INSTITUTE OF INTERNATIONAL FINANCE

INSTITUTE *of* INTERNATIONAL FINANCE

October 2019

Digital Identities in Financial Services

Part 2: Responsible Digital Identities, *The Key to Creating More Inclusive Economies*

Abstract: Financial service providers have an important and ever-increasing role in emerging digital identity ecosystems. We investigate the potential positive impacts digital identities can have on underserved markets and how financial institutions can help to responsibly and inclusively grow digital identities by adopting the latest emerging technologies. Financial institutions are well positioned to act as trusted, regulated players that can provide the building blocks for responsible digital identity initiatives by empowering individuals to control and extract value from their digital identities in a secure and inclusive manner. Financial institutions, as trusted data custodians and veteran risk managers and are well positioned to be at the forefront of protecting client privacy and ensuring financial well-being.

Table of Contents

Global Developments in Digital Identity Initiatives...4

Digital Identity vs. the Digital Identification Process...10

Applied Digital Identity Operational Models 11

The Impact of Responsible Digital Identity and Identification Processes on Financial Inclusion...13

Digital Identity's Impact on the Broader Economy...17

Gaps in the Current Ecosystem and the Role Financial Service Providers Need to Play in Developing Responsible Digital Identities..18

The Cautionary Tale of Pairing Digital Payments with Low Financial Literacy............................19

China's Credit Boom...20

The Sub-Saharan Digital Credit Revolution..21

Libra's Electronic Wallet Unintended Consequences...22

The Outlook - Responsible Digital Identity Ecosystems..24

Glossary..26

List of Figures and Tables

Figure 1: How Technology Companies are Creating Digital Identities..6

Figure 2: Data and Trust..8

Figure 3: Barriers to Inclusion...13

Table 1: Potential Beneficial Impacts of Digital Identities...17

Table 2: Ecosystem Stakeholder Attributes...18

Figure 4: China Household Short-term Consumption Loans (in Yuan).....................................20

Figure 5: Percentage of Borrowers who Report having Repaid Late or Defaulted on a Digital Loan...21

Table 3: Financial Literacy and Potential Unbanked Libra Users..22

Figure 6: Potential Ecosystem Interoperability...24

Digital Identities in Financial Services

Part 2: Responsible Digital Identities,

The Key to Creating More Inclusive Economies

Global Developments on Digital Identity Initiatives

Digital Identity has become a critical focal point in global policy discussions this year as governments, digital platform companies, foundations, and international organizations push for solutions that include more of the population into the formal economy. The current identity system is not efficient and effective enough for all involved, with 1.7 billion people unbanked and 1 billion lacking legally recognized identities. As the future economy emerges, financial service providers need to be at the center of discussions and play a critical role in the new digital identity ecosystem.

Governments are trying to include their citizens in the formal economy and several national initiatives have successfully improved global inclusion statistics. Most notably, China, India, and Kenya have all managed to include around 80%[1] of their citizens in the formal economy by creating successful ecosystems that serve the needs of their people. The developed ecosystem in each of these countries is quite different from one another, China relies on national technology companies using smartphone applications linked to financial institution accounts to facilitate payment transactions. India created the largest single digital biometric ID program in the world to become the base for citizen services and public welfare. Kenya's mobile money model focuses on providing tailored financial services through mobile money accounts.

Each of the aforementioned progressive ecosystems is an example of how nations have managed to digitally include their citizens in the formal economy while creating a digital footprint for segments of the society whose members were previously classified as underserved and financially excluded.

Information about an underserved individual that exists online, and the data derived from their digital footprint, can be used to characterize and identify unique behavioral patterns. Financial institutions and governments can leverage this digital data to create digital personas and access previously untapped market segments, gain insights on opportunities for products and services, personalize customer engagements based on life cycle needs and provide a frictionless transaction process - all key benefits for civilians at the base of the access to financial services pyramid.

[1] Global Findex Database, 2017

While the above ecosystem solutions have all managed to increase inclusion, some fundamental issues such as the lack of ecosystem **interoperability, privacy concerns**, **active usage**, and a **gender gap** have persisted. Responsible interoperable digital identities have the potential to overcome these issues and throughout this paper we will reflect on how responsible digital identities can address these issues. We also observe the emergence of lower tier requirements (a parallel due diligence system) in some places to provide access to basic financial products for lower income segments which could inhibit their growth and integration into the broader economy through mainstream financial services.

International initiatives such as the World Bank's ID4D, ID 2020 and the WEF Good ID have all been reviewing current digital ID initiatives and promoting best practice governance and policy design considerations for a more interoperable, secure, and gender inclusive ecosystem that connects all stakeholders involved. Impact investment firms and foundations such as Omidyar Network and the Gates Foundation have also shown keen interest in digital identities, mainly focusing on conducting advisory and research, and funding businesses that develop applicable interoperable technologies to enable user data control, while empowering women and the poor.

More recently we have also seen big technology companies such as Facebook more aggressively use their digital presence and 2.4 billion active monthly user base to extend digital personas and identities on a global scale. In the white paper introducing Facebook's latest initiative, Libra, they state: "An additional goal of the association is to develop and promote an open identity standard. We believe that decentralized and portable digital identity is a prerequisite to financial inclusion and competition."[2]

We expand on decentralized digital identity models later in this paper, but we begin by illustrating how technology companies such as Facebook are trying to enter the digital identity arena with initiatives that may reach billions of people around the globe.

Initiatives by Multilateral Organizations

ID4D

The World Bank's ID4D has the objective of globally spreading fully functional and interoperable identity systems that provide all individuals with the right to a unique and secure identity. ID4D believe that a strong identity system is the means by which financial, health, and technological services can be made accessible to those that are currently excluded. ID4D plays numerous roles across different regions of the world; globally they operate as a thought leader, conducting research and reviewing current practices and the digital landscape.

WEF Good ID

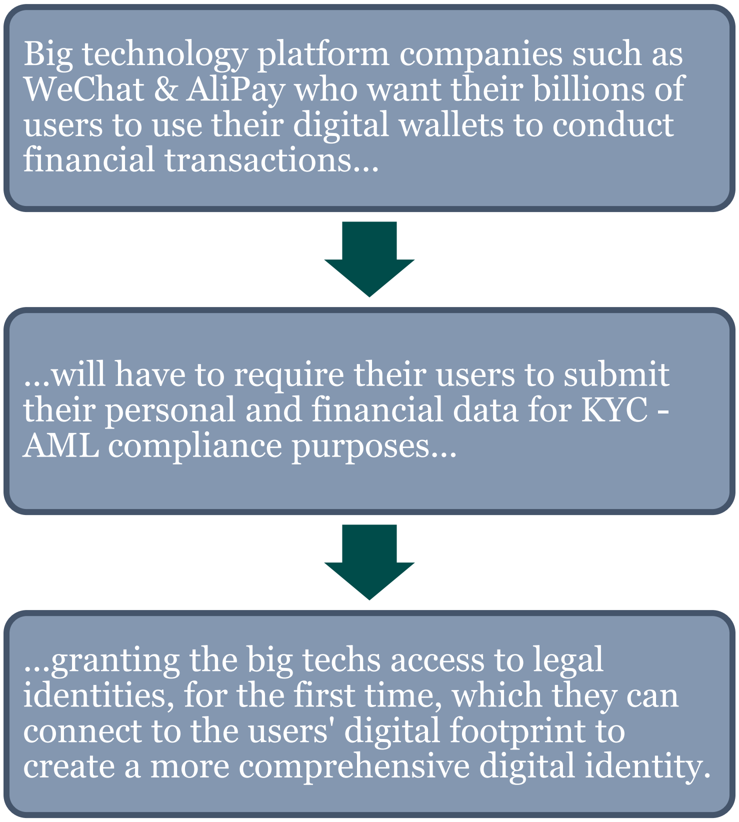
The World Economic Forum's Good ID Platform was created to bring identity's transformative effects to those with limited access to health services, economic opportunities, and citizen safety, and additionally to improve traceability in supply chains. The Good ID Platform connects stakeholders, conducts discussion and collaboration, and looks to offer best practice guidance on governance, stewardship, and policy design.

ID2020

ID2020 is an alliance consisting of governments and public and private sector organizations. The alliance model enables a synchronized approach to digital identity initiatives by enabling diverse stakeholders to work collaboratively and by coordinating funding to support high-impact projects. ID2020's fundamental role is to connect financing to identity-based projects; the selected projects aim to provide digital ID systems that are secure, interoperable, and controlled by the individual.

[2] Libra, *Libra White Paper*, https://libra.org/en-US/white-paper/

Figure 1: How Technology Companies are Creating Digital Identities



Big technology platform companies such as WeChat & AliPay who want their billions of users to use their digital wallets to conduct financial transactions...

...will have to require their users to submit their personal and financial data for KYC - AML compliance purposes...

...granting the big techs access to legal identities, for the first time, which they can connect to the users' digital footprint to create a more comprehensive digital identity.

Chinese BigTech Payment Platforms

WeChat Pay

WeChat Pay is the payment tool embedded into China's dominant mobile messenger platform, WeChat, and was originally intended for P2P transfers and in-app purchases in WeChat and QQ. WeChat Pay had 38.87% of Q4 2018 mobile transactions and over 600 million users[3] who leverage their confirmed WeChat identity to pay for and access an extensive list of in-app goods and services such as buying movie tickets, using Didi-Rider, making utility bill payments and repaying loans, making donations and investing spare money, into various wealth management options.

AliPay

AliPay is now the dominant force in Chinese mobile payments, particularly in the realm of online marketplaces, as the platform on which approximately 53.78% of mobile transactions took place in Q4 2018.[4] Over 520 million people use AliPay as their payment provider to shop online, to shop in person, to transfer money, and to invest excess funds in their digital wallet.[5]

[3] Analysys, Analysis of the digitalization process of the mobile payment industry, 26 Mar. 2019, https://www.analysys.cn/article/analysis/detail/20019244

[4] Ibid.

[5] Ibid.

WeChat and AliPay are not the only big technology companies trying to disrupt the financial services industry by offering e-payments on their platforms, with competition from players such as Facebook (intending to launch Calibra by 2020) and Apple (launching ApplePay). Technology companies with large customer bases entering the digital identity ecosystem will have tremendous power and oversight and some privacy advocates are particularly concerned given the less-than-ideal data privacy track record of some of these companies.

> ***Data Privacy:*** *The data used to establish digital identities and define a person's behavior is becoming increasingly important for digital identity ecosystem stakeholders. Access to and use of the data enable the creation of tailored products and services offered in real time to accommodate the individual's lifestyle needs.*

Three broad models have emerged regarding data ownership, management, collection, storage and use. In the United States, big technology companies such as Facebook, Amazon, and Google have access to and control over vast amounts of user data. In Europe, with the emergence of the General Data Protection Rules (GDPR), individuals retain data ownership and consumer rights are given priority. Finally, the third model is a state-backed technological model where governments have more access and control of user data, such as in China.

China Social Credit Score

China has implemented a patchwork of social credit scoring systems across multiple regions with the aim to launch a nationwide project in 2020; the system was introduced to address the trust deficit in China, which grew during (or, "has grown since") the 20th century revolution (which one?).

The credit scoring system compiles online and offline data including public behavior, transaction history, and social media data. Individuals who are deemed to have violated their social obligations can face sanctions such as blocked access to air travel, high speed trains, and hotels. Additionally, Zhima Credit, a credit scoring function within AliPay, monitors a wide range of data sources that are generated through an individual's online activity to calculate a credit score. Whilst not formally a part of the social scoring system, users can opt into having their credit score datashared with social scoring projects in order to receive benefits.

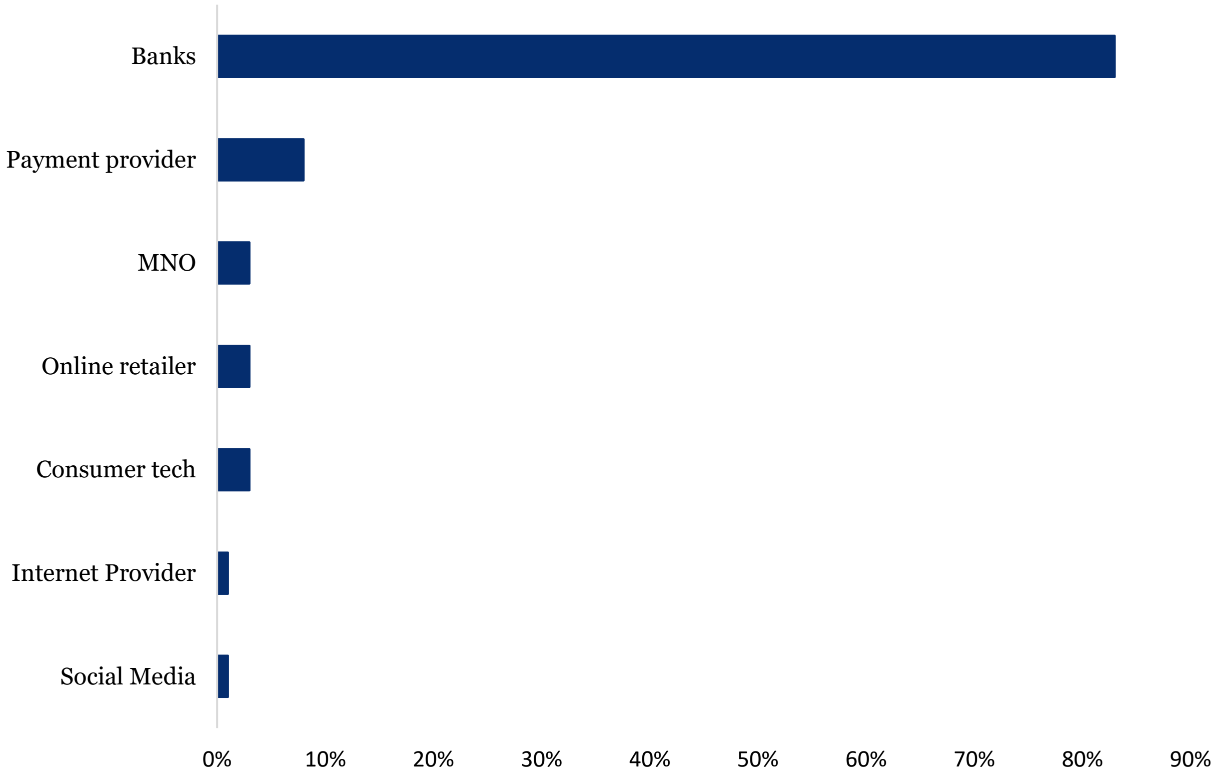
Privacy concerns arise in the American and Chinese models because individuals do not always know who has how much information about them, and how it is accumulated, stored, used or shared, leading to a loss of control over one's personal information.

It is crucial to protect an individual's privacy and information security. Policy makers and standard setters need to ensure that data privacy policies serve the individual's best interest, minimizing data misuse and enforcing data proportionality standards.

With the emergence of technologies such as 5G and the expansion of Internet of Things (IoT) connected devices, the amount of data and information collected on consumers will significantly increase in the near future. Having financial institutions that are well-positioned to be trusted and regulated can provide the building blocks for responsible digital identity initiatives by empowering individuals to control and extract value from their digital identities in a secure and inclusive manner. As trusted data custodians and veteran risk managers, financial institutions are at the forefront of protecting client privacy and ensuring financial well-being while avoiding de-risking practices.

Figure 2: Data & Trust

Which type of company do you tust most to securely manage your data? (% of respondents)



Source: Boston Consulting Group, Capgemini

The financial services industry has sound policies and regulations in place to conduct proper due diligence, protect personal information, reduce the risk of misuse of personal information by criminals, and ultimately ensure financial stability. However, the risk of running afoul of these regulations, and the will to reduce the risk of exposure to financial crime has also contributed to the financial industry's "de-risking" practices, with firms limiting their business in certain markets and product offerings. These practices can restrict low-income segments of the population from gaining access to finance. In response, we observe that lower tier requirements have been created in some places to provide access to basic financial products while creating a parallel due diligence system for lower income segments. Even though lower tier requirements could facilitate onboarding, we believe having different standards for different income groups will de-harmonize financial services frameworks, jeopardize financial crime risk mitigation, and will not automatically result in broader access to the full suite of financial services and products. Additionally, relegating these customers to a separate system could inhibit their growth and integration into the broader economy through mainstream financial services.

In the IIF's first paper on digital identities, "Embedding Digital Identities in AML Frameworks,"[6] we highlight considerations for international standard setters and local regulators on how to embed Digital Identity into their Anti-Money Laundering (AML) frameworks, ensure their widespread practical uptake, strengthen the defense mechanisms against financial crime, increase the efficiency of the system, and contribute to more inclusive AML frameworks.

Financial service providers are not the sole source for digital identities, as trusted sources for each digital identity attribute should be considered the ideal provider, nevertheless, financial service providers have proven to be trusted data custodians and are capable of securely managing digital identity data attributes.

In this paper we will investigate the role financial service providers can play, in the broader digital identity ecosystem, in positively impacting underserved markets and economies, while growing their business and building on the sound policies and regulations meant to ensure consumer protection and global financial stability.

[6] Institute of International Finance, *Digital IDs in Financial Services Part 1: Embedding in AML Frameworks*, August 2019, https://www.iif.com/Portals/0/Files/content/Innovation/08272019_iif_digital_id_part_1.pdf

Digital Identity vs. The Digital Identification Process

Digital Identity is a rapidly developing ecosystem with many different stakeholders involved.

Throughout this paper we will be referencing the term digital identity and the process digital identification frequently. **Digital Identity** can best be described as a compilation of electronically captured and developed attributes and credentials of a uniquely identifiable persona that can be linked to a physical person. It should be noted that there is an evolving taxonomy of the term and it is used broadly and interchangeably by different actors in the ecosystem. In order to be able to achieve inclusiveness, a wide variety of digital identity data attributes (as opposed to one true source of identity, e.g., government issued document) need to be considered.

> ***Trusted Digital Identity Issuers**: For a government, a non-governmental organization, or a person to be a reliable source of identification information they must do the following:* [7] *1) Support an ongoing relationship (as opposed to providing) a one-time service 2) Be in a sector which requires strong record-keeping practices and controls for all stages of a customer's lifecycle 3) Only provide identification that has an active and sustained relationship with the person being identified 4) Provide traceability to demonstrate the identification is in place and can be relied upon 5) Provide security features.*

Digital Identification on the other hand, is the process of verifying claimed attributes and credentials unambiguously linked to a persona in a domain through a digital channel. For the electronic Know-Your-Customer (e-KYC) process financial institutions – in addition to identifying potential customers – must conduct thorough due diligence.

In most jurisdictions, government-issued documents have been used as the primary identification method for individuals. Due to the integrity of government-issued documents, financial service providers have traditionally relied upon them to conduct customer due diligence and fight financial crime. However, with the emergence of technology and an individual's digital footprint, the identification process needs to evolve to include multiple digital identity attributes issued from reliable and trusted entities to match them to a person's identity.

As a precursor to our three-part digital identity series the IIF published a document called "Digital Identity: Key Concepts"[8] which clearly distinguishes between Digital Identity and Digital Identification as two separate yet related concepts. Please refer to that text for a more detailed description on these key concepts. Additionally, please find a glossary at the end of this paper with key terms related to digital identities.

[7] Di Mira, Digital Identification Methods and Testing for AML Programs, 2019, https://www.acams.org/white-paper-digital-identification-methods-and-testing-for-aml-programs/

[8] Institute of International Finance*, DIGITAL IDENTITY: KEY CONCEPTS*, July 2019, https://www.iif.com/Portals/0/Files/content/Regulatory/iif_digital_id_07022019.pdf

Applied Digital Identity Operational Models

The three most common operational models for digital identity are either a public, private, or a hybrid model. We covered in detail the digital identity operational models in our first paper; however, we have provided a brief refresher to help readers recap the main takeaways.

As mentioned in our first IIF paper, "Embedding Digital Identities in AML Frameworks,"[9] in **the public model** government agencies are the main source in charge of defining what constitutes digital identities, driving adoption and usage, and incurring the infrastructure and associated operational costs to launch and maintain a national digital identity initiative. The public model is also sometimes referred to as a "centralized model" where all digital identity use cases are centralized with a single provider (usually a government agency). India's Aadhaar, Estonia's e-ID, and Singapore's Singpass are all examples of public/centralized digital identity models. The benefit of this model is that services are usually streamlined, and data is aggregated and consolidated on a national level. However, since the role of digital identity issuance and management is centralized to one agency, there is a concentration and liability risk involved.

The second model type is known as the **private model** where digital identities are developed and maintained by private sector entities. Examples of the private model include Canda's Verified Me and Sweden's BankID and Freja eID+. These digital identity solutions are usually more decentralized models wherein the user has more control of his or her data. The rise of data privacy concerns has enabled **self-sovereign identities,** a version of a highly decentralized identity, to gain momentum-with companies such as IBM, Microsoft, and MasterCard creating solutions based on blockchain's distributed ledger technologies. The obvious benefit of this model is that the data on digital identities is often controlled by the user, where the individual would be able to grant access to their data on a voluntary basis, minimizing the risks of data mismanagement and abuse. However, prerequisites for such a model to work efficiently include high security

Canada's Verified.Me:

SecureKey's Verified.Me digital identity platform stores data on a user's device and allows them to opt to share the data with various commercial parties they want to engage with. Verified.Me requires the user to be a customer of one of the partnering financial institutions; consequently, the user's information is verified as it is assumed that the financial institution performed customer due diligence upon onboarding. After this point the user can use the Verified.Me platform on their mobile device to identify institutions that they want their initial institution to share information with. Verified.Me is beneficial to financial inclusion as it reduces the overhead associated with conducting KYC at scale which broadens the scope for financial inclusion.

The UK's Gov. Verify:

Gov.UK Verify allows users access to a range of online public services with a long-term plan to extend into the private sector; developments in this area are ongoing. Users have five potential identity providers that the UK government has partnered with: Barclays, Digidentity, Experian, Post Office, and Secure Identity.

[9] Institute of International Finance, *Digital IDs in Financial Services Part 1: Embedding in AML Frameworks*, August 2019, https://www.iif.com/Portals/0/Files/content/Innovation/08272019_iif_digital_id_part_1.pdf

standards and recognizing an approved body to handle grievances and address problems that might arise.

Finally, we also see **hybrid or federated models** arise in which ownership and responsibility are shared by multiple private and public entities. The ecosystem usually operates on shared common standards where the network is publicly endorsed or based on standards issued by the public sector. Examples include the UK's GOV.UK. This model requires coordinated decision making, which introduces complexity that may disincentivize institutions from participating as ID providers.

One of the most important aspects when designing operational models for digital identities is creating a set of interoperable ecosystems to facilitate the transaction process for users across different industries and jurisdictions.

> ***Ecosystem Interoperability:*** *The ability of different functional units—e.g., systems, databases, devices, or applications—to communicate, execute programs, or transfer data in a manner than requires the user to have little or no knowledge of those functional units will be essential for digital identities to be globally recognized. For digital identities to be globally recognized and accepted, a universal definition and agreed upon features need to be in place.* ***Currently the digital identity ecosystems that are in place are closed looped systems and function within national boundaries. Creating a cross-border solution will greatly increase uptake and functionality of digital identities.*** *As emphasized in our first paper, states should set basic criteria for what defines digital identities. This will enable the emergence of a global standard for digital identities. States can then build their own solutions and keep them interoperable in design. Member states would have the freedom to build and maintain their own digital identity solutions while keeping the door open for cross-border interoperability.*

There are several digital identity ecosystem stakeholders that provide different services to consumers. As the lines between technology companies and financial service providers get blurrier, technology companies are entering the space of providing financial services and financial service providers are undergoing digital transformations to become more like technology companies.

In the current state of play**, technology companies** are gathering vast amounts of data that can help identify digital behavior and create corresponding digital personas. **Financial institutions** are conducting customer due diligence and providing financial services and products while ensuring financial stability and safe financial management practices are being adhered to; **governments/regulators** are enforcing the appropriate standards, policies and regulations to advance digital identity issuance and management in an inclusive manner while ensuring financial stability is maintained. Later in the paper we will dissect the ecosystem stakeholders and highlight obvious gaps and opportunities for creating a more interoperable model that will serve low income segment customers more efficiently.

Responsible Digital Identity and Identification Processes: Impacts on Financial Inclusion

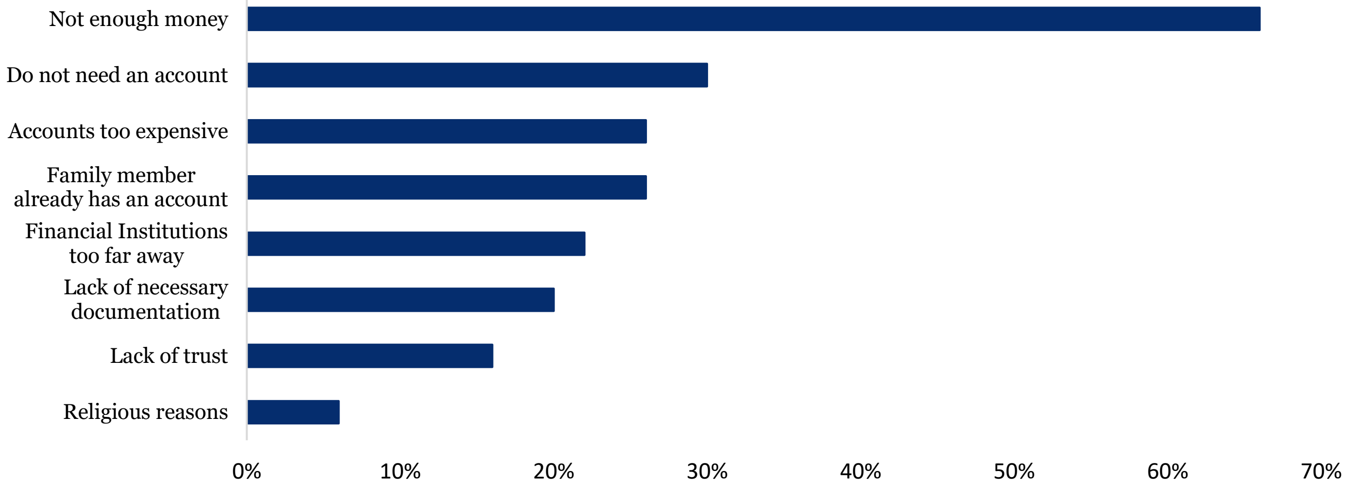
Gaining access to financial services enables entrepreneurs and small and medium enterprise (SME) owners to utilize institutions' valuable consulting services to help invest capital and grow their businesses. This in turn empowers them to make better business decisions, which results in business expansion and job creation, and supports economic prosperity. However, for an individual or business to be recognized in the formal economy and for nations to reap the benefits, citizens first need to possess some form of identification. As mentioned earlier, around 1.7 billion people are unbanked and 1 billion lack legally recognized identities and consequently can be denied for crucial economic and national benefits. The gender gap in identity ownership is also noteworthy with 45% of women (over the age of 15) in low income countries lacking a legal identity compared to 30% of men.[10]

> ***Gender Inclusivity:*** *A gender gap in account ownership has been a persistent challenge for financial inclusion especially in developing economies (there has been a consistent 9% gender gap since 2011 according to the latest Findex numbers). Digital identification will enable a more efficient customer due diligence process and overcome the common account opening barriers that disproportionately affect women and girls in developing countries. Financial institutions will have the opportunity to partner with governments to receive and pay government subsidies and cash transfer programs targeted at women. The increasing use of transactional data on mobile phones will also help financial service providers target women with products and services that cater to their lifestyle needs.*

Digital identification and identities can have profound impacts on financial inclusion. In this section we will aim to identify some of the major challenges faced by the unbanked and highlight which of those can be overcome by implementing responsible digital identity and identification procedures.

Figure 3: Barriers to Inclusion

Lack of enough money is the most commonly cited barrier to account owenrship
Adults without a financial instituion account reporting barrier as a reason for not having one (%), 2017



Source: Global Findex database
Note: Respondents could choose more than one reason

[10] Global Findex Database, 2017

As evident from the latest 2017 Global Findex graph, the largest dataset on financial inclusion provided by the World Bank every three years, some common recurring barriers to account ownership have been identified.

The most evident barriers where the digital identification process can have an impact are:

i. accounts are too expensive,
ii. financial institutions are too far away, and
iii. the lack of necessary documentation.

Account opening fees and a minimum opening deposit balance are usually prerequisites for most financial institutions, which can be a burdensome ask for low income segments. High account opening cost was cited by 26% of the surveyed unbanked as being a main barrier to account ownership (the figure jumps to 60% in some developing Latin American countries).

The traditional (brick and mortar) banking model has high operational expenses, which makes banking low-income population segments challenging. High costs are also the reason why many financial institutions choose not to expand their branch networks into rural areas, another major obstacle to inclusion (22% of the Findex responders cited distance as one of the major barriers to opening an account - the figures goes up to 33% in some emerging economies). Finally, regulators in several countries necessitate physical copies of onboarding documentation as part of the KYC procedures financial institutions are required to abide by. Usually financial institutions require potential customers to bring a legal form of ID (whether it be a birth certificate/national ID or passport) along with proof of address to be able to open an account. The lack of necessary documentation was cited by 20% of Findex respondents (reaching 49% in some economies).

The temptation of creating a lower requirement for low income customer segments continues to be an attractive but misguided method for facilitating the onboarding of underserved citizens and is evident in several ecosystem models such as mobile money initiatives in Africa and platform companies in China. Even though the ecosystem has offered some solutions, challenges persist regarding KYC processes, AML procedures, data privacy breaches and granting access to a broader spectrum of financial services and products.

By implementing and integrating with the latest emerging technologies in digital identification, financial institutions can solve for some of these barriers while ensuring sustainability and consumer protection when banking low-income segments. Financial institutions have said that by relying on the Aadhaar tech stack, account opening costs have decreased by over 40% and opening an account has become instant instead of taking three days to approve new-to-bank customers.

Pakistan’s Nadra

Nadra was established as a national database organization under the Pakistan government with a corresponding digital identity program ‘Pak-identity’. The chip contains fingerprint, iris, and facial biometric data and an internal function to destroy all data if the card is tampered with. The smart-ID card contains the data required to function as an e-driver’s license and as an e-health insurance card and can also be used for voting and through numerous biometric scans can ensure that the voting system was not tampered with.

Biometric Technology: *A combination of physical and behavioral characteristics such as retinas, fingerprints, gait, key swipes, and pressure applied in holding a device change the way digital identity can be formulated and authenticated, allowing claimants to verify themselves as a unique identity. Biometrics reduce the time and cost for financial institutions when conducting KYC onboarding practices. A pilot project run by ASB in New Zealand that used facial recognition to onboard customers received positive customer feedback due to the speed of process and convenience, whilst a PwC*[11] *report suggested that biometric onboarding reduces time and costs for banks in processing applicants. Biometrics simplify and remove some of the traditional credentials required by service providers for digital identity establishment and the time and cost savings associated with biometrics as a part of KYC compliance broadens the scope for financial inclusion.*

Emerging technologies in digital identification such as e-KYC are being used to accelerate the remote onboarding process for financial institutions. When implemented right they can have a profound impact on minimizing turnaround time, costs and documentation requirements for new-to-bank customers. Several technology companies are providing electronic e-KYC solutions, where new bank clients can complete their onboarding through a mobile phone. This in turn drives down account opening costs, eliminates documentation requirements, and avoids long commute times for potentially underserved population segments living in rural areas, where bank branches or agent networks are not easily accessible. Financial institutions are utilizing digital technologies to instantly provide access to financial services by aggregating emerging mobile technologies and government identity verification solutions. Customers would conduct a short quick live video stream enabling financial services providers to instantly verify the customer by authenticating the user's information against the national identity database to ensure validity of the person as a natural citizen. This natural person verification process ensures there is a real person associated with the customer's digital

India's Aadhaar:

India decided to take an active role and created a foundation layer for digital identities as a public service. They have managed to ease access to financial services by relying on tech-stack solutions such as Aadhaar. An Aadhaar number is a 12-digit unique number issued by the UIDAI ("Authority") to the residents of India after satisfying the verification process laid down by the authority. A person willing to enroll must provide minimal demographic (name, date of birth, gender, address) and biometric information (fingerprints, iris scans, and a facial photograph) during the free of enrollment process. Aadhaar has become the largest single digital biometric ID program in the world with 1.2 billion Indians enrolled in the program.[12] A suite of open application program interfaces (APIs) is linked to Aadhaar.

For example, the Unified Payments Interface platform integrates other payment platforms in a single mobile app that enables quick, easy, and inexpensive payments among individuals, businesses, and government agencies.[13] Even though the technology stack used for Aadhaar has managed to prove a successful means of opening access to financial services, several data breaches have been reported. **Ensuring that customer data is protected will be of utmost importance when creating future technology stacks serving digital identities.**

[11] PwC, *The Future of Onboarding*, December 2016, https://www.pwc.com/il/he/bankim/assets/pwc-the-future-of-onboarding.pdf

[12] Unique Identification Authority of India | Government of India, About Your Aadhaar - Unique Identification Authority of India: Government of India, uidai.gov.in/my-aadhaar/about-your-aadhaar.html, Viewed 19 Sep. 2019.

[13] Kaka et al., Digital India: Technology to Transform a Connected Nation, McKinsey & Company, Mar. 2019, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-india-technology-to-transform-a-connected-nation

identity. This enables financial institutions to drive digital inclusiveness by removing location barriers to conducting business constraints to establishing mutual trust and removes the need for physical identity documentation.[14]

Active Usage: *Opening a bank account is insufficient for financial inclusion. Practitioners need to ensure that underserved segments remain actively engaged. Using digital identities, financial institutions can use the real time digital attributes of individuals to analyze and predict customer behavior and create tailored digital financial savings and credit products that serve clients lifecycle needs.*

Another reason the unbanked are denied access to credit is due to their lack of financial history data. Low income segments usually have no formal proof of income and are considered "thin file customers" with no credit history and alternatively no credit score which making them high risk customers for financial service providers. This is where digital identities can play an important role in providing alternative data sources. Digital identities are a set of digital credentials and attributes that uniquely identify a person and their behavioral patterns. The attributes can include alternative data sets to create virtual/digital personas of potential bankable customers based on their digital behavior. For example, through taking digital bill payment-or MNO call data records and analyzing the potential customer's payment transaction history, financial service providers can create alternative data scores based on the customer's digital footprint. Digital tax, subsidy and e-commerce activity are all examples of alternative digital data sets that can be used to profile historically unbanked consumers. We emphasize the use of alternative data in detail in IIF's "Accelerating Financial Inclusion with New Data"[17] report and will further be highlighting the business opportunity of digital identities in our third and final report.

South Africa's Smart ID:
South Africa has launched a national digital identity program known for its high level of security and advanced data-protection mechanisms. A user is authenticated through biometric verification and a pin code only known to the user. South Africans can apply for their smart ID cards at local banks and receive a Smart ID embedded with a secure software that can only be verified by authorities using contactless readers.[15]

e-Estonia: Nearly every one of Estonia's 1.3 million citizens has an ID card, which is much more than simply a legal photo ID. It is a mandatory national card with a chip that carries embedded files and can function as definitive proof of ID in an electronic environment. The ID card provides digital access to all of Estonia's secure e-services, releasing a person from tedious red tape and making daily tasks faster and more comfortable whether they involved banking, signing documents, or obtaining a digital medical prescription.[16]

[14] Busisiwe, Mbuyisa- Muhammed,Omarjee and Stanton, Naidoo from Standard Bank. (2019, June). Phone interview with Amin,Khairy.
[15] Gemalto, South African ID Card : Identity and Citizenship, 6 Mar. 2019, https://www.gemalto.com/govt/customer-cases/south-africa.
[16] E-Estonia, We Have Built a Digital Society and so Can You, e-estonia.com
[17] Center for Financial Inclusion & Institute of International Finance, *Accelerating Financial Inclusion with New Data*, May 2018, https://www.iif.com/portals/0/Files/private/finewdata_cfi.pdf

Digital Identity's Impact on the Broader Economy

Bringing entrepreneurs and their businesses into the formal economy is an important first step to building better connected financial markets and ultimately global markets. It allows those operating in mature markets, who have capital, to connect with the next generation of young entrepreneurs in emerging markets, who need capital.

McKinsey & Company estimates that nations implementing Digital ID could add value of up to 13% of GDP by 2030.[18] The diagram below highlights the potential beneficial impact (Efficiency-E, Revenue R, Security-S, Cost-C and Privacy-P) for stakeholders with digital identity. It is noteworthy to mention though that the below benefits would apply to digital identities that have large digital identity attributes (for example health data records, employment history, bill payment transactions), all of which would need to be standardized in both syntax and semantics to ideally function across borders for a more interoperable ecosystem.

Table 1: Potential Beneficial Impacts of Digital Identities

<table>
<tr><th colspan="3">Applications and Benefits of Digital Identity</th></tr>
<tr><th>Governments</th><th>Individuals</th><th>Entities</th></tr>
<tr><td>Tax collection (R)</td><td>Access to financial services (E,R,S &P)</td><td>e-kyc (E,C &S)</td></tr>
<tr><td>Subsidy/social program payout (E,C,R,S)</td><td>Consolidated health profile (E)</td><td>Alternative data (R)</td></tr>
<tr><td colspan="3">Secure/efficient digital payments (E,C,S,P)</td></tr>
<tr><td colspan="2">Monetary transmission mechanism (E,R)</td><td></td></tr>
<tr><td colspan="3">Preventing identity theft/fraud (S)</td></tr>
<tr><td colspan="3">Better Customer Service (E)</td></tr>
<tr><td>G2P & G2B payments (E,C,S)</td><td colspan="2">Streamlined authentication/registration (remote onboarding) (E,C)</td></tr>
<tr><td>Better AML/CFT (S)</td><td>Data Management/transparency (E,P)</td><td>Better AML/CFT (S)</td></tr>
<tr><td colspan="3">Better Credit Scoring (E,C, R)</td></tr>
<tr><td colspan="3">Single Customer View (E,C)</td></tr>
<tr><td colspan="3">Digitizing Documentation Management (E,C,S,P)</td></tr>
<tr><td colspan="3">Frictionless/Seamless Transactions (E,C,S,P)</td></tr>
<tr><td>reducing gender gap (R)</td><td colspan="2">talent matching (jobs to skills) (R)</td></tr>
<tr><td></td><td colspan="2">formalized business registration (R)</td></tr>
<tr><td colspan="3">platform interoperability (E,C,R)</td></tr>
</table>

[18] McKinsey & Company, *Digital Identification: A Key to Inclusive Growth*, April 2019, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-identification-a-key-to-inclusive-growth

Governments tend to gain from broader tax collection, more efficient subsidy/social program payouts, digitized G2P & G2B payments, and enabling women to be more engaged in the economy by decreasing the gender gap. After India implemented Aadhaar, for example, the leakage of funds for pension payments dropped by 47% when the payments were made through biometric smartcards rather than being handed out in cash.[19] However, benefits for consumers would only be reaped if data is managed and utilized responsibly.

Financial institutions have an important role to play in ensuring that vulnerable consumers are not being taken advantage of and that practices ensuring consumer protection and financial wellbeing are enforced appropriately.

Gaps in the Current Ecosystem

As outlined earlier, the three main ecosystem players in the digital identity space are financial service providers, technology companies, and regulators. The lack of common standards and policies has led to recent data privacy issues and high default rates related to consumer indebtedness through easy and irresponsible digital finance. The figure below maps out the current ecosystem players with their corresponding attributes.

Table 2: Ecosystem Stakeholder Attributes

Ecosystem Players Attributes	Financial Service Providers	Technology Companies	Regulators
Trust	✓	✗	✓
Risk Management	✓	✗	✓
Alternative Data	✗	✓	✓
Regulated	✓	✗	▬
Human Capital	✗	✓	✗
Consumer Protection	✓	▬	✓
Financial Literacy	✓	✗	✓
Standard Policies & Regulations	✗	✗	✗
Technology Infrastructure	✗	✓	▬

To be able to fully leverage the capabilities of digital identities financial service providers will need to gain access to and analyze **alternative data sets** such as MNO call data records, global positioning data, digital payment data (bill, subsidy, and tax payments records, for example), social media data, and digital health data among others. This will be crucial data when creating alternative credit scores based on the digital data footprint for low-income population segments, known for being "thin file customers" with limited financial transaction histories. Technology companies currently possess this data on large scale consumer segments and are equipped with experienced human capital (data scientists) leveraging an agile technology infrastructure. Regulators on the other hand are struggling to come up with standard policy and regulation frameworks that would protect consumers in this new ecosystem of easy finance through digital identities.

[19] Muralidharan, Niehaus, and Sukhtankar (2016).

Data scientists are working to analyze alternative data sets and come up with unbiased, transparent, and explainable machine learning algorithms that can help provide credit and mitigate risk at a fraction of the cost and at much faster processing speeds, making digital credit an easy touch-of-a-button-service to obtain . In the coming section we will look at some emerging ecosystems materializing from this digital revolution and highlight some of the risks that we have observed arise when consumers' digital data is abused.

Having regulated, trusted and experienced risk management financial service providers be a part of the digital identity ecosystem has never been more important. Financial service providers would be able to safeguard consumers while educating the unbanked, considered to be one of the more the vulnerable segments of society, on financial management best practices. The importance of having trained banking representatives educate financially illiterate underbanked customers and ensure financial stability, in an ever-growing digital finance world, cannot be overstated.

Pairing Digital Payments with Low Financial Literacy: A Cautionary Tale

The fact that mobile phone penetration *(unique mobile phone subscribers as of end of 2018 were 5.1 billion,[21] up from 3.6 billion at end of 2014[22])* and mobile payments *(registered mobile money accounts as of end of 2018 were 866 million,[23] up from 299 million at end of 2014[24])* have surged tremendously over the past decade gives hope to a lot of practitioners trying to advance financial inclusion. The possibility of a new wave of digital finance products and services becoming available to low-income population segments through quick convenient mobile technology is becoming reality.

Banking on mobile phones is attractive because digital finance is economically more efficient for providers and, more importantly, it is more convenient for consumers to use. However, issues might arise if digital finance propositions are not targeted to solve specific consumer pain points and are instead used as a platform to gain access to easy credit without appropriate supervision. A study by the Global Financial Literacy Center found that millennials who use mobile payments are at greater risk of experiencing financial distress and engaging in financial mismanagement. Millennials who use mobile payments compared to non-users were more likely to report that they occasionally overdraw their checking account (33% vs. 19%), they made withdrawals from their retirement account (37% vs. 9%) and they used alternative financial services such as pawnshops or payday loans (50% vs. 23%).[24] Increasing the ease of transaction processing through technology**,** if unsupervised, could increase financial vulnerability especially for low-income population segments known for their low financial literacy rates. Below are a few examples of the possible negative impact of easy unsupervised access to finance through technology or mobile platforms.

[20] GSMA, The Mobile Economy 2019, 2019 https://www.gsmaintelligence.com/research/?file=b9a6e6202ee1d5f787cfebb95d3639c5&download

[21] GSMA, The Mobile Economy 2015, 2015 https://www.gsma.com/mobileeconomy/archive/GSMA_ME_2015.pdf

[22] GSMA, The Mobile Economy 2019, 2019, https://www.gsmaintelligence.com/research/?file=b9a6e6202ee1d5f787cfebb95d3639c5&download

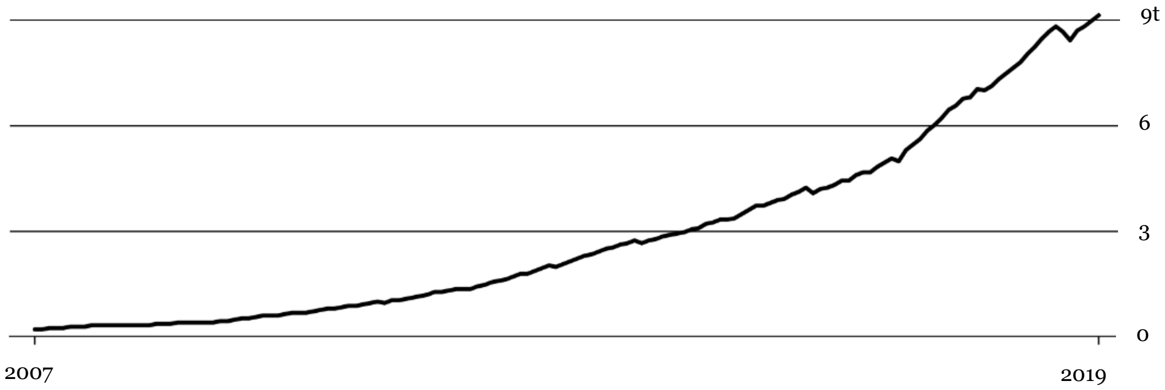
[23] GSMA, The Mobile Economy 2015, 2015, https://www.gsma.com/mobileeconomy/archive/GSMA_ME_2015.pdf

[24] Lusardi, et al., *Millennial Mobile Payment Users*, Global Financial Literacy Excellence Center (GFLEC), gflec.org/initiatives/millennial-mobile-payment-users/

China's Credit Boom

Even though China's financial inclusion numbers have significantly improved in recent years, easy access to credit through technology platforms such as Alipay and TenCent has raised several concerns over indebtedness, especially amongst younger generations, which can have negative effects on the health of the economy. According to a recent Bloomberg article, credit secured through technology has skyrocketed in China with unsecured consumer loans growing on average 20% annually since 2008.

Figure 4: China Household Short-term Consumption Loans (In Yuan)



Data: People's Bank of China

'China Household Short -term Consumption Loans (in Yuan),' sourced from Luo, Han & Hu, *China's Generation Z Is Hooked on Credit*, Bloomberg, July 2019.

The credit which has ranged from 500-50,000 yuan (eq. USD 70-7,000) is being used to buy basic everyday staples such as clothes, food, and travel and is approved virtually on the spot through mobile applications even for consumers with no previous credit history. This leads to a boom in debt-fueled consumption that can negatively impact future spending and consumer purchasing power since future disposable income will be used to repay outstanding debt. Consumer finance through the internet in China is expected to double by 2021 to reach 19 trillion yuan (USD 2.7 trillion) up from 7.8 trillion yuan (USD1.1 trillion) last year.[25]

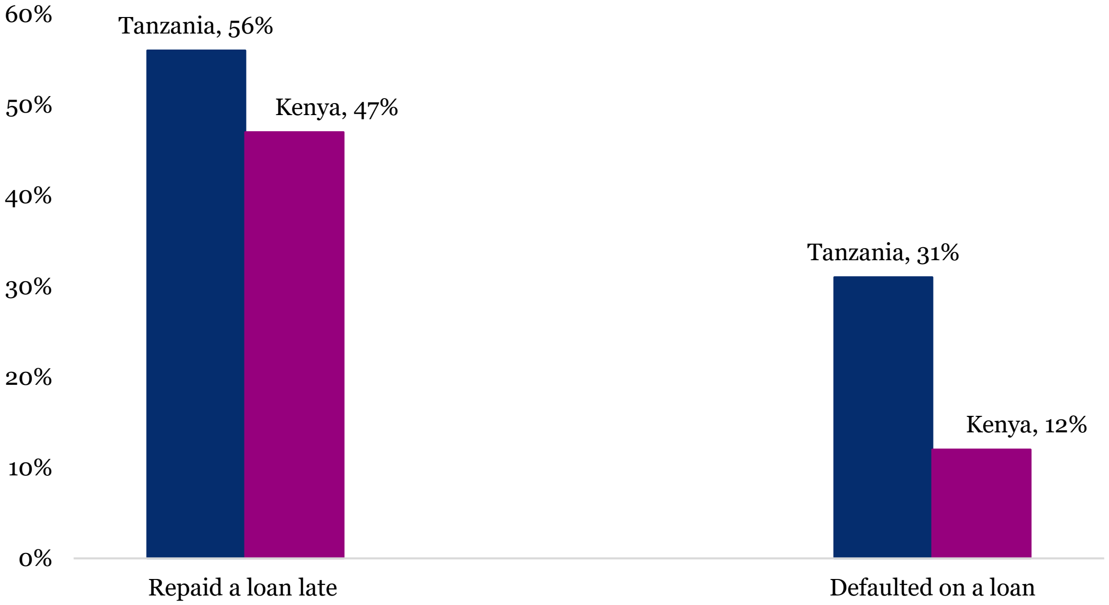
[25] Luo, Han & Hu, *China's Generation Z Is Hooked on Credit*, Bloomberg, 31 July 2019, www.bloomberg.com/news/articles/2019-07-31/china-s-generation-z-is-hooked-on-credit

The Sub-Saharan Digital Credit Revolution

Sub-Saharan Africa is arguably the first region to have introduced digital credit on a mass scale with initiatives such as M-Pesa which has brought mobile money to millions of borrowers since 2012 in countries such as Kenya and Tanzania. Automated credit decisions resulting in instant loans coupled with remote disbursement and repayment make mobile money an efficient and convenient ecosystem for many low-income borrowers.

In a working paper titled "A Digital Credit Revolution," CGAP (Consultative Group to Assist the Poor), a global partnership of more than 30 leading development organizations that works to advance the lives of poor people through financial inclusion, highlights the dangers of the sub-Saharan digital credit surge fueled by mobile money in the region. Fifty-six percent of borrowers in Tanzania and 47% in Kenya have repaid a digital loan late; 31% in Tanzania and 12%in Kenya report having defaulted.

Figure 5: Percentage of Borrowers who Report having Repaid Late or Defaulted on a Digital Loan



Source: National phone survey of N=3,150 in Kenya, of whom 1,037 have used digital credit and national phone survey of N=4,574 in Ta of whom, 1,132 have used digital credit. Both surveys were conducted June--August 2017 and were weighted to be representative of phone owenrs.

The paper goes on to explain that late repayments can have significant consequences for borrowers, such as having their accounts frozen or getting charged a second origination fee on rolled over loans. The unpaid loans get reported to the Credit Risk Bureau resulting in a negative credit score for borrowers and making it harder for low-income segments to re-borrow once they have been deemed too risky. In order to be able to repay the loan, research respondents in Kenya and Tanzania have cited actions such as reducing food purchases, borrowing additional money to repay the loan, and even skipping school and medical treatments in some instances.[26]

[26] Kaffenberger, Michelle, and Edoardo Totolo., A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania, Working Paper, *CGAP*, 2018, Washington, D.C.

Libra's Electronic Wallet and Unintended Consequences

Now imagine a technology company with a scale such as Facebook's platform (including Facebook, WhatsApp, and Instagram) entering the digital finance arena. Facebook has promised to find remittance solutions for the unbanked population by granting access to the Calibra wallet through WhatsApp to a customer base of over 2.4 billion monthly active users across its three platforms. Libra/Calibra promises to attract unbanked customers who need to transfer or receive remittances and are usually considered to be financially illiterate.

Facebook's Libra Proposal

The Libra Association

A membership organization, headquartered in Switzerland designed to facilitate the operation of the Libra Blockchain; to coordinate agreement among its stakeholders - the network's validator nodes- in their pursuit to promote and develop the network and to manage the reserve.

Libra

A digital currency built on blockchain and backed by a one -one reserve of assets. Libra is governed by the Libra association

Calibra

Facebook's electronic wallet for the storage of Libra coins. According to David Marcus, head of Calibra and co-creator of Libra, Calibra will be the only wallet embedded into WhatsApp and Messenger

Table 3: Financial Literacy and Potential Unbanked Libra Users[27]

Country	Increasing Need for Banking Services (see footnote) *(higher number = worse score)*	Financial Literacy Score *Scale from 0-100* *(lower number = worse score)*
Yemen	17	13
Cambodia	5	18
Sierra Leone	0	21
Nicaragua	21	20
Sudan	20	21
Burundi	16	24
West Bank and Gaza	10	25
Chad	4	26
Congo, Republic	7	31
Congo, Democratic Republic	16	32
Niger	6	31
Mexico	4	32
Mauritania	5	33
Madagascar	3	38
Kazakhstan	8	40
Tanzania	7	40
Zimbabwe	0	42
Myanmar	5	52

[27] Source: Bruegel based on S&P Global FinLit Survey and Global Findex dataset (World Bank). Notes:" Increasing need for banking services" is measured as the difference between the % of people sending/receiving remittances in the previous year and the % of people that have a bank account

The above data was published by Brugel, a European think tank, and derived from the S&P Global FinLit Survey and Global Findex dataset. It conveys that countries that most need access to banking services are also those that are the least financially literate.[28] For now, remittances are the only product that Calibra is promising to offer, however if other financial products are to be offered, using alternative data to create digital identities and behavioral patterns on a platform with such scale, potential systemic **financial stability risks are bound to arise.**

Low income segments who have low financial literacy will be particularly vulnerable to financial distress. Financial service providers that are regulated, experienced in risk management, and that can ensure both consumer wellbeing and financial stability will be essential to creating a sustainable digital financing solution based on an individual's digital footprint/identity.

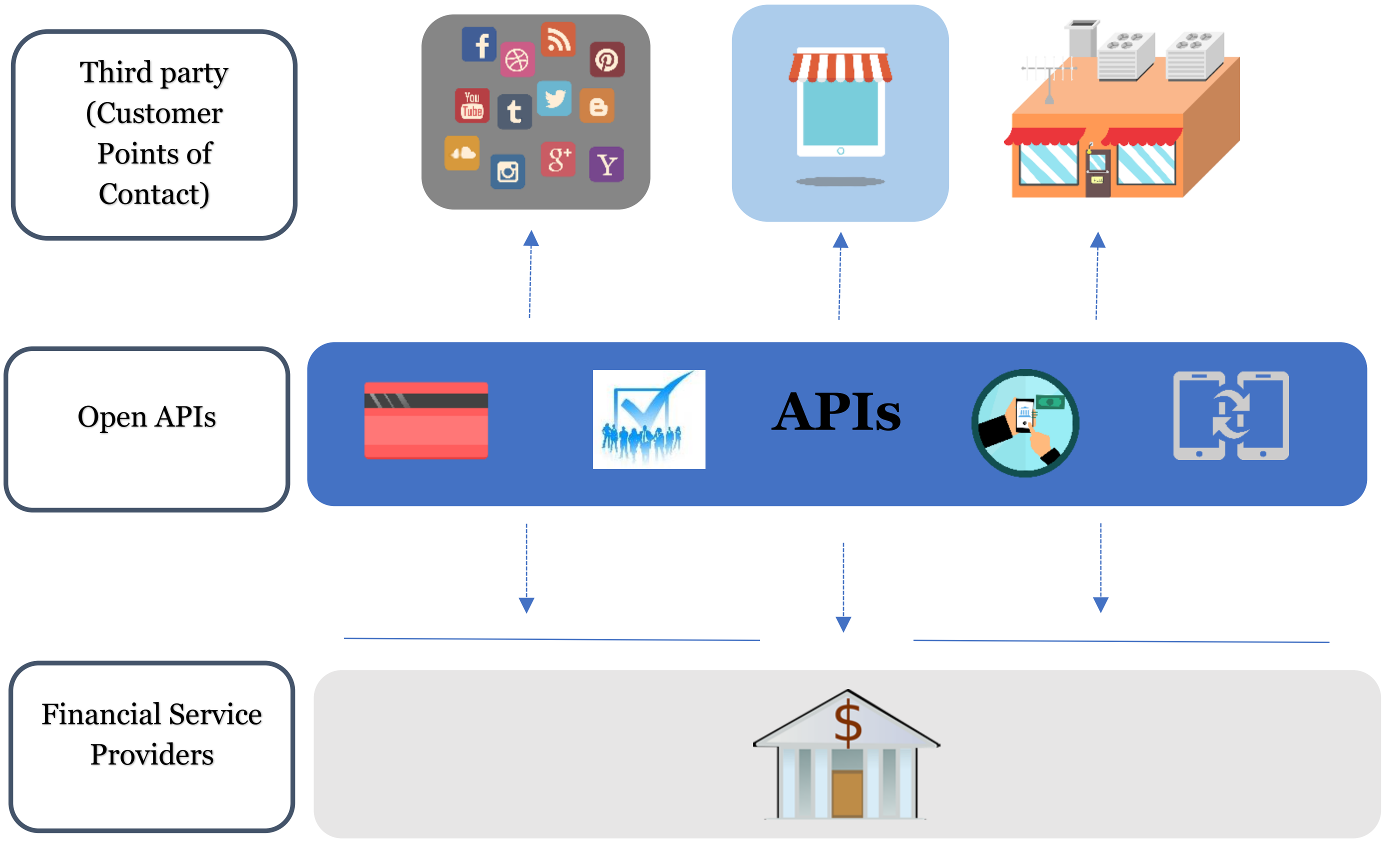
Financial service providers are risk managers at heart. Regulatory supervision incentivizes them to keep non-performing loans to a minimum and ensure that consumers do not exceed allocated debt burden ratios set in place by regulators. Financial service practitioners are also the best versed to advise on financial management best practices and ensure that consumers with low financial literacy are well positioned to overcome arising liquidity issues and thus are best positioned to act as crucial focal points in this new emerging ecosystem of digital finance based on digital identities.

[28] Demertzis, Maria, and Jan Mazza, *Libra: Possible Risks in Facebook's Pursuit of a 'Stablecoin'*, Bruegel, 17 July 2019, bruegel.org/2019/07/libra-possible-risks-in-facebooks-pursuit-of-a-stablecoin

The Outlook: Responsible Digital Identity Ecosystems

As it stands, the digital identity ecosystem players are operating in silos with financially excluded low-income population segments being affected the most. However, some progressive financial institutions are trying to make the current ecosystem work more efficiently by promoting interoperability between all stakeholders in order to reach common standards among all players. This ecosystem is one in which trusted financial service providers leverage their experience with risk management, gained through decades of abiding by banking regulation, while utilizing the alternative data amassed by technology companies and third-party vendors. In this ecosystem identities can be verified by multiple digital identity attributes (bill and tax payment records, financial statements, call data records, etc.) that are issued by trusted entities who have an established relationship with consumers. In this ecosystem financial service providers would act as financial advisors, while utilizing technology platforms' large consumer bases to best help protect low-income populations with low levels or financial literacy.

Figure 6: Potential Ecosystem Interoperability


Third party (Customer Points of Contact)
Open APIs
APIs
Financial Service Providers

We have observed a trend wherein open banking platforms and APIs create the interoperability and data sharing frameworks required between the ecosystem players, helping financial service providers harness the vast amounts of data collected through customer touchpoints. However, to fully leverage the power of data, two key aspects need to be in place: (i) a truly open data ecosystem beyond financial services where customers can benefit from their data regardless of who holds it (financial institutions, retail companies, technology platforms, mobile network operators etc.) and (ii) international harmonization in terms of common standards to at least ensure a level of interoperability instead of multiple fragmented standards. To fully engage customers, companies should reap the power of data and be able to use all the available customer data (based on previous customer consent) regardless of where it resides. Consequently, this will improve the customer experience and provide safer and more tailored digital products and service offerings.

Financial service providers looking to compete in the new ecosystem and serve a larger customer base are transitioning from the brick and mortar banking approach traditionally aimed at high net worth individuals (known for having a high Average Return Per Customer [ARPU]- low frequency and high value transactions), to contextual banking aimed at mass market segments (known for having a low ARPU - high frequency and low value transactions). To make this transition sustainable and economically more viable financial institutions are harnessing emerging A, B, C, D (Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics) technologies to increase efficiencies and drive down operational and transactional costs. A trend has appeared in which financial service providers are becoming more like open platforms embracing innovation and collaboration in order to make banking more affordable, accessible, tailored, and sustainable. We will be discussing this phenomenon in greater detail in our upcoming third paper which explores the potential business opportunities that can be harnessed from digital identities.

Glossary

Digital Identity is a rapidly developing area, with some actors outside the traditional financial service industry, and terminology is still emerging and evolving. As a result, we thought it would be useful to share a sizable glossary of terms and common definitions as a convenient reference for the reader.

5G

5G is the 5th generation of cellular network technology with key features including one millisecond latency and up to 10Gbps download speed. Additionally, the 5G network is ready to allow 1 million devices to connect per square km which is key to connecting the devices required for Internet of Things. Finally, 5G will provide a connection to the internet for devices travelling up to 500km/h.

Automated Fingerprints Identification System (AFIS)

A system which automatically compares an unknown fingerprint or set of fingerprints against a database of stored fingerprints in order to find a potential match. Although this system is primarily used by law enforcement agencies to verify identities there is additional application in civil or government agencies.

Alternative Data Sources

Data sources such as mobile phone billing, utility billing, e-commerce billing, social media, geographic and others that have not traditionally been used in financial services.

Application Program Interface (API)

A set of protocols and definitions that are used to standardize and automate communication between computer programs allowing them to access the features or data of an operating system, application or other service. [29]

Artificial Intelligence/Machine Learning

Artificial intelligence enables software to exhibit human-like intelligence, including learning, planning, reasoning, problem-solving, and decision-making. Artificial intelligence is a broad field with many sub-fields and related fields, including "machine learning," "deep learning," and "cognitive computing." [30]

Machine Learning is an increasingly important area of cognitive computing which has built upon many of the tools of statistics and econometric modeling. Four key attributes that most ML approaches conform to are: 1. A primary goal of optimizing out-of-sample predictive performance facilitated by welltuned regularization. 2. A significant degree of automation in the model development process. 3. The use of cross-validation to model relationships in the data, i.e., divide data into random separate sets for the purpose(s) of training, testing, and validation.

[29] PRETA, *PRETA Open Banking Europe Directory: Frequently Asked Questions,* https://www.openbankingeurope.eu/media/1174/preta-obe-ug-001-000-obe-directory-public-faq.pdf, viewed 15th August 2019.

[30] Institute of International Finance, *DIGITIZING INTELLIGENCE: AI, ROBOTS AND THE FUTURE OF FINANCE*, March 2016, https://www.iif.com/portals/0/Files/private/ai_report_copy.pdf

4. Applicable to very large volumes of data (although some techniques also work well on small data sets), including, in some cases, unstructured data sources.[31]

AI and ML in Behavior and Biometrics

In the context of identification systems these algorithms are focused on recognizing patterns; notably including convolutional neural networks (CNNs) which are used to process large amounts of data to recognize behavioral patterns and perform highly precise biometric matching.[32]

Assurance

The level of confidence reached in the authentication process that the *persona* is the entity that it claims to be or is expected to be.[33]

Authenticator Assurance Level

A category describing the strength of the authentication process.[34]

Attributes

Identity attributes are a quality, trait, characteristic or knowledge of either a legal, biometric or memorized nature ascribed to an individual and used in the formation or authentication of a unique digital identity within a population. Examples of attributes include legal names, identity numbers, fingerprints, iris scans and mobile phone numbers.

Authentication/Verification

The process of establishing confidence in determining if the authenticators asserted to claim a digital identity are valid; that is, to prove that they are bound to the same person to whom the identity or credential was originally issued. This is often as a prerequisite to allowing access to a system's resources. Examples of authenticators include passwords, fingerprints, voice recognition and facial recognition.

Note: For further information see PSD2, subpoint 'Strong Customer Authentication'

Multi-Factor Authentication/MFA

MFA combines use of two or more authentication factors for enhanced security. MFA may be implemented either by presenting multiple factors directly to the verifier or by using one or more factors to protect a secret, which in turn is presented to the verifier--i.e., MFA can be performed, using a single authenticator that provides more than one factor, or by a combination of authenticators that provide different factors.[35]

[31] Institute of International Finance, *Machine Learning in Credit Risk 2nd Edition Summary Report*, August 2019, https://www.iif.com/Publications/ID/3519/Machine-Learning-in-Credit-Risk-2nd-Edition-Summary-Report

[32] Biometric Update, *Glossary of ID4D terms*, April 2019, https://www.biometricupdate.com/201904/glossary-of-id4d-terms

[33] International Telecommunication Union, *Baseline identity management terms and definitions*, April 2010, https://www.itu.int/rec/T-REC-X.1252-201004-I

[34] National Institute of Standards and Technology, *Digital Identity Guidelines*, June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[35] Financial Action Task Force, *DIGITAL IDENTITY – HIGH - LEVEL ISSUES FOR GUIDANCE*, September 2018.

Authorization

Permission granted to perform a given action based on successful authentication and permissions with corresponding levels of assurance.

Biometrics

A biological (fingerprint, face, iris) or behavioral (gait, handwriting, signature, keystrokes) attribute of an individual[36] that can be used for automated recognition.[37]

Blockchain

A blockchain is a distributed structure to record data in blocks and then chain them to the next block using a verification method such as a cryptographic signature. These blocks form a common distributed ledger which can be viewed and validated by any node on the network and has attributes similar to a database.

Claimant

A digital persona asserting ownership of certain identity attributes

Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. With cloud customers share the same physical resources, securely separated at the logical level, supporting heterogeneous client platforms such as mobile devices and workstations.

Concentration Risk

A market in which few players concentrate most of the market share for the provision of a good or service. Such a market condition can pose a substantial threat in the case of operational failure by a provider; introducing portability standards and encouraging multiple vendors is a strategy to mitigate this risk.

Credential

A credential is an object or data structure that signals ownership over an identity as validated by the entity that issues it. Passports, ID cards, passwords are credentials; in the digital identity space credentials can include digital tokens or registered biometrics.

Customer Due Diligence (CDD)

The objective of CDD is to enable the bank to understand the nature and purpose of customer relationships, which may include understanding the types of transactions in which a customer is likely to engage. These processes assist the bank in determining when transactions are

[36] International Organization for Standardization & International Electrotechnical Commission, *ISO/IEC 2382-37, INFORMATION TECHNOLOGY -- VOCABULARY -- PART 37: BIOMETRICS*, February 2017, https://www.iso.org/standard/66693.html

[37] National Institute of Standards and Technology, *Digital Identity Guidelines*, June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

potentially suspicious.[38] FATF's Recommendation 10 on CDD is based on four pillars, requiring: 1) identification and verification of customers, 2) identification and verification of beneficial owners, 3) understanding the nature and purpose of transactions, 4) monitoring the clients and their transactions on an ongoing basis.[39]

Cybersecurity

Technologies, processes and measures that are designed to protect systems, networks, and data from cyber-attacks and other incidents.[40]

Cyber-resilience

Maintaining the entity´s overall ability to deliver the intended outcome continuously at all times, even when regular delivery mechanisms have failed, such as during a crisis or when a security breach occurs. Being cyber resilient includes the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.[41]

Data Analytics

Data analytics refers to an analysis process that encompasses the sorting and cleansing raw datasets, the subsequent modelling and analysis of sorted data and the conclusions drawn from the analysis. Through using algorithms and applied computational power data analysis allows for the observation of trends that are typically unobservable to humans given the magnitude of the dataset.

Data Proportionality

When assessing the processing of personal data, proportionality requires that only that personal data which is adequate and relevant for the purposes of the processing is collected and processed.[42]

Data Portability

Part of open banking and new data frameworks; data portability allows users to take their banking history and/or identity attributes to additional financial service providers than those that they have existing relationships with.

Note: Data portability is linked to the concept of self-sovereign ID.

Device ID/Device Fingerprinting

Device fingerprinting is a device identification technique for identifying a computing device based on its unique configurations. While many people might own the same device model factors such as location, time zone settings, operating system, apps and plugins installed,

[38] Federal Financial Institutions Examination Council, *Customer Due Diligence — Overview,* May 2018, https://www.ffiec.gov/press/pdf/Customer%20Due%20Diligence%20-%20Overview%20and%20Exam%20Procedures-FINAL.pdf

[39] Financial Action Task Force, *The FATF Recommendations*, June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[40] Institute of International Finance, *IIF Staff Paper on Addressing Cybersecurity Regulatory Fragmentation*, May 2018, https://www.iif.com/portals/0/Files/private/iif_cyber_reg_04_25_2018_final.pdf

[41] Ibid.

[42] European Data Protection Supervisor, *Necessity & Proportionality*, April 2017, https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en, viewed 20th August 2019.

browser history and browser versions can be tracked to identify a unique device. The goal of device fingerprinting is to connect online identities to real-world ones. It is predicted that device fingerprinting will be increasingly important through the transition into the Internet of Things era of technology.

Digital Identity

A Digital Identity can best be described as a compilation of electronically captured and developed attributes and credentials of a uniquely identifiable persona that can be linked to a physical person.[43] It should be noted that there is an evolving taxonomy of the term and it is used broadly and interchangeably by different actors in the ecosystem.

Digital Identification

The process of verifying claimed attributes and credentials unambiguously linked to a persona in a domain through a digital channel.[44]

Distributed Ledger Technology

A database held across multiple locations and with multiple participants (nodes), in which there is no single authority and edits to existing data only proceed with a majority of node consensus. In financial services, each node will keep a timestamped record of all transactions that occur across the network, irrespective of whichever node inputs the data.

Encryption

A means of securing data by applying it to an algorithm which converts it into ciphertext. Through encryption individuals and companies can protect sensitive information from unauthorized access.

Homomorphic Encryption

A process by which encrypted data, ciphertext, can be computed without decryption such that when decrypted the plaintext reflects the transformative effects of the earlier computation. This allows third parties, such as cloud computing providers, to compute user data without decryption nor knowing the personally identifiable information. The advantages of this are decreased security risk and increased privacy protection.

Factor

Identity credentials and/or attributes that the claimant possesses and controls that are required in the authentication process.[45] Authentication factors are something you know, something you

[43] ID4D, *Practitioner's Guide*, June 2019, http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-Guide-Draft-for-Consultation.pdf

[44] McKinsey, *Digital Identification: A Key To Inclusive Growth*, January 2019, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx

[45] ID4D, *Practitioner's Guide*, June 2019, http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-Guide-Draft-for-Consultation.pdf

have or something you are.[46] Examples of factors include passwords, fingerprints, iris scans and keycards.

Financial Inclusion

Providing access to an adequate range of safe, convenient and affordable financial services to disadvantaged and other vulnerable groups, including low income, rural and undocumented persons, who have been underserved or excluded from the formal financial sector.[47]

Unbanked

The unbanked refers to those without a checking or savings account.

Underserved/Underbanked

The underbanked may have a checking or savings account but regularly rely on alternative financial service providers due to barriers in use such as access, financial literacy, thin credit history and costs.

Fraud Prevention

The prevention of the use of false or misrepresented information by entities to gain illicit access to services.[48] A primary focus of fraud prevention solutions is addressing weaknesses in current manual processes where false information or manufactured identities are used. Strong digital identity frameworks with widespread implementation will strengthen the connection between physical persons and information on record, lessen the spread of fake identities and allow for greater traceability and verification of transactions, thereby consolidating efforts to prevent fraud.

Foundational Identification System

An identification system primarily created to be used for all legal identity purposes. Examples of this include national IDs, civil registries and passport numbers.

Functional Identification System

An identification system created for a particular service such as voting, tax administration and social programs. Examples of this include tax ID numbers, ration cards or voter IDs.

Transactional Identification System

A transactional digital identity is intended to ease the conduct of transactions[49]; typically, a transaction identity comprises biographical data. The specific set of biographic data required depends on the requirements of the transaction.

General Data Protection Regulation

[46] National Institute of Standards and Technology, *Digital Identity Guidelines*, June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[47] Financial Action Task Force, FATF Guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence , November 2017, https://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

[48] World Economic Forum, *A Blueprint for Digital Identity*, August 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[49] International Telecommunication Union, *Digital Identity Roadmap Guide*, November 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-DIGITAL.01-2018-PDF-E.pdf

A European Union directive that establishes binding parameters for the collection and use of data that can be used to identify residents of the European Union. The GDPR is designed to protect data across all sectors harmonize data privacy laws across Europe, Protect and empower all EU citizens data privacy and Reshape the way organizations across the region approach data privacy.[50]

Identity Provider

A trusted entity—e.g., a government agency or private firm—that issues and/or authenticates credentials.[51]

Internet of Things

The Internet of Things refers to the state in which most devices are connected to the online network and are therefore in a perpetual state of sending and receiving data. This allows for person to person, person to machine and machine to machine communication to occur and consequent opportunities for both significant efficiency gains and significant security concerns over data breaches.

Interoperability

The ability of different systems, databases, devices, or applications to communicate, execute programs, or transfer data in a manner than requires the user to have little or no knowledge of those functional units.[52]

Know Your Customer (KYC)

Refers to the collecting, generating and processing of customer and applicant data as a means of preventing financial crime. Know-Your-Customer processes include sanctions and politically exposed person-checks, transaction and behavior monitoring and risk assessments.

Note: See Customer Due Diligence for further information

Electronic-Know Your Customer (E-KYC)

E-KYC is a process in which approved entities either query a digital (and usually national) ID system to authenticate or verify their customers' identities and, in some cases, retrieve basic information about them, or, allow customers to onboard remotely using biometric technology such as facial recognition software and fingerprint or iris scanning. E-KYC systems can improve the onboarding process by reducing or eliminating paper-based procedures and record-keeping, which reduces cost and time spent on verification, making it more profitable to provide services to low-income customers.[53]

[50] European Union, *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016*, April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[51] ID4D, *Practitioner's Guide*, June 2019, http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-Guide-Draft-for-Consultation.pdf

[52] International Organization for Standardization & International Electrotechnical Commission, *ISO/IEC 2382:2015, INFORMATION TECHNOLOGY -- VOCABULARY*, May 2015, https://www.iso.org/standard/63598.html

[53] Pisa, Michael & Woodsome, Jim, "*Overcoming the "Know Your Customer" Hurdle with E-KYC*," Center for Global Development, February 2019, https://www.cgdev.org/blog/overcoming-know-your-customer-hurdle-e-kyc

Note: See Customer Due Diligence for further information

Legal Entity Identifier

The Legal Entity Identifying number is a 20-digit code of letters and numbers assigned to a financial institution thereby allowing regulators to track their transactions across multiple jurisdictions. The first four digits in the code correspond to the local issuing organization, the middle 14 digits are an assigned unique code and the final two digits are check digits. Through the LEI businesses can calculate their risk through exposure to other firms.

Liability Risk

The threat of a company or individual having to bear the consequences of damage or of breaching standards due to operations, a product, an act or neglect.[54] In the context of digital identities, a private digital identity model might see liability risk emerge in the context of one financial provider establishing and issuing an interoperable digital credential on the basis of false information which then exposes another provider to fraud derived damages.

Machine Readable Data

Machine readable data refers to the presentation and arrangement of data such that it can be automatically recognized and processed by a computer equipped with the capability to scan and retain the data. This is opposed to human readable data which can be understood and interpreted by humans but not by computers.

Digital Identity Operation Models

Centralized

A model in which a central authority determines use cases and regulations, prompts widespread use, funds the operation and is responsible for all data capturing and storage.

Decentralized

A model that leverages distributed ledger technologies like blockchain resulting in a system characterized by both the lack of central authority responsible for management and the enhanced control of the user over their data distribution and storage.

Federated

An association of users and identity service providers that allow for the use of a token from one process to authenticate the same users for a different system. Ownership is shared among multiple stand-alone systems that share common standards.

Hybrid

A model in which ownership and responsibility of production and infrastructure of Digital IDs are shared by multiple private and public entities. The ecosystem operates on

[54] IF Insurance, Risk Management Services, https://www.if-insurance.com/large-enterprises/service-concept/risk-management-services, viewed 22nd August 2019.

shared common standards where the network is publicly endorsed or based on standards issued by the public sector. [55]

Public

In this model governments determine what constitutes the identity of a person, use cases and regulations, they incur digital identity infrastructure and operational costs, they drive widespread adoption and (usually) hold a central repository. [56]

Private

Digital identities are developed, implemented and maintained entirely by private entities and typically users retain greater control over the management of their data; a number of these solutions are based on blockchain technology, with private entities maintaining the nodes. [57]

Self-Sourced

A model pertaining to the distribution of decentralized, portable and lasting digital identities that are completely controlled by their owners. This model allows the user to determine exactly who they want to share data with and exactly which data they want to share. Another feature of this model is the notion of transparency, in which institutions must be transparent with users in how their data is being stored, used and computed. This ensures that user control over their data is maintained.

PSD2

The revised Directive on Payment Services aims to; provides the legal foundation for the further development of a better integrated internal market for electronic payments within the EU; put in place comprehensive rules for payment services, with the goal of making international payments (within the EU) as easy, efficient and secure as payments within a single country; open up payment markets to new entrants leading to more competition, greater choice and better prices for consumers; and provide the necessary legal platform for the Single Euro Payments Area (SEPA).[58]

Strong Customer Authentication

An authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.[59]

Remote Onboarding

[55] Institute of International Finance, *Digital Identities in Financial Services Part 1: Embedding in AML Frameworks, August 2019*, https://www.iif.com/Publications/ID/3534/Digital-IDs-in-Financial-Services-Part-1-Embedding-in-AML-Frameworks

[56] Ibid.

[57] Ibid.

[58] European Commission, *DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015*, November 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

[59] Ibid.

Remote onboarding is the culmination of e-KYC and e-signatures in which the digital transmission of attributes allows individuals to apply for financial services and have their claimed attributes verified without having to be present within a branch. Remote onboarding reduces the time and money associated with onboarding compared to previous practices and given facial recognition technology it can be KYC compliant. Facial recognition technology matches a user's face from a real time photo to one in a scan of a of a government issued ID, thereby matching the individual to the claimed identity.

Sustainable Development Goals

A set of goals adopted by all UN member states in 2015, the SDGs area call to action by all countries to promote prosperity while protecting the environment. They recognize that ending poverty must go hand-in-hand with strategies that build economic growth and address a range of social needs including education, health, equality and job opportunities, while tackling climate change and working to preserve our ocean and forests.[60]

Sustainable Development Goal 16.9

By 2030, provide legal identity for all, including birth registration.[61]

Third Party Reliance, Digital Identity

In the context of digital identity relying parties (RPs) are entities that accept attestations from identity providers about user identity to allow users to access their services.[62] In a third-party reliance scenario, the third party should be subject to CDD and record-keeping requirements and be regulated supervised or monitored.[63] More broadly, in financial services the role and legal responsibility of third-party service providers is an active area of debate.

Token/Tokenization

Tokenization is a data management technique that replaces sensitive data with 1-to-1-mapped random data comprising a token.[64] The original personally identifiable information is represented by this digital token which can then be used by commercially engaged third parties as an accepted representation of the sensitive data it protects.

An example of tokenization in payment transactions may provide clarity. Upon payment initiation a merchant will provide the token to their bank, which will contact the token issuer to match the token with a corresponding card or bank account in their token vault. The customer's bank would then approve or deny the payment to complete the transaction. [65] The original

[60] United Nations, The Sustainable Development Agenda, https://www.un.org/sustainabledevelopment/development-agenda/, viewed 22nd August 2019.
[61] United Nations, Peace, Justice and Institutions, https://www.un.org/sustainabledevelopment/peace-justice/, viewed 22nd August 2019.
[62] World Economic Forum, *Identity in a Digital World*, September 2018, http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf
[63] Financial Action Task Force, *The FATF Recommendations,* June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf
[64] Tokenex, *Tokenization vs Encryption: Which One is Best for Your Business?,* July 2013, https://www.tokenex.com/blog/tokenization-vs-encryption-which-one-is-best-for-your-business
[65] Visa, *All you need to know about Tokenization*, https://usa.visa.com/dam/VCOM/download/security/documents/visa-security-tokenization-infographic.pdf, viewed 23rd August 2019.

personal information did not form part of the payment message between the parties involved and therefore the sensitive information could be better protected in a secure environment.

Transaction Monitoring

Transaction monitoring is an Anti-Money Laundering compliance obligation referring to a financial institution's ongoing surveillance of their customer transactions to ensure they are not participating in financial crimes. It is predicted that digital identities will simplify the compilation of data at onboarding and beyond to better understand customers and therefore better classify their transactions as fitting their behavior profile or presenting a risk.

Trust Score

A trust score is an assessment of the probability of a correct match in the authentication of a user.[66] Typically, a trust score is assessed by a third party authentication service provider who will aggregate factors such as the registered email address and whether it contains an alphanumeric string, the time of transaction, the IP address, typical user behavior and even the cadence of the password entry.

Unique Identifier

An alphanumeric string frequently used in payment services that is assigned and issued to a specific individual, entity or transaction for the purpose of unambiguous identification within interoperable ecosystems. [67]

Verification

See Authentication

[66] Biometric Update, *Glossary of ID4D terms*, April 2019, https://www.biometricupdate.com/201904/glossary-of-id4d-terms

[67] European Commission, *DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015*, November 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

Amin Khairy
Policy Advisor, Digital Finance
akhairy@iif.com

Other Contributors

Brad Carr
Senior Director, Digital Finance
bcarr@iif.com

Conan French
Senior Advisor, Digital Finance
cfrench@iif.com

Marcus Wimalajeewa
Intern, Digital Finance
mwimalajeewa@iif.com