It is expected that some of these cost reductions will be passed on to the consumers as lower cost for services.
4.	Low adoption of technology by	The adoption of PhilSys as a foundational identity and authentication system in a digital economy will compel

	Barriers	Description
	smaller financial institutions	downstream financial applications to adopt the technology. This will play a huge role in catalyzing the development of innovative tech-enabled financial solutions and promote PhilSys authentication as the primary method of uniquely identifying beneficiaries/consumers. This would not only propel the growth of the fintech industry, but the increased competition would ultimately lead to the creation of accessible tech solutions for smaller financial institutions like rural and thrift banks.
5.	Unreliable credit scoring framework	Credit scoring methods are critical to the design of credit and other financial products. This cannot be performed effectively at scale if the identity of the beneficiary/consumer is not uniquely established. PhilSys can potentially fill this gap by linking financial profiles of customers/ beneficiaries in various databased to create a more effective and consolidated near real-time financial profiles of people.

4.2 Functions and Features of the Philippine Identification System

As stated above, PhilSys is envisaged as a foundational ID that can uniquely establish the identity of the holder and can be verified digitally. However, in the context of financial inclusion it must have certain features to perform the functions detailed in table 7:

Table 7: Functions and Features of PhilSys

	Functions	Features
1.	**Enrolment**	As per the Republic Act No.11055, components of PhilSys have already been identified. However, it is essential that strict monitoring procedures are devised to verify documents submitted in support of demographic information. It is also necessary to ensure capturing of good quality biometrics that meets the minimum operational requirement. An effective enrolment procedure will be key to uniquely identifying beneficiaries/consumers during service delivery. In developing countries, particularly India and Pakistan, it has been observed that people living in rural areas or belonging to lower economic groups do not have a birth certificate, which is a critical input to the enrolment process. In such cases, exception processes must be invoked to retain the spirit of inclusivity. As an example, in India enrolment process permits 'introduction' by a designated Aadhaar holder for a new enrollee who doesn't

	Functions	Features
		possess a birth certificate. The ID authority designates such 'introducers' by their reputation in their area of residence and familiarity with people in their communities; typically, village heads, local representatives, etc.
2.	**Authentication**	Authentication is a vital function of a digital identity platform that allows service providers to digitally verify the identity of their beneficiaries/consumers in the real time. The PhilSys platform must be designed as an online platform that will enable authentication of PhilID holder using demographic information and/or biometric information anytime anywhere. The platform must also contain a feature to return demographic information of the individual undergoing authentication with the purpose of completing e-KYC.
3.	**Authorization**	PhilSys will give the authorization to deliver a service upon successful authentication. PhilSys must be designed in such a way that response to an authentication request, whether a simple “yes/no” or KYC data, can be used by downstream applications for service delivery.
4.	**Consent framework**	Data privacy considerations must always be given priority while designing the digital Id platform. No demographic data or biometric data must be shared with a third party unless consent is obtained from the concerned PhilID holder.

Figure 5: Financial Services and Digital Id Ecosystem

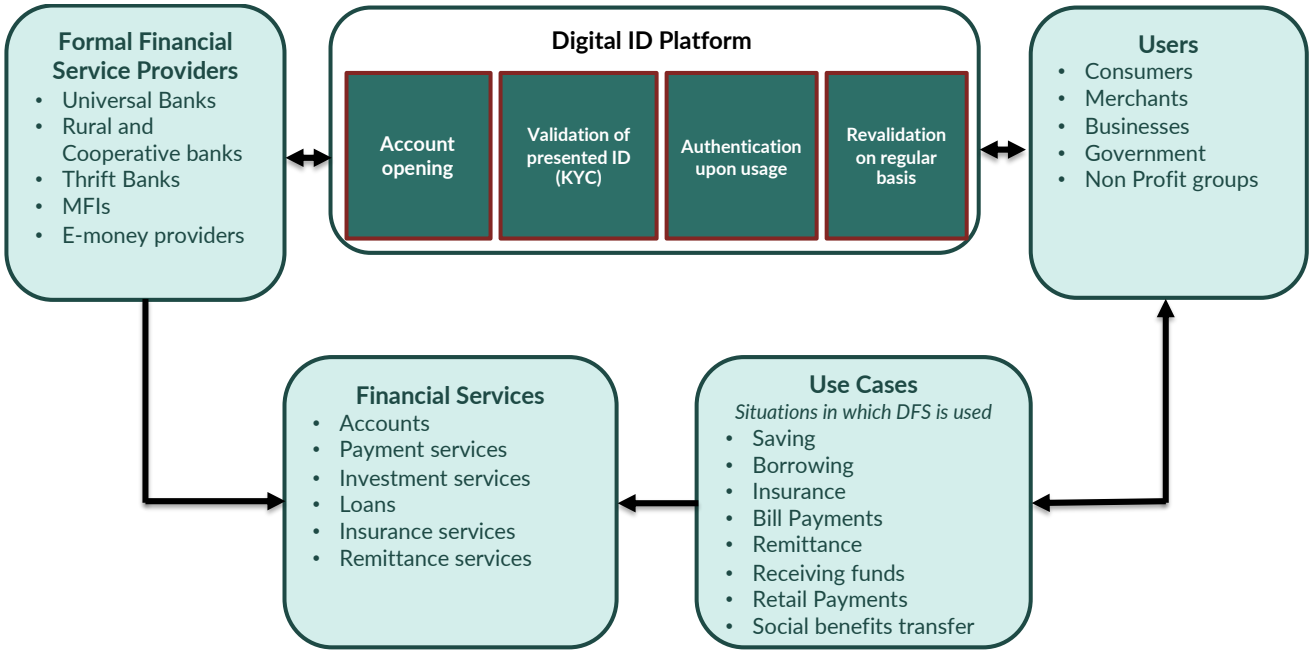


Figure 5 is a representation of the ecosystem that leverages a digital ID platform for service delivery. Building on the success of its initiatives, the Philippines government is now keen to create an enabling financial ecosystem that utilizes digital technology as a catalyst for financial inclusion. Digital technology with its ability to reduce transactional costs has massive potential of serving the largely untapped low-income market and support the needs of all classes of customers in a sustainable, convenient, and affordable manner.

4.3 Enabling Industry Developments

While a digital identity is a necessity to operationalize an ecosystem that promotes financial inclusion effectively, there are other enablers that play a key role in achieving the end objectives. The following subsections describe the National Retail Payment System (NRPS) strategy of BSP and the role of e-money with relevance to achieving the objective of financial inclusion. We will also outline the role of Self-Sovereign ID System (SSIS) envisaged to be a common infrastructure capable of storing KYC information of every customer in a distributed ledger.

4.3.1 National Retail Payment System

One of the critical factors in promoting financial inclusion is the availability of a payment system that can be used for government-to-person (G2P) and person-to-person (P2P) remittances, as well as from merchant payments. This payment system must be able to transact online and must have a substantial cash-in/cash-out infrastructure, allowing people to move money from cash to digital in their local neighborhoods. It is also natural to expect that for such an online payment system to function effectively, participating

individuals or institutions must have a financial address — a bank account, mobile money account, digital wallet, etc. To further establish the ownership of such accounts, authentication on the basis of a verifiable digital ID becomes essential. The Philippines national payments system could be stronger and more functional, as well as cheaper for providers and customers, if it is enabled using a digital ID system.

As a forerunner to the development of the country's backbone for an efficient payments infrastructure, BSP achieved critical milestones in 2017 with the launch of the Philippine Payments Management Inc. (PPMI) in June, followed by the issuance of the NRPS circular in November 2017. PPMI is an industry-driven, self-governing body that aims to catalyze the responsible development and operations of the country's retail payment system. NRPS, launched in 2015, is a policy and regulatory framework that seeks to promote the efficiency and safety of retail payments in the country, as characterized by the increased usage of digital payments, from the current 1 percent to 20 percent by 2020. The NRPS is envisioned to be a platform for delivering innovative financial products, particularly those designed for the low-income market. BSP issued Circular No. 980 on 6 November, 2017, which operationalizes and enforces the adoption of the NRPS principles by the BSP-supervised financial institutions. NRPS principles promote interoperability, "coopetition", level playing field, and transparent and fair market pricing. Central to the NRPS platform are the multilateral clearinghouse agreements for payment schemes that will facilitate convenient, affordable, and secure fund transfers between bank and e-money accounts. The two priority payment schemes are 'PESO Net' for batch fund transfer credit, and 'InstaPay' for real-time, anytime, low-value transfer credit.

'PESONet', launched November 2017, is a batch electronic fund transfer (EFT) credit stream and the country's first automated clearing house under the NRPS that was established to help bring about an interoperable ecosystem for seamless electronic fund transfers and payments. 'InstaPay', launched in April 2018, is an EFT service that allows customers to transfer Philippine Peso (PHP) funds almost instantly between accounts of participating banks and non-bank e-money issuers in the Philippines. Both 'InstaPay' and 'PESONet' are expected to potentially contribute to the shift from a cash-based economy towards a cash-lite economy, in line with emerging global trends.

To leverage NRPS as a critical enabler in further expansion of financial inclusion, it is recommended that NRPS promotes the use of PhilID or its token as a financial address whereby individuals are identified uniquely on the basis of their PhilSysId and demographic data and/or biometric data, for seamless fund transfers.

4.3.2 Electronic Money (E-Money)

BSP's pioneering regulatory framework for e-money issued in 2009 played a positive role in creating an enabling regulatory framework that provides an open and level playing field, allowing both bank and NBFIs — including mobile operators — to offer mobile money services. Considering that mobile phone users outnumber those with bank accounts, mobile banking, and e-money also present a significant opportunity to help Filipinos access financial services. In 2015, there were 51 million unique mobile subscribers in the

country, with a smartphone penetration of 59 percent. In 2017, the total number of registered e-money accounts was 11.4 million.[46]

In the Philippines, fintech services are mostly dominated by e-money service providers such as Globe Cash, Smart Money and a few others. Apart from e-money, there are payment service providers, including Dragonpay, Paymaya, and Mynt; remittance service providers like MyRemitHub; and digital lending service providers like Lendr & Loan Solutions.ph. In recent years, fintech companies offering financial services based on blockchain technology have started operations: Rebit, BuyBitcoin.ph, and Bitmarket.ph. Although BSP does not regulate cryptocurrencies, it recognizes virtual currency (VC) systems have the potential to revolutionize the delivery of financial services, particularly for payments and remittances, in view of their ability to provide faster and more economical transfer of funds, both domestic and international, and their potential to further support financial inclusion.[47]

At present, e-money service providers perform KYC of their customers using a government-issued ID card. It is recommended that they are advised to use authentication through the PhilSys platform on the basis of customers' PhilID, demographic information, and/or biometric data. Using one PhilSysId across all e-money accounts and bank accounts will slowly lead to the creation of a financial profile of people that can be used for design and roll-out of new financial products and services.

4.3.3 Self-Sovereign ID System (SSIS)

SSIS, owned by Bankers Association of Philippines (BAP), is envisaged by the participating banks to be a common infrastructure that stores KYC information of every customer in a distributed ledger. This ledger facilitates access of KYC information to all member banks for account opening purposes. Development of SSIS is expected to reduce KYC costs and time taken to onboard a new customer by avoiding redundancies caused by dispersed systems.

As per the current design of SSIS, each new customer will submit 11 data elements, including name, date of birth, address, mobile number, and tax identification number (TIN) to uniquely identify themselves. Apart from capturing these data fields, SSIS also facilitates uploading of other identification documents (copies of passport, driving license, etc.).

While SSIS may prove to be a good starting point, it is crucial that a robust de-duplication capability is built in to avoid misrepresentation of information like name, date of birth, or TIN, either knowingly or unknowingly. Secondly, fixing of liability issues across member banks is to be considered by BAP for a scalable and robust implementation of the SSIS. Thirdly, commercial agreements between member banks must be put in place for the effective operation of the financial ecosystem. Fourthly, access criteria must be clearly defined to allow access by non-bank institutions. Lastly, it is imperative that the accuracy, consistency of the customer demographic data and address is maintained.

While BAP may take the above-stated considerations into account while designing SSIS, it might be prudent to consider seeding the SSIS database with the unique and verifiable PSN of each customer. Since one person cannot have more than one PSN, on account of biometrics-based de-duplication, the chances of misrepresentation of a customer will be significantly reduced.

5 Overview of Legal and Regulatory Requirements

An enabling legal and regulatory framework is essential to maximize the utility of digital national identification for financial inclusion. Following is a summary of critical legal issues that impact the use of digital identification for financial inclusion purposes, along with legal recommendations aimed at ensuring that the digital national ID scheme will enable financial inclusion to the greatest extent possible.

5.1 Remote Account Opening Using Digital Identification

5.1.1 Government Sanctioned Central Identification Platform

Republic Act No. 11055 or the Philippine Identification System Act (PISA) enabled PhilSys to serve as the government's central identification platform for all citizens and resident aliens in the Philippines. The PhilSys, implemented by the PSA, offers a ready and centralized system to which a digital national ID scheme that will enable financial inclusion may be integrated.

The law was enacted for the purpose of promoting "seamless delivery of service, to improve the efficiency, transparency, and targeted delivery of public and social services, and … to strengthen financial inclusion" (PISA, Sec. 2). The law recognizes the role of the private sector and provides incentives to mobilize private resources for the purpose of promoting the use and ensuring the maximum efficiency of the national ID system.

Under the PISA, "[a]n individual's record in the PhilSys shall be considered as an official and sufficient proof of identity" (Sec. 6). The PhilSys has three components: (i) PhilSys Number or PSN; (ii) PhilSys Registry; and (iii) PhilID. The PSN is "a randomly generated, unique and permanent identification number that will be assigned to every citizen and resident alien upon birth or registration by the PSA." (PISA, Sec. 7a). The Phil Registry will contain the "PSN, registered records, and information of all person registered in the PhilSys" (PISA, Sec. 7b). The PhilID is a nontransferable card that will be issued to all citizens and resident aliens under the PhilSys (PISA, Sec, 7c), and shall serve as the official, government-issued ID document of cardholders in dealing with all national government agencies, local government units, government financial institutions, and all private sector entities (PISA, Sec. 7c[2]). The PSA is also mandated by law to issue a mobile PhilID.

The law requires entities to honor and accept the PSN (subject to authentication) notwithstanding the absence or non-presentation of a PhilID (PISA, Sec. 13).

Information to be collected and stored under the PhilSys is limited to the fields mentioned in Box 1. Both government and private entities (BSP and BSP-supervised financial institutions or BSFIs) are legally required to honor and accept, subject to authentication, the PhilID as a person's proof of identity. The law states that, "The PhilID shall be honored and accepted, subject to authentication, in all transactions requiring proof or verification

of citizens or resident aliens" (PISA, Sec. 13). The transactions explicitly include "opening of bank accounts and other transactions with banks and other financial institutions".

Under the PISA, "for purposes of establishing the proof of identity for transacting business with any government agency, the presentation of the PhilID or PSN shall constitute sufficient proof thereof, subject to proper authentication". Private entities such as banks and other financial institutions are also required to accept the PhilID or PSN as valid proof of identity (Sec. 12).

Entities must mandatorily accept the PhilID or PSN. Any person or entity who, without just and sufficient cause, refuses to accept, acknowledge and/or recognize the PhilID or PSN, may be fined in the amount of PHP500,000. Hence, BSFIs, in establishing and verifying customer identity, are mandated to accept and honor the PhilID or PSN as an identity for KYC purposes. Nonetheless, there are some additional data that BSFIs are required to collect that are not included in the PhilID or PhilSys, such as employment details, source of income, TIN, SSS, and GSIS numbers.

5.1.2 Recognition of Electronic Transactions

One key building block of a legal regime for digital ID is a strong legal framework for the use of electronic or digital data in electronic commerce. The Electronic Commerce Act of 2000 [48] (ECA) establishes legal certainty with respect to digital signatures and transactions. In particular, the ECA provides for full legal recognition of data, documents, and signatures submitted electronically (Sec. 6-8).

With respect to electronic documents, the ECA clarifies that any legal requirement for a document to be "in writing" can be met by an electronic document, provided that the integrity, reliability, and authenticity of this document can be verified. Furthermore, any legal requirement for a document to be "presented or retained in its original form" can be met by an electronic document if there is sufficient certainty regarding the document's integrity (Sec. 7 of the Act).[49]

Similar provisions apply to electronic signatures (e-signatures). They are presumed to be equivalent to written signatures as long as the e-signature process follows a prescribed procedure that is reliable, appropriate, and unalterable (Sec. 8).

The provisions of this Act have been supplemented by the Act's Implementing Rules and Regulations (IRR_ECA)[50] and the Supreme Court of the Philippines' Rules on Electronic Evidence (REE),[51] which accord equal weight to electronic documents and signatures in legal proceedings.

5.1.3 Remote Customer Identification and Verification

The Anti Money Laundering Act of 2001 (AMLA)[52] requires "*covered persons*" (which include, among others, BSFIs) to "establish and record the true identity of their clients based on official documents" (Sec. 9A). The definition of "official documents" as provided in the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9160, as

Amended (RIRR_AMLA) [53] includes any Philippine government-issued documents (RIRR_AMLA, Sec. 3M). Thus, a government-issued national ID can be used to meet this requirement. Customer information from individual persons that must be gathered includes the following (RIRR_AMLA, Sec. 9A(1)(b)(i)):

- Name
- Date/place of birth
- Name of beneficial owner (if applicable)
- Name of beneficiary (if applicable)
- Current address
- Permanent address
- Contact number or information
- Nationality
- Specimen signatures or biometrics
- Nature of work and name of employer (or nature of self-employment/business)
- Source of funds/property
- Tax Identification Number, Social Security System number, or Government Service Insurance System number (if applicable)

Pursuant to its mandate to issue rules and regulations implementing the AMLA, the BSP Pilipinas issued BSP Circular 950[54] requiring covered persons to undertake customer due diligence in four instances: (i) when establishing business relations with any customer; (ii) when undertaking any occasional but relevant business transaction for any customer who has not otherwise established relations with the covered person; (iii) when there is suspicion of money laundering or terrorism financing; or (iv) when there is doubt about the veracity or adequacy of previously obtained customer data (Sec. 4).

The same BSP Circular defines the term “business relations” as the “opening or maintenance of an account or the provision of financial advice by the covered person to a customer”. Thus, as long as a person opens or maintains an account with a BSFI, such BSFI needs to conduct KYC procedures on the said person. Moreover, the BSFI also needs to conduct KYC procedures on a person who may not have an account with the BSFI but still performs a business transaction.

As part of the customer due diligence process (otherwise known as the Know Your Customer (KYC) procedure), the Rules and Regulations require “face-to-face contact,” either (i) at the beginning of the business relationship; or (ii) “as reasonably practicable so as not to interrupt the normal conduct of business,” so long as money laundering risks are effectively managed (RIRR_AMLA, Rule 9A(1)(a)). The RIRR of the AMLA does permit the use of information and communications technologies for the purposes of compliance with the “face-to-face contact” requirement (RIRR_AMLA, Sec. 9A(1)(a)[55]; BSP Circular 950[56], Sec. 6), provided that the BSFI is already in possession of and has verified the identification documents of the prospective customer prior to the conduct of the digital “face-to-face” interview and the entire procedure is documented. Furthermore, BSFIs may outsource the customer identification process to agents (RIRR_AMLA, Sec. 9A(1)(d)[57]; BSP Circular 950[58], Sec. 6). Nevertheless, some form of face-to-face meeting seems to be required.

If lower risks of money laundering or terrorism financing have been identified, providers may apply "reduced due diligence procedures" that are "commensurate with the lower risk factors," provided that there is no suspicion of money laundering or terrorism financing (RIRR_AMLA, Sec. 9A(2)(a)[59]; BSP Circular 950[60], Sec. 4). For "low-risk customers," providers may access "any document or information reduced to writing which the (provider) deems sufficient to establish the client's identity" (BSP Circular 950[61], Sec. 2). However, a face-to-face meeting is still required even when opening accounts for "low-risk" customers.

5.2 Customer Data Protection

5.2.1 Customer Consent

Requirements related to the sharing of customers' personal information are governed by Republic Act No. 10173 or the *Data Privacy Act of 2012* (DPA)[62]. The DPA applies to "personal information" (PI), which is broadly defined to include "any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual" (DPA, Sec. 3(g)).

The DPA also includes a definition of "sensitive personal information" (SPI), to which stronger protections apply. SPI covers PI related to factors such as a person's race, age, health, genetics, sex life, and religious or political affiliations, among others. It also includes social security numbers and other information issued by government agencies that is "peculiar to an individual" (DPA, Sec. 3(l)).

The DPA covers both biometric information and national ID numbers (i.e., the PSN). Biometric information is deemed to be SPI, as one could use this biometric information to obtain information about an individual's genetics. Similarly, as a unique identifier issued by a government agency, national ID numbers are also considered SPI.

Considering that both the biometric information and the national ID number are deemed SPI, a request to the centralized ID database to share this information can only be granted if the "data subject" (the individual whose personal information is being processed) has provided prior consent that is specific to the purpose for which the data are to be processed (DPA, Sec. 13).[63] Consent must be "freely given, specific, [and] informed" and must be "evidenced by written, electronic or recorded means" (DPA, Sec. 3(b)).

Recognizing the need to protect disclosures made by government agencies of personal information under their control to third parties, the National Privacy Commission (NPC) issued NPC Circular No. 16-02[64], prescribing guidelines on such transfers. All transfers made by government agencies to a third party for the purpose of performing a public function or providing of a public service must be governed by a data sharing agreement (NPC Circular No. 16-02, Sec. 1). Furthermore, the government agency charged with the collection of the personal data directly from the data subject, on its own, or through a

processor, shall obtain the consent of the data subject prior to collection and processing, except where such consent is not required for the lawful processing of personal data, as provided by law (NPC Circular No. 16-02, Sec. 4).

The PSA is required under the PISA to ensure that individuals are adequately informed upon registration for PhilSys about how their data will be used and how they can access their registered information and record history (PISA, Sec. 18). Reading the PISA together with the DPA and its related issuances, it appears that the PSA must still comply with the consent requirements of the DPA before any information about a data subject may be shared with a requesting entity, unless the sharing or transfer of any personal data is already authorized or required by law.

Providers face penalties for the unauthorized use or misuse of PI or SPI, ranging from fines to imprisonment. The following actions are all subject to penalties: (i) unauthorized processing (DPA, Sec. 25); (ii) processing for unauthorized purposes (DPA, Sec. 28); (iii) unauthorized access or intentional breach (DPA, Sec. 29); (iv) malicious disclosure (DPA, Sec. 31); and (v) unauthorized disclosure (DPA, Sec. 32). In all cases, stricter penalties are applied for misuse of SPI.

There are also civil and criminal penalties for the (i) utilization of the PhilID or PSN in an unlawful manner or use of the same to commit any fraudulent act or unlawful purpose (PISA, Sec. 19); (ii) use of the PhilID or PSN, or unauthorized possession of a PhilID, without any reasonable excuse by any person other than the one to whom it was issued or the possession of a fake, falsified, or altered PhilID (PISA, Sec. 19d); (iii) use of the personal data in violation of the allowed purposes in Section 12 of the PISA; and (iv) disclosure of data in violation of Section 17 of the PISA.

5.2.2 Theft or Misappropriation of Personally Identifiable Information

The DPA also addresses data security. Section 20 requires the "personal information controller"[65] to implement "reasonable and appropriate" measures to protect PI against a variety of risks, including "accidental or unlawful destruction, alteration and disclosure," "unlawful access, fraudulent misuse," or "any other unlawful processing." With respect to SPI maintained by the government, this information "shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission" (DPA, Sec. 22).

Penalties related to inadequate data security include: (i) penalties for negligence that enables unauthorized access to PI or SPI (DPA, Sec. 26); (ii) improper or negligent disposal of PI or SPI (DPA, Sec. 27); and (iii) concealment of security breaches involving SPI (DPA, Sec. 30). Any actions that are also classified as "*cybercrime offenses*" may also be punishable under the Cybercrime Prevention Act of 2012[66].

6 Key Design Principles of PhilSys for Supporting Financial Inclusion

The PhilSys system design is currently being finalized. In this section, we provide suggestions on the design of the PhilSys system that can help accelerate financial inclusion in the Philippines. Some of the suggestions include:

- **Physical card to be issued should be International Civil Aviation Organization (ICAO) compliant**: The PhilID Act 2018 states that the physical card (PhilID) is to be issued by PhilSys to all citizens and resident aliens registered under PhilSys. However, the Act does not specify the material to be used, e.g., Teslin, Polycarbonate or Polyvinyl Chloride (PVC) etc. While the choice of the substrate would depend on a number of factors including cost, it is suggested that the card should be compliant to the ICAO.[67] A card issued as per ICAO standards would be long-lasting and will be in accordance to international protocols if the card is to be used as a future machine-readable travel document. The card should also contain a machine-readable zone (MRZ) apart from the Quick Response (QR) code mentioned as per the Act. MRZ would make it easier for the FSPs to read the card digitally and speed the KYC process. The card should also contain physical security features that lend themselves to visual inspection at the time of physical card presentment. Some of the features suggested are micro-lettering, optically variable ink, latent image, etc. to prevent easy counterfeiting.

- **Authentication services to be federated:** As the level of assurance needed for a particular transaction depends on the specific use case, the PhilSys system should offer multiples modes of authentication. The authentication services offered should be based on any one or combination of the following factors for establishing the identity of an individual: something you have (e.g., ID card), something you know (e.g., PIN or password), or something you are (e.g., biometrics such as fingerprints, iris, etc.). The sector regulators (such as BSP) or the sector players would then be in a position to use any one or combination of factors of authentication, coupled with their own authentication system, to verify the identity of individual either for KYC or for purposes of other transactions (e.g., cash withdrawal, deposits, remittances, etc.). The details of the authentication (demographic/biometric etc.) are explained in the next section.

- **Demographic authentication should be available:** There would be instances where there may not be a need, or it would not be possible, for FSPs to use biometric authentication for customer ID (due to network connectivity, for example). For such cases, the PhilSys system should offer demographic authentication wherein the FSP could send the PSN and the name, date of birth, and so on to the PhilSys system and it could then confirm if the PSN and the demographic data match the one that is on record with the PhilSys. A use case that is envisaged is that a PSN-holder could send his/her PSN and name remotely through a mobile means using either USSD/SMS/ smartphone app to the FSP. The FSP could then send this demographic information to the PhilSys system and upon confirmation, allow opening of a financial account.

- **One-time password (OTP) based authentication:** The PhilSys system could also offer OTP-based authentication services where the OTP could be sent to a mobile number registered in the PhilSys database. This form of authentication can be used remotely (for non-face-to-face transactions) and offers the additional layer of consent of the PSN-holder for the opening of accounts by FSPs. For example, BSP could allow basic deposit accounts (as defined in circular 992 coupled with circular 950 on risk-based KYC) to be opened using OTP as a factor of authentication for e-KYC purposes.

- **Biometrics-based authentication:** As online biometrics represent one of the most robust factors of authentication that can be used by any PSN-holder (*barring biometric exceptions*), PhilSys should offer both fingerprint and iris-based authentication. The authentication system should return a "yes/no" or the e-KYC demographic data (name, address, photograph, etc.) depending on the use case. The biometrics-based authentication uses 'what you have' and provides for explicit customer consent.

- **Mobile ID option like 'mPhilID' to be explored:** As the Philippines has a very high penetration rate of smartphones at 59 percent, PhilSys could also consider offering a facility that allows a PhilID holder to download his/her PhilID profile (digitally signed, secure) on the smartphone using a mobile app. Thereafter, the mPhilID profile stored on the smartphone could be shared by the owner with any service provider in an offline manner using multiple sharing options; e.g. Viber, WhatsApp, e-mail, etc. As the shared ID profile would be digitally-signed, the service providers including FSPs would be able to verify the authenticity of the ID details. (Refer to the FAQs on India's mAadhaar).[68]

- **Development of authentication ecosystem:** PhilSys should promote an authentication ecosystem with clearly-defined policies, standards, legal obligations of users, pricing policy for users and device standards.

- **Use of open application program interface (API) architecture for authentication:** While PhilSys would establish its own set of security protocols and rules for the public and private sector players to integrate with the PhilSys system, it should follow an open API architecture for automation, efficiency and lower cost of operation.

7 Technology Infrastructure Overview

In order to achieve maximum benefit out of a country-wide digital ID adoption in the Philippines, financial institutions need to adopt technology that supports latest KYC, AML, biometrics, anti-fraud, and identity theft technologies as well as advanced authentication solutions. Acquiring new technologies that can access and verify digital identity will not only help expand the reach of affordable and efficient financial services among the unbanked but will also allow financial institutions to increase operational efficiencies and avoid hefty administrative overheads associated with identity, particularly around KYC and AML requirements.

Part of BSP's "Continuity Plus Plus" agenda is leveraging digital technology and innovation through fintech to allow more efficient delivery of financial services and products to everyone, specifically the financially excluded and vulnerable sectors of society. This includes supporting the inter-agency initiative to utilize the national ID biometric system and to allow remote onboarding of clients by leveraging innovative digital and mobile banking solutions. Using a shared KYC platform as a substitute to face-to-face KYC requirements over mobile phones, will not only make banking services accessible to low-income consumers without relying solely on a brick and mortar bank presence but will also help in creating a digital credit history for the financially unserved and underserved.

Incorporating digital identity in FSP systems will also promote greater trust amongst both the providers and the consumers towards adopting mobile wallets and e-money. For an archipelago like the Philippines, where providing a 100 percent physical banking access point coverage is a challenge, e-money is a safe, cost-effective solution to perform a plethora of financial transactions remotely and conveniently. Performing e-KYC for e-money accounts at telecom agent touchpoints by making use of PhilSys will facilitate easier customer onboarding with reduced cost of KYC fulfillment. This could ultimately allow e-money apps like PayMaya or G-cash to transfer that benefit back to the customers, furthering its adoption and usage.

Although e-KYC has the undeniable capability of bringing the overall cost of KYC fulfillment down, it still has an initial adoption cost which would vary on the basis of the current digital capacity of an institution. The overall cost of hardware and software procurement will play a vital role in the uptake of these integrated solutions, especially for smaller institutions to calculate their return-on-investment (ROI) on the cost of acquisition and maintenance. It is, therefore, imperative to understand the level of technology adoption at most financial institutions in the Philippines today.

7.1 Information Communications Technology (ICT) Gap Assessment for Financial Institutions

Most financial institutions in the Philippines are at some level of technology adoption. While new and sophisticated financial technology solution providers have entered the

market, a majority of banks are still using core banking solutions (CBSs) that were designed decades ago, and that makes it extremely difficult for banks to keep up with modern, rapidly-changing technological advancements. Stand-alone management information systems (MISs) are also prevalent, which is a serious barrier to progress since it prevents an institution having full access to its data.

Universal and commercial banks, accounting for more than 90 percent of the banking system's total resources,[69] are the most technically-capable financial institutions in the country. While almost all universal and commercial banks have adopted integrated CBSs, most top-level and mid-level banks are offering services like online banking, mobile banking, and paperless branch banking. Most commercial and universal banks are financially and technically well-placed to acquire the latest hardware and software required to incorporate digital ID and allow online authentication and remote customer onboarding.

The thrift banking system – comprising savings and mortgage banks, private development banks, stock savings and loan associations, and microfinance thrift banks – is at a reasonable level of tech adoption. While some thrift banks have implemented integrated CBSs, most others still rely on standalone MIS. However, stakeholder interviews revealed that bringing thrift banks on-board for an online, biometric-based authentication system should not be challenging as they might be willing to invest in a solution that ultimately helps them to improve their risk assessment processes.

Rural and cooperative banks naturally have the greatest presence in rural areas. However, this restricts many of these banks, especially the ones with a sizeable presence in extreme far-flung regions, from utilizing an integrated CBS since network access is unreliable. Rural and cooperative banks today are at varying levels of technology adoption. While approximately the 50 top-level rural banks are already live on CBSs, almost all mid-level banks and about 200-member banks of the lower category (having 1-5 branches, and about 10,000–20,000 customers), are using standalone MIS. Although most of these banks are now willing to adopt a centralized CBS, possibly on the cloud, geographical and network barriers might delay or disrupt their tech adoption for a considerable time. As such, most rural and cooperative banks would like to be offered a combination of both online and offline authentication options on the digital ID platform.

MFIs still have a long way to go in terms of their IT capacity. Currently, there are fewer than five MFIs that are fully digitized, while the remaining 80 percent are only equipped with standalone management information systems. Off-the-shelf CBSs do not seem to work for the MFIs, and they would be willing to use a shared platform/service that is developed specifically for the Philippines market. Bearing in mind the rural geographical spread of the MFI network, a combination of both online and offline authentication options for customer onboarding would represent the best solution.

7.2 Digital Financial Inclusion Ecosystem Adoption: Issues and Challenges

Although the Philippines is a global leader in social media usage, with 67 million internet and active social media users and the average user in the country spending almost 4 hours on social media[70], the current digital banking landscape in the country is not advancing in a similar fashion. As of 2017, there were only 7 million active e-money accounts, and most Filipino consumers still chose to pay bills over the counter. Regarding the supply side, financial institutions are still struggling with network challenges, the cost of acquiring the latest hardware and software, and an unclear understanding of how it might bring about cost-savings in the long run.

While the final structure of a financial service sector digitally-transformed and enabled by a digital national ID could take different forms, the degree to which the digital financial services (DFS) ecosystem adapts to the presence of a centralized digital national ID will largely depend on how the existing conditions and barriers are dealt with.

Lack of a compelling digital user experience

In terms of digital financial services, customers like to keep things simple, and they expect an easy-to-use, personalized, omnichannel experience for handling their finances, similar to what they experience in their social media and other online activities. It is essential for banks and other FSPs to create an engaging, yet simple to learn and use user interface, that is not only customer-centric but also provides a seamless user experience. It is only then that users can be hooked on to a digital banking solution and the trust developed is then utilized to sell them the most relevant products and services.

Lack of a reliable network infrastructure

According to Akamai's Q1 2017 State of the Internet Connectivity Report, the Philippines ranks the lowest among Asia Pacific countries for the average connection speed metric. Intermittent or no network connectivity in rural areas has not only prevented financial institutions from investing in an integrated MIS but has also created doubts among consumers in wholeheartedly adopting digital financial services. It is critical that the government pushes for reliable and complete network coverage, to allow hosting of the online financial services, and provide access to digital and mobile financial services in the remotest areas of the country.

Lack of an integrated, uniform IT solution

The majority of core banking solutions (CBSs) in the Philippines are legacy systems, which deploy out-of-date programming languages that can't easily be integrated with the rapidly changing IT platforms. Silo systems can also be a barrier to progress, especially when they prevent a bank from having full access to its own data. Financial institutions need to invest in a step-by-step holistic IT transformation, replacing their manual or legacy systems with real-time, modern banking solutions that adaptable and respond quickly to change.

7.3 Online/Offline Customer Onboarding Process Steps for Financial Institutions

Once the PhilSys is rolled out, the usage of the digital national ID for customer onboarding would depend upon the level of technology adoption for the financial institution in question. For the more technically advanced institutions, like the universal and commercial banks, online authentication or e-KYC is the preferred option whereas for the institutions in earlier phases of technology adoption, like thrift banks or rural and cooperative banks, an offline authentication would be more suitable. Finally, for the institutions restricted by limited network connectivity, like the rural banks and MFIs, a combination of offline and online modes of authentication would be ideal for seamless customer onboarding utilizing the PhilSys.

In the online method of authentication, the PhilSys number (PSN) – along with demographic data, biometric data or both of the PhilID holder – will be sent to PhilSys for authentication over a secure network. To leverage the PhilSys for a paperless, e-KYC, the financial service providers (FSP) will need to define the following operational procedures:

1. Ensure that the licensing requirements with the PSA are fulfilled to enable FSPs to access the PhilSys e-KYC service.

2. Ensure access to a reliable and secure network connection.

3. Deploy standardized hardware and software (including certified biometric readers) for utilization of e-KYC service across various delivery channels.

4. Develop or procure a software application to enable the use of e-KYC across various customer touch points as per PSA defined PhilSys Application Programming Interface (API) protocols.

5. Define a procedure for directing customer authorization to PhilSys for sharing e-KYC data with the financial institution. This authorization can be in **physical** (by way of a written explicit consent) or **electronic** as defined by PSA from time to time.

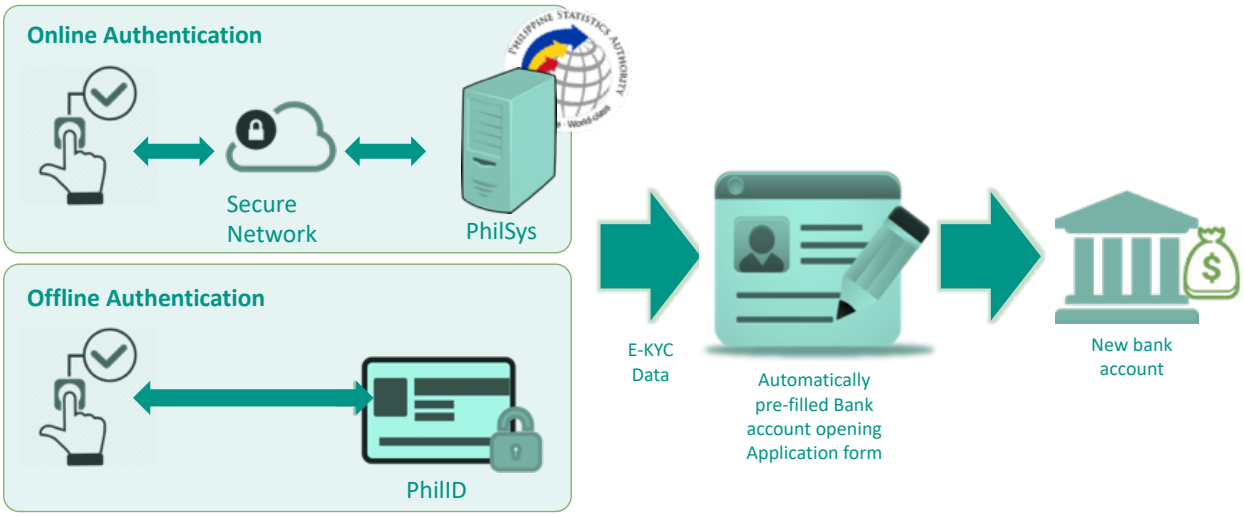
In the offline mode of authentication, PSN and other demographic and biometric attributes will be matched with those stored on the PhilID. FSPs must ensure that the following operational procedures are defined to utilize the offline authentication feature of PhilSys:

1. Ensure that the licensing requirements with the PSA (if any) are fulfilled to establish proof of identity upon the presentation of the PhilID.

2. Based on the design and features of the PhilSys (OTP-based, offline biometric-reader, QR code or mPhilSys) deploy standardized hardware and software for utilization of the offline authentication service across various delivery channels and customer touch points.

3. Define a procedure to ensure customer consent is taken before authenticating the data captured on the PhilID either manually or through an offline, software-directed process.

Figure 6: Opening a bank account using online and offline modes of authentication



It is recommended that online mode is the preferred means of authentication given that data stored on PhilID in the offline mode is 'trusted' which may not always hold, given the possibility of tampering of the PhilID card.

8 Cost-Benefit Analysis

Financial inclusion essentially means access to a bank or mobile money account for savings and payments, to credit for financial growth, and to insurance for managing risks. According to BSP's latest financial inclusion survey, at least 69 percent of adults in the Philippines do not have access to formal financial services, which is a huge barrier to implementing initiatives aimed at financial inclusion, poverty reduction, and eliminating inequality. In addition to the problem of low access to formal financial services, there is no common verifiable ID, currently in use, that can effectively promote targeted financial inclusion in the country to de-risk the operations of financial institutions and the governments that must identify their customers/beneficiaries accurately to prevent financial losses and leakages.

This section assesses the cost of using PhilSys to advance financial inclusion and the expected benefits. 'Cost' here refers to the expense incurred by financial institutions and governments to accept PhilID as a valid ID for remittances and service delivery only. However, it does not consider the cost incurred by PSA and other government agencies to create the infrastructure for enrolment and card issuance.

8.1 Costs

In order to leverage the PhilSys infrastructure, a significant amount of investment will be required by financial institutions and government departments to recognize the new form of ID as a valid ID and use it to authenticate the holders. The 'Act' clearly articulates that the PSA will issue PhilID to citizens and alien residents which will display and store requisite information to establish the identity of the holder in an offline or online mode. In order to use the PhilID, technology solutions must be developed to read data from the card in combination with biometric data to authenticate the holder in a robust and fool-proof manner.

While the cost of enrolment of Filipinos and resident aliens and issue of cards is out of the scope of this document, it would still be pertinent to mention the overall cost of the ID rollout. We can look to Pakistan where the incremental cost of issue of every new ID is US$8.00.[71] By contrast, India spends only US$1.20.[72] Costs indicated here are inclusive of enrolment and all other administrative costs. The higher cost incurred in Pakistan can be attributed to the fact that every resident of Pakistan is issued a plastic card with an embedded electronic chip, which is not the case in India where only a printed letter is issued as a medium to communicate the unique identity number.

Cost elements in this document are limited only to the expenditure incurred by the ecosystem (comprising financial institutions and DSWD) to adopt PhilID for unique identification of their customers/beneficiaries. Cost of adoption includes procurement of necessary software, biometric devices, card readers (chip or non-chip), integration with the PhilSys platform, and a database linking with PSN and other miscellaneous costs (see table 8)

Table 8: Estimated cost for PhilSys adaption by financial service providers (US dollars)

SL. No.	Description	Count	Rate	Total Cost	Comments
a)	PoS devices for agents	50,000	$250	$12.5 million	Portable devices which can be used in the field by pawnshops and e-money agents
b)	Software development & integration with PhilID platform	600	$25,000	$15 million	Cost towards development of software modules as standalone applications or as enhancements to CBS applications
c)	Fingerprint readers	90,000	$50	$4.5 million	Deployment by ~60,000 touchpoints of FSPs
d)	Iris readers	9,000	$130	$1.2 million	Deployment by ~60,000 touchpoints of FSPs
e)	Seeding of beneficiaries' records in Pantawid database (4P) with PSN	4,400,000	$0.50	$2.2 million	The count of 4.4 million is on the basis of the number of Pantawid household beneficiaries
			Total Procurement Cost	**$33.2 million**	
			Total Pantawid database seeding cost	**$2.2 million**	
			Total Cost	**$35.4 million**	

Assumptions:

i. Enrolment of all Filipinos and resident aliens will be completed within 12 months (as indicated in the Act)
ii. Above figures are only indicative and apply to a regular class of components. Actual cost may change at the time of procurement on the basis of quantity, complexity and rating of the devices and software
iii. Procurement of hardware will take place over a period of three years with 20 percent in the first year, 50 percent in the second year, and 30 percent in the third year. Also, a fixed depreciation rate of 20 percent has been used for hardware assets
iv. All 60,000 customer service points of the FSPs will procure at least one fingerprint device. However few of them will purchase two such devices. Therefore, a multiplying factor of 1.5 has been applied on the count of devices
v. Iris readers will be fewer in number, the count is assumed to be 10 percent of fingerprint devices
vi. A discount rate of 9 percent has been applied to arrive at the net present value (NPV) in the final cost-benefit analysis (CBA) table.

vii. Number of periods considered here is five years
viii. It will cost 50 US cents to seed each household record in Pantawid database with the PSN of concerned beneficiaries
ix. The cost of seeding (linking Pantawid beneficiaries to PSN) has been spread over a two-year period

Table 8 does not consider the cost of database digitization other than Pantawid and linking with PhilID. It is recommended that estimation for digitization and linking with PhilID is conducted on a case-to-case basis as cost varies with the current state of digitization and the complexity associated with the linking of a customer/beneficiary record with PhilID.

8.2 Benefits

Going by the experiences of other developing countries, use of digital national ID results in targeted delivery of services and also enhances the efficiency of service delivery, which is largely manual and suffers from losses at every point of a handshake between ecosystem partners. The following three key benefits have been identified in the case of Philippines: 1) the number of bank accounts will grow on account of a common and verifiable identity, which will result in significant reduction of KYC costs; 2) administrative costs related to delivery of the Pantawid program will fall significantly as a result of availability of a bank account for direct benefit transfer; and 3) thorough verification of beneficiaries under Pantawid program will bring down inclusion errors significantly.

As mentioned earlier in this document, 69 percent of Filipinos do not have a bank account, therefore, a large section of this population can be potentially brought into the financial net after they get a unique identity. As per the census records, there are 62.6 million[73] adults in the Philippines. BSP's Financial Inclusion Survey 2017 estimates that only 22 percent of adults have an account with a formal financial institution. Thus, we can estimate that there are currently approximately 20 million accounts in the country. For the purposes of this study, it is estimated that the number of accounts will double over the next five years and that PhilID based e-KYC would be used for account opening. Through the interviews conducted during in-country visits, the BFA team learned that the cost of performing KYC processes costs US$5-10 each time, which is comparatively high. As stated in Section 3.1, in India, cost of KYC fell from INR40 (60 US cents) to INR5 (7 US cents), which is an 80 percent reduction as a result of use of Aadhaar. Assuming a similar reduction in KYC cost would mean that a Filipino financial service provider would now spend just US$1 instead of US$5. Total savings could amount to US$80 million, if we multiply 20 million new accounts by the US$4 cost reduction per account.

DSWD runs Pantawid (the 4P program) with an annual budget allocation of approximately US$1.8 billion. This program is mostly manual, incurring a substantial administrative cost. Most of the disbursements are in cash either through Land Bank or their employees. It is assumed that the administrative cost of handling cash can be significantly curtailed if monetary benefits are directly transferred to the bank account of the beneficiaries. As per a World Bank report on Financial Inclusion and Inclusive Growth[74], in Niger, 20 percent and in South Africa approximately 33% of the administrative cost of government transfers

of social benefit schemes was saved through direct remittance to bank accounts of beneficiaries. It is assumed that an average saving of 25 percent on the administrative cost can be achieved in the Philippines. As per an ADB report,[75] 10 percent of the annual budget is allocated to cover administrative expenses, totaling US$178 million. Going by the experiences of other countries, it would safe to calculate that the administrative cost of running the Pantawid program could be reduced by 25 percent, saving US$44 million a year. There would also be lower costs on other payments to and from the government by citizens and potentially revenue increases as well. The GSMA study[76] of P2G payments in Kenya saw non-tax revenue increases of 30-200 percent in different government departments after the adoption of digital payments.

As per the previously-mentioned ADB report, there are inclusion errors of at least 10 percent to 13 in the Pantawid program, which effectively means that a large share of monetary benefits is misdirected. While a digital national ID cannot fix the issue entirely, it can be presumed that inclusion error can be brought down to 5 percent through better identification, the use of technology tools, and the building of a universal social registry. Calculations indicate that if the inclusion error rate is brought down to 5 percent, it would generate savings of US$8 million every year.

In addition to the immediate cost savings, other financial and social benefits include higher bank profits (due to lower costs and better loan assessment); reduced household vulnerability (due to access to savings, loans, and remittances); greater investment in production by microbusinesses (that now have access to formal credit) and ultimately a more robust and modern financial sector and domestic economy.

8.3 Conclusion

Comparing the cost and benefits in table 9, there are significant net benefits – with a net present value (NPV)[77] of US$517 million – that should encourage financial institutions to adopt the digital national ID as a priority.

8.4 Cost-Benefit Analysis Table

Table 9. Cost-benefit analysis for rollout of digital national ID in the Philippines

Year	2018	2019	2020	2021	2022	2023
Total Cost	**$ 7,294,000**	**$ 18,851,800**	**$ 12,494,800**	**$ 3,634,000**	**$ 3,634,000**	**$ 3,634,000**
Software and Device Procurement	$ 6,634,000	$ 16,585,000	$ 9,951,000	-	-	-
Depreciation and Amortization	-	$ 726,800	$ 2,543,800	$ 3,634,000	$ 3,634,000	$ 3,634,000
Seeding of Pantawid database with PSN	$ 660,000	$ 1,540,000	-	-	-	-
Total Benefits	**$ 2,000,000**	**$ 159,104,152**	**$ 167,104,152**	**$ 167,104,152**	**$ 159,104,152**	**$ 159,104,152**
Savings in KYC Costs	$ 2,000,000	$ 16,000,000	$ 24,000,000	$ 24,000,000	$ 16,000,000	$ 16,000,000
Reduction in 4P administrative cost	-	$ 44,704,152	$ 44,704,152	$ 44,704,152	$ 44,704,152	$ 44,704,152
Drop in exclusion error in 4P	-	$ 98,400,000	$ 98,400,000	$ 98,400,000	$ 98,400,000	$ 98,400,000
Net Benefits	**$ (5,294,000)**	**$ 140,252,352**	**$ 154,609,352**	**$ 163,470,152**	**$ 155,470,152**	**$ 155,470,152**

NPV	**$ 517,910,494**

9 Recommendations

With the passing of the Republic Act No. 11055— "An Act establishing the Philippine Identification System", the Philippines' government has taken a giant leap forward in establishing a digital national ID system. PhilSys has the potential to not only simplify public and private transactions by providing valid proof of identity, but also to further BSP's financial inclusion agenda.

Adoption of the proposed PhilSys system has the potential to transform the country's financial sector landscape. It would help mitigate entry-level barriers for the consumer to get access to a bank account and other financial services, including credit. The ID system has the potential to improve access to financial services and also contribute to the reduction of the overall transaction costs for the financial institutions and consumers. However, it is important to note that provision of a unified, digital proof of ID to all citizens alone will not be able to overcome multiple other barriers to achieving sustainable financial inclusion ecosystem in the Philippines. Adoption of the digital ID platform can trigger a cascading effect in terms of technology adoption, awareness, and competitive pricing that could subsequently overcome some of the other barriers stated in earlier sections of this document.

Based on our analysis of the Philippines' current financial inclusion landscape, we make the recommendations outlined in table 10 to best utilize the digital national ID in achieving greater financial inclusion in the country. Our recommendations clearly indicate the primary institution responsible for implementation. The institution may collaborate with others – namely the government, banks, and other MFIs, the Bankers Association of the Philippines, and innovators, among others – to implement the recommended changes:

Table 10: Recommendations for the effective roll-out of PhilSys

PSA	**Provide both online and offline authentication methods:** PSA must include provisions in the PhilSys design and infrastructure to allow both online and offline authentication methods. While online authentication will be the preferred mode, offline authentication methods must also be devised that are reliable and secure given that large parts of Philippines do not have dependable network coverage. In an online mode of authentication, a PhilID holder will be authenticated against enrolment data stored in the PhilSys database (including demographics and biometrics) in real-time over a secure network connection. However, in the case of offline authentication, it is recommended that minimum information is stored securely on the PhilID that the holder will present to the service provider for authentication.

Preference for open source technology architecture: The PhilSys platform must be designed in such a way that it does not impose constraints in the selection of vendor or technology for developing client software applications. It is recommended that the PhilSys platform provides cross-platform support, maximum uptime, real-time access to authentication service, a detailed transaction log, and an efficient inquiry system to a wide range of end-user institutions.

Conduct pre-launch pilot of authentication services: It is necessary to define optimal performance benchmarks and biometric device/ application specifications before large-scale rollout of the authentication service. It may be remembered that effectiveness of the use of biometrics-based authentication varies with the age and economic profile of the person. Therefore, it is essential that pilot projects are conducted with controlled groups, comprising people from different age groups and economic backgrounds.

Issue guidelines for digitization and seeding of customers'/ beneficiaries' databases with PSN. It is recommended that robust procedures are defined to uniquely identify customers/beneficiaries and link their record(s) in a service delivery database with PSN. Benefits of such an exercise are that fake and ghost records will be eliminated and duplicate records, if any, will be either purged or merged. Secondly, service can be automated and made more cost-effective by reducing the cost of KYC processes and leakages, if any. PSA may issue general guidelines that MFIs, the government, and other service providers may adopt without change or customize according to the needs of the schemes/services. India offers an example of best practice in the issue of guidelines, which may be preceded by a workshop with a few of the government agencies and service providers to develop an understanding about the risks and scale of implementation.

Explore the option of ID on mobile phones: Given the Philippines' high smartphone penetration rate, PhilSys could also consider offering a facility that allows a PhilID holder to download encrypted and digitally-signed PhilID profile containing name, date of birth, gender, and address, along with a photograph as linked with their PhilSys number on the smartphone using a mobile app. This is ideal for offline authentication since the mPhilID profile stored on the smartphone could be shared by the owners with any service provider using multiple sharing options (e.g., Viber, WhatsApp, e-mail, etc.). The digital signature would help the service providers, including FSPs, to verify the authenticity of the ID details. Reference may be drawn to mAadhaar, the mobile equivalent of the Aadhaar letter in India, which

contains digitally-signed e-KYC data of the Aadhaar holder and can be carried on a smartphone.

BSP

Promote universal bank–rural bank/MFI partnerships: Given the strong IT capability of universal and commercial banks, and the extensive rural outreach of rural and cooperative banks and MFIs, we recommend partnerships that leverage the last-mile reach of the rural banks and MFIs. This would help bring the rural banks on the integrated and connected tech platform of universal and commercial banks, utilizing the on-the-spot authentication feature of a digital national ID even in the remotest parts of the country.

Promote digital and financial literacy: In order to deliver financial services to the largely unbanked and underserved populations that are otherwise hard to reach using the conventional brick and mortar bank branch presence, a trend to deliver financial services through digital channels is on the rise. However, for these unconventional and modern methods to achieve adoption and scale, it is essential to promote digital literacy through both conventional and trusted channels like TV, radio and newspapers, and government-moderated village/barangay-level campaigns.

Promote remote account opening: The Philippines can boast of a largely supportive legal framework underlying the use of digital identification for financial inclusion purposes. The ability to use digital national ID numbers for remote account opening, however, appears to be limited by the “face-to-face contact” requirement described above. Steps to enable remote account opening will be necessary if the digital national ID scheme is to achieve its full potential with respect to financial inclusion. The creation of the PhilSys and the PhilID, with a mobile identification system functionality, is consistent with the financial inclusion objectives of the BSP. The provision under the PISA which states that the PSN shall be honored and accepted as sufficient proof of identity (without the the need of presenting the PhilID) will likewise make remote account opening as well as KYC processes more efficient and cheaper.

Simplify due diligence procedures: Providers may apply "reduced due diligence procedures" when opening accounts where lower money laundering or terrorism financing risks have been identified. The AMLA and the various BSP regulations allow BSFIs to conduct a risk-based approach in determining the level of diligence to be used in assessing information required from customers and verifying customer identity and information. As opening an account with a national ID number would uniquely identify the user and therefore limit the user to one account per financial institution, this would significantly reduce the risk of abuse. The money laundering or terrorism financing risk could be further reduced through the establishment of account functionality limits (i.e., transaction and maximum balance limits) that could only be lifted following face-to-face CDD.

Impose functionality limit to remotely-opened accounts: When determining the limits to account functionality that might apply to an account that could be opened remotely with the customer's digital national ID number, BSP could consider using the Framework for Basic Deposit Accounts as a guide. The Framework already allows opening of basic deposit accounts using simplified CDD for low-risk customers. Furthermore, basic deposit accounts are already subject to a maximum balance limit of PHP50,000. If desired, this could be supplemented by transaction limits to ensure that such accounts are not abused for money laundering or terrorism financing purposes. One possibility would be to apply the monthly transaction limit for e-money accounts (currently PHP100,000 per Circular No. 649) to these accounts as well.

Devise standard operating procedures for financial institutions to leverage the PhilSys authentication service for the opening of bank accounts and to provide access to other financial services. It is thereby recommended that BSP publishes guidelines for banks and other financial institutions that should be applied if a customer is onboarded by successful authentication (biometrics preferred) using PhilD.

Galvanizing fintech firms to innovate new financial products that leverage PhilID will be a significant step in popularizing the use of the digital national ID for various social and commercial services. BSP may consider calling for "hackathons" periodically to present innovative solutions that will go a long way in furthering the objective of financial inclusion.

These are all complex, multi-stakeholder challenges and success will hinge on strong partnerships with digital ID and financial inclusion pioneers to harmonize systems and ensure that even the most vulnerable voices are heard. We must commit to working collaboratively to promote the power of ID in bringing an all-encompassing change and achieving a sustainable and holistic financial inclusion.

BFA Publications

- *Financial Digital Identity: Landscaping a digital financial identity for SADC.* 2018. http://finmark.org.za/landscaping-a-digital-financial-identity-for-sadc/

- *Person-to-government (P2G) payment digitisation: Lessons from Kenya.* 2017. https://www.gsma.com/mobilefordevelopment/programme/mobile-money/kenya-went-digitising-person-government-p2g-payments/

- *Building an Inclusive Digital Payments Ecosystem: The Way Forward.* 2017. https://www.betterthancash.org/tools-research/case-studies/country-diagnostic-ghana

- *Know Your Customer Requirements for DFS in Uganda.* 2017. http://www.uncdf.org/article/2593/study-know-your-customer-requirements-dfs-uganda

- *Going Beyond Regulatory Sandboxes to Enable Fintech Innovation in Emerging Markets.* 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059309

More publications at **www.bfaglobal.com**

References

[1] ADB. 2016. *Technical Assistance to the Republic of the Philippines for Financial Inclusion Framework* Strengthening. Manila.

[2] ADB. 2018. *Report and Recommendation of the President to the Board of Directors: Proposed Programmatic* Approach *and Policy-Based Loan for Subprogram 1 to the Republic of the Philippines for the Inclusive Finance Development Program*. Manila.

[3] Bangko Sentral ng Pilipinas. 2017. *Financial Inclusion Survey 2017: Moving towards Digital Financial Inclusion*. http://www.bsp.gov.ph/downloads/Publications/2017/2017FISToplineReport.pdf

[4] USAID. 2017. *Identity in a Digital Age: Infrastructure for Inclusive Development.* https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

[5] World Bank Group and Center for Global Development. 2017. *Principles on Identification for Sustainable Development: Toward the Digital Age.* http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-WP-REVISED-PUBLIC.pdf

[6] For the purposes of this document, E-KYC is defined as customer identification process wherein demographic data including the photograph of the customer is made available digitally to the requesting entity (financial service provider) subsequent to successful authentication.

[7] Senate of the Philippines*. "Senate OKs Lacson bill on national ID system". March 19, 2018.* http://www.senate.gov.ph/press_release/2018/0319_prib1.asp

[8] https://www.afi-global.org/policy-areas/general-fi

[9] A. Hannig and S. Jansen. 2010*. Financial Inclusion and Financial Stability: Current Policy Issues.* ADBI Working Paper 259. Tokyo: Asian Development Bank Institute. http://www.adbi.org/working-paper/2010/12/21/4272.financial.inclusion.stability.policy.issues/

[10] Robin J. Lewis, John D. Villasenor, and Darrell M. West. 2017*. The 2017 Brookings Financial and Digital Inclusion Project Report*. Washington DC: Center for Technology Innovation at Brookings. https://www.brookings.edu/wp-content/uploads/2017/08/fdip_20170831_project_report.pdf

[11] Bangko Sentral ng Pilipinas. 2017. *Financial Inclusion Initiatives2017.* http://www.bsp.gov.ph/downloads/Publications/2017/microfinance_2017.pdf

[12] https://www.britannica.com/place/Philippines

[13] http://www.worldbank.org/en/country/philippines/overview

[14] http://www.bsp.gov.ph/downloads/Publications/2017/2017FISToplineReport.pdf

[15] Bangko Sentral ng Pilipinas. 2017*. Financial Inclusion in the Philippines: Dashboard: As of Fourth Quarter 2017.*

[16] Bangko Sentral ng Pilipinas*. Annual Report.* 2017

[17] Bangko Sentral ng Pilipinas. *Factbook- The Philippine Banking System, 2017 Volume I* http://www.bsp.gov.ph/downloads/Publications/2017/FACTBOOK_2017V1.pdf

[18] Bangko Sentral ng Pilipinas. *Factbook- The Philippine Banking System, 2017 Volume I* http://www.bsp.gov.ph/downloads/Publications/2017/FACTBOOK_2017V1.pdf

[19] Bangko Sentral ng Pilipinas. *Factbook- The Philippine Banking System, 2017 Volume I* http://www.bsp.gov.ph/downloads/Publications/2017/FACTBOOK_2017V1.pdf

[20] Bangko Sentral ng Pilipinas*. Factbook- The Philippine Banking System, 2017 Volume I* http://www.bsp.gov.ph/downloads/Publications/2017/FACTBOOK_2017V1.pdf

[21] Bangko Sentral ng Pilipinas. 2017. *Financial Inclusion in the Philippines: Dashboard: As of Fourth Quarter 2017*

[22] Bangko Sentral ng Pilipinas. 2017*. Financial Inclusion in the Philippines: Dashboard: As of Fourth Quarter 2017*

[23] Bangko Sentral ng Pilipinas. 2017*. Financial Inclusion in the Philippines: Dashboard: As of Fourth Quarter 2017*

[24] The World Bank Group. 2014*. Country Partnership Strategy for the Republic of the Philippines. Report No. 78286-PH.* http://documents.worldbank.org/curated/en/328351468332470964/pdf/782860CPS0P132060Box385222B00OUO090.pdf

[25]The World Bank. 2017*. Financial Inclusion Data/ Global Findex* http://databank.worldbank.org/data/reports.aspx?source=global-financial-inclusion

[26] Hokans J*. Development Results Focused Research Program Country Diagnostic: Philippines* (Better than Cash Alliance, Bankable Fronteir Associates)*,* 2015 https://btca-prod.s3.amazonaws.com/documents/38/english_attachments/UNCDF-BTCA-Philippines-diagnoctic-20151014.pdf?1445264531

[27] Bangko Sentral ng Pilipinas. *National Baseline Survey on Financial Inclusion survey, 2015* http://www.bsp.gov.ph/downloads/publications/2015/NBSFIFullReport.pdf

[28] Bangko Sentral ng Pilipinas. 2017*. Financial Inclusion Survey 2017: Moving towards Digital Financial Inclusion.* http://www.bsp.gov.ph/downloads/Publications/2017/2017FISToplineReport.pdf

[29] The World Bank. 2017*. Financial Inclusion Data/ Global Findex* http://datatopics.worldbank.org/financialinclusion/country/india

[30] Robin J. Lewis, John D. Villasenor, and Darrell M. West. 2017*. The 2017 Brookings Financial and Digital Inclusion Project Report. Washington DC: Center for Technology Innovation at Brookings.* https://www.brookings.edu/wp-content/uploads/2017/08/fdip_20170831_project_report.pdf

[31] BangkoSentral ng Pilipinas. 2017*. National Strategy for Financial Inclusion.* http://www.bsp.gov.ph/downloads/publications/2015/PhilippinesNSFIBooklet.pdf

[32] https://www.pwc.in/assets/pdfs/publications/2017/fintech-india-report-2017.pdf

[33] http://fintechnews.sg/20712/indonesia/fintech-indonesia-report-2018/

[34] https://www.statista.com/outlook/295/119/fintech/india#market-revenue

[35] BangkoSentral ng Pilipinas. 2017*. Annual Report 2017: Sustaining the Growth Momentum.* http://www.bsp.gov.ph/downloads/publications/2017/annrep2017.pdf

[36] USAID. 2017*. Identity in a Digital Age: Infrastructure for Inclusive Development.* https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

[37] *An Act Establishing the Philippine Identification System.* Republic Act No. 11055. Congress of the Philippines, Metro Manila http://www.officialgazette.gov.ph/downloads/2018/08aug/20180806-RA-11055-RRD.pdf

[38] http://www.senate.gov.ph/lis/bill_res.aspx?congress=17&q=SBN-1738

[39] http://www.officialgazette.gov.ph/downloads/2018/08aug/20180806-RA-11055-RRD.pdf

[40] E&Y. 2015. *A Study on the Design of the Proposed 'Filipino National Identification System'.*

[41] Asian Development Bank. 2016*. Identity for Development in Asia and the Pacific*

[42] https://www.gsma.com/mobilefordevelopment/programme/digital-identity/gsmas-case-study-on-aadhaar-a-digital-identity-programme-that-is-inclusive-by-design/

[43] http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

[44] http://www.cgap.org/web-publication/fraud-mobile-financial-services-protecting-consumers-providers-and-system

[45] https://www.coa.gov.ph/phocadownloadpap/userupload/annual_audit_report/NGAs/2017/National-Government-Sector/Department-of-Social-Welfare-and-Devt/DSWD_ES2017.pdf

[46] Bangko Sentral ng Pilipinas. 2017. *Financial Inclusion in the Philippines: Dashboard: As of Fourth Quarter 2017*

[47] BangkoSentral ng Pilipinas. *Guidelines for Virtual Currency (VC) Exchanges*. Circular No 944 (Series of 2017)

[48] https://www.lawphil.net/statutes/repacts/ra2000/ra_8792_2000.html

[49] Certain exceptions apply, including with respect to existing laws that require specific formalities for executed documents to be deemed valid (Sec. 7).

[50] http://www.wipo.int/edocs/lexdocs/laws/en/ph/ph028en.pdf

[51] http://www.chanrobles.com/rulesonelectronicevidence.htm#.W1t5N9JKg1I

[52] http://www.bsp.gov.ph/regulations/laws_aml.asp

[53]http://www.amlc.gov.ph/faqs/2-uncategorised/55-revised-implementing-rules-and-regulations-of-republic-act-no-9160

[54] http://www.bsp.gov.ph/downloads/regulations/attachments/2017/c950.pdf

[55] http://www.amlc.gov.ph/faqs/2-uncategorised/55-revised-implementing-rules-and-regulations-of-republic-act-no-9160

[56] http://www.bsp.gov.ph/downloads/regulations/attachments/2017/c950.pdf

[57] http://www.amlc.gov.ph/faqs/2-uncategorised/55-revised-implementing-rules-and-regulations-of-republic-act-no-9160

[58] http://www.bsp.gov.ph/downloads/regulations/attachments/2017/c950.pdf

[59] http://www.amlc.gov.ph/faqs/2-uncategorised/55-revised-implementing-rules-and-regulations-of-republic-act-no-9160

[60] http://www.bsp.gov.ph/downloads/regulations/attachments/2017/c950.pdf

[61] http://www.bsp.gov.ph/downloads/regulations/attachments/2017/c950.pdf

[62] http://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/

[63] Sensitive personal information may be processed without the data subject's consent under certain circumstances, including when such processing is permitted by existing law/regulation, in life-or-death circumstances, for the purposes of medical treatment, in court proceedings, or when provided to public authorities (DPA, Sec. 13).

[64] https://privacy.gov.ph/wp-content/uploads/2016/10/Sgd-NPC-Circular-16-02-Data-Sharing-Agreements-Involving-Government-Agencies.pdf

[65] The DPA defines "personal information controller" as "a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf."

[66] http://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/

[67] https://www.icao.int/publications/Documents/9303_p9_cons_en.pdf

[68] https://uidai.gov.in/your-aadhaar/faqs.html

[69] https://www.pressreader.com/india/banking-frontiers/20170925/282209421044297

[70] http://business.inquirer.net/246015/ph-world-leader-social-media-usage

[71] https://tribune.com.pk/story/1395573/nadra-losing-rs40-every-identity-card/

[72] https://timesofindia.indiatimes.com/business/india-business/uidai-has-spent-rs-9055-crore-to-enrol-despatch-aadhaar-numbers/articleshow/59774867.cms

[73] https://psa.gov.ph/statistics/quickstat/national-quickstat/all/*

[74] http://documents.worldbank.org/curated/en/403611493134249446/pdf/WPS8040.pdf

[75] https://www.adb.org/sites/default/files/linked-documents/43407-014-fa.pdf

[76] https://www.gsma.com/mobilefordevelopment/programme/mobile-money/government-person-p2g-payment-digitisation-lessons-kenya/?utm_source=staff&utm_medium=referral

[77] For the calculation of NPV, a discount rate of 9 percent has been assumed (as per ADB guidelines) and 6 years have been considered, including 2018 which has little more than a quarter left.