European Banking Institute

EBI Working Paper Series

2018 – no. 28

Douglas W. Arner/Dirk A. Zetzsche/
Ross P. Buckley/Janos N. Barberis

The Identity Challenge in Finance:
Identity to Digitized Identification to Digital KYC Utilities

14/08/2018

The European Banking Institute

The European Banking Institute based in Frankfurt is an international centre for banking studies resulting from the joint venture of Europe's preeminent academic institutions which have decided to share and coordinate their commitments and structure their research activities in order to provide the highest quality legal, economic and accounting studies in the field of banking regulation, banking supervision and banking resolution in Europe. The European Banking Institute is structured to promote the dialogue between scholars, regulators, supervisors, industry representatives and advisors in relation to issues concerning the regulation and supervision of financial institutions and financial markets from a legal, economic and any other related viewpoint. The Academic Members of EBI are the following:

1. Universiteit van Amsterdam, Amsterdam, The Netherlands
2. Universiteit Antwerpen, Antwerp, Belgium
3. Πανεπιστήμιο Πειραιώς / University of Piraeus, Athens, Greece
4. Alma Mater Studiorum – Università di Bologna, Bologna, Italy
5. Academia de Studii Economice din București (ASE), Bucharest, Romania
6. Universität Bonn, Bonn, Germany
7. Trinity College, Dublin, Ireland
8. Goethe-Universität, Frankfurt, Germany
9. Universiteit Gent, Ghent, Belgium
10. Helsingin yliopisto (University of Helsinki, Helsinki, Finland)
11. Universiteit Leiden, Leiden, The Netherlands
12. Universidade Católica Portuguesa, Lisbon, Portugal
13. Universidade de Lisboa, Lisbon, Portugal
14. Univerze v Ljubljani / University of Ljubljana, Ljubljana, Slovenia
15. Queen Mary University of London, London, United Kingdom
16. Université du Luxembourg, Luxembourg
17. Universidad Autónoma Madrid, Madrid, Spain
18. Universidad Complutense de Madrid/CUNEF, Madrid, Spain
19. Johannes Gutenberg University Mainz (JGU), Mainz, Germany
20. University of Malta, Malta
21. Università Cattolica del Sacro Cuore, Milan, Italy
22. Πανεπιστήμιο Κύπρου / University of Cyprus, Nicosia, Cyprus
23. Radboud Universiteit, Nijmegen, The Netherlands
24. Université Panthéon - Sorbonne (Paris 1), Paris, France
25. Université Panthéon-Assas (Paris 2), Paris, France
26. Stockholms Universitet/University of Stockholm, Stockholm, Sweden
27. Tartu Ülikool / University of Tartu, Tartu, Estonia

EBI Working Paper Series

EBI Working Paper Series are a project of the European Banking Institute e.V.. EBI Working Paper Series represent a selection of academic researches into the area of banking regulation, banking supervision and banking in general which have been drafted by professors and researchers of EBI Academic Members and selected by the Editorial Board.

Editorial Board

Faculty of Law,
Economics
and Finance

Law Working Paper Series
Paper number 2018-008

The Identity Challenge in Finance:

From Analogue Identity to Digitized Identification to Digital KYC Utilities

Douglas W. Arner, University of Hongkong
douglas.arner@hku.hk

Dirk A. Zetzsche, University of Luxembourg
Dirk.Zetzsche@uni.lu

Ross P. Buckley, University of New South Wales
ross.buckley@unsw.edu.au

Janos N. Barberis
janos@fintech.hk

25/09/2018

UNIVERSITÉ DU LUXEMBOURG

University of New South Wales Law Research Series

The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities

DOUGLAS W. ARNER, DIRK A. ZETZSCHE, ROSS P BUCKLEY AND JANOS N. BARBERIS

[2018] *UNSWLRS* 45

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Electronic copy available at: https://ssrn.com/abstract=3224115

The Identity Challenge in Finance:
From Analogue Identity to Digitized Identification to Digital KYC Utilities

Douglas W. Arner[1], Dirk A. Zetzsche[2], Ross P. Buckley[3] and Janos N. Barberis[4]

Abstract: Identity is fundamental in finance. From a business standpoint, knowledge of clients' identities is essential to protect against fraud and crime, and underpins all know-your-customer obligations, as well as being essential to providing quality services. From a risk management and regulatory standpoint, identity is essential to market integrity. At the same time, identification and KYC rules can be major barriers to accessing financial services, for individuals and small businesses in particular. This paper considers the various requirements for identification in the financial sector and the evolving nature of identity and its evolution from analogue to digitized to digital. We argue that technology presents an opportunity to solve this challenge through the development of digital identity infrastructure and related utilities. The establishment of such utilities for digital or electronic identification requires addressing design questions such as registration methods, data availability and cross-jurisdiction recognitions. Yet, as with any reform, a balance between flow-through efficiency and cyber-security needs to be reached to ensure the objectives of financial inclusion and market integrity are not achieved at the detriment of financial stability.

Keywords: Finance, Identity, Digital Identification, eKYC Infrastructure, KYC Utilities, Market Integrity, Anti-money laundering, Financial inclusion, FinTech, RegTech.

[1] Kerry Holdings Professor in Law, University of Hong Kong. Douglas.Arner@hku.hk

[2] Professor of Law, ADA Chair in Financial Law (Inclusive Finance), Faculty of Law, Economics and Finance, University of Luxembourg, and Director, Centre for Business and Corporate Law, Heinrich-Heine-University, Düsseldorf, Germany. Dirk.Zetzsche@uni.lu

[3] KPMG Law King & Wood Mallesons Chair of Disruptive Innovation, Scientia Professor, and Member, Centre for Law, Markets and Regulation, UNSW Sydney. Ross.Buckley@unsw.edu.au

[4] Co-Founder, SuperCharger, and Research Fellow, Asian Institute of International Financial Law, University of Hong Kong. janos@fintech.hk.

The authors are grateful for comments from Iris Chiu, Emilios Avgouleas, Pierre Schammo, Jean-Louis Schiltz, Anton Didenko, Tsany Ratna Dewi as well as participants of the Alliance for Financial Inclusion Global Policy Forum (AFI GPF) in Sochi (September 2018), and for the research assistance of Rohan Balani. All responsibility is the authors'.

The authors gratefully acknowledge the financial support of: the Luxembourg National Research Fund, project "A new law for Fintechs – SMART Regulation", INTER/MOBILITY/16/11406511; the Australian Research Council, project "Regulating a Revolution: A New Regulatory Model for Digital Finance"; and the Hong Kong Research Grants Council Theme-based Research Scheme.

Contents

"On the internet, nobody knows you are a dog."

Peter Steiner, The New York Times (5 July 1993)

1 Introduction

The technological developments of the last three decades are challenging policymakers, regulators and financial institutions alike. In particular, this is seen around peoples' identity. Identity can today be either analogue (paper documents), digitized (as in the scan of an ID document) or digital (such as online footprints). Whilst any and all may be used for authentication purposes (such as accessing a social media or banking account), they are not universally compatible nor acceptable for all purposes. Anonymity is a feature, not necessarily a failing, of the internet and this directly conflicts with various customer identification requirements in finance. The coming sea-change in finance is the entry of technological and data companies into financial services, best exemplified, globally, by the rise of Ant Financial from the e-commerce origins of Alibaba in China.[5] The critical question, in this context, then becomes whether such new entrants, which we in other work have dubbed "TechFins",[6] should adapt to existing identity regimes, or, as they have in China, be permitted effectively to privatise, the previously essential sovereign, function of identity verification.

The development of the internet since the mid-1980s has transformed much of financial services. For example, the combination of personal computers and the internet gave rise to e-banking in the 1990s. With it came a series of unanswered questions: Can a pin code replace a "wet signature" to identify a person and authenticate a transaction? If services can be rendered digitally and globally what happens with the cross-border marketing of financial services and remote onboarding of new customers?[7] Three decades later, whilst the industry has made progress in terms of digital transformation, an end-to-end online experience for most financial services customers remains more a dream, than a reality.

The internet has led to the development of new industries such as social media (i.e. Facebook, Instagram, Tencent) and e-commerce (i.e. Amazon, Alibaba). Each of these have (re)defined what identifies a person and how to authenticate them. For example, social media credentials can be used to open an e-commerce account,[8] and a person can simply transfer payment information from one merchant to another (i.e. via Amazon Pay) without the necessity of re-registering. While it is important to ensure the right party is accessing these services, mis-identifying an e-commerce customer does not carry the consequences it does for a financial services customer in terms of fraud prevention, combatting money laundering and terrorist financing, financial stability or regulatory compliance.

To repeat, anonymity is a feature, not a failing, of the internet. The possibility and acceptability of anonymity and use of avatars for one's online persona underpin some internet businesses. Following the 2008 financial crisis reforms and various counter terrorism financing requirements, no financial institution could accept that nearly 10% of their customers are registered under false names. However, this is so for Facebook, which reported that 270 million

[5] Zetzsche, Buckley, Arner, & Barberis (2018).
[6] Id.
[7] See, Future of Banking in Hong Kong – The Impact and Implications of Internet Banking (HKMA), last accessed 2nd July 2018, available at: http://www.hkma.gov.hk/eng/key-information/speeches/2000/.
[8] Example: the google email identity may be used to certify a personality for online accommodation service Airbnb.

accounts from its 2.1 billion user base could be fraudulent or duplicates.[9] And whilst this number is lower with e-commerce platforms, as they process payments and need to make physical delivery of goods, the standard of customer identification does not need to go beyond a payment mechanism and delivery address. Once paid for, the goods can be sent to whomever you like; e-commerce providers usually do not care.[10]

In practice, the various know-your-customer (KYC) requirements across industries create different onboarding procedures, identification requirements and authentication methods. This seems to be in line with the notion of proportionality, given the lesser impact of mis-identification for a social media platform compared to a universal bank. But if a technology or data driven company is moving into financial services, its less rigorous regime, while more "efficient", at some stage will have to rise to the level required in financial services, both from the standpoint of preventing the criminal and terrorist use of the financial system as well as from the standpoint of having a level playing field in terms of compliance and regulatory requirements for participants offering similar services, regardless of the underlying structure of their technological or other platform.

In both digitized and digital forms, one's identification – and even identity – is converted into an electronic form, whether a digitized version of a passport (i.e. e-KYC) or a digital aggregation of one's online footprint (i.e. through analysis of browsing cookies). In some cases, these identities are collected and verified on a regular basis (i.e. for bank account maintenance) or instead transferred between entities (i.e. social media credentials).

Whilst the acceptability of varying forms of online identification and identities, whether a digitized passport or someone's cookies, can be solved by changing regulatory requirements, the cross-compatibility, whether legally or technically, of someone's online identity raises the question about the necessity to develop a new regulatory framework (see Part 4) or technical utility design (see Part 5).

This paper addresses these increasingly pertinent questions. At a time where TechFins are making inroads into the financial services industry, and therefore collecting or transferring customer money, a tension emerges as to which is the most effective method of customer identification and KYC. Should the solution be found in the redefinition of one's identity? In the methodology of retrieving one's identification? Or both or in other ways?

To answer the above, this paper is structured as follows: following this introduction, Part 2 considers the challenge of identity and identification in finance. Part 3 provides a taxonomy of digital identities, designed to create a common basis of understanding. Part 4 looks at the opportunities brought by the digitization of identities at the consumer or national levels, to guide policy and highlight industry incentives that will function as pillars for this market reform. Part 5 considers the design of e-KYC infrastructure on the basis of digital identification infrastructure and submits a three-part framework covering design, responsibility and governance aspects of such digital identity utilities. Part 6 concludes.

[9] See, Facebook quietly admits to as many as 270 million fake or clone accounts (Mashable), last accessed 5th July 2018, available on https://mashable.com/2017/11/02/facebook-phony-accounts-admission/#mF1YEcTMmPqp.

[10] The degree of e-identification depends on the business model. Certain e-commerce platforms require a greater degree of identification. For instance, accommodation providers such as Airbnb require digital passport copies in addition to payment information, car rental service providers require a digital copy of a drivers' license etc.

2 The Identity Challenge in Finance

The financial services sector supports economic growth and development through allocating financial resources, providing investment opportunities, and managing risks. Financial regulation seeks to promote these functions through minimizing the frequency and severity of financial shocks (financial stability), enhancing access to financial services (financial inclusion), and promoting market integrity.[11] For an international financial centre such as Hong Kong, Luxembourg, London or New York, competitiveness derives from balancing these objectives and providing the necessary infrastructure for financial markets to function well.[12] For any economy, balancing these objectives is central to economic growth and development.

Verifying customer identity and carrying out "know your customer" (KYC) due diligence on acceptance of a new customer (on-boarding) and on an ongoing basis are fundamental to market integrity, as these are essential to maintaining confidence and trust in the financial system and reducing the likelihood of criminal or terrorist access to financial services. The rules for these measures are embodied in a wide range of AML/CFT/CDD requirements (anti-money laundering/countering the financing of terrorism/customer due diligence),[13] based on internationally agreed approaches.[14] In addition, CDD underpins how customer needs are understood, and is essential to providing appropriate financial services, a function often summarized under the general framework of suitability.[15]

At the same time, these requirements restrict access to financial services and must, therefore, be balanced against the objectives of financial inclusion and economic growth. In particular, loss of access to the financial system restricts access to financial services for small- and medium-sized enterprises (SMEs). SMEs are central to economic growth, innovation and reducing, or in some cases eliminating, their access to finance has important consequences for growth, innovation, and development. For example, it is estimated that in Asia, the funding gap

[11] For instance, by striving to prevent the criminal or terrorist use of the financial system and limit market manipulation and misconduct; as all of this behavior impacts confidence and trust in the financial system.
[12] Financial Stability Board (2017).
[13] For the E.U. rules, see the Fourth AML Directive (Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 141, 5.6.2015, p. 73–117; for Hong Kong see (i) the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance ("AMLO"), (ii) the Organized and Serious Crimes Ordinance ("OSCO"), (iii) the Drug Trafficking (Recovery of Proceeds) Ordinance ("DTROP"), and (iv) the United Nations (Anti-Terrorism Measures) Ordinance ("UNATMO"); for Singapore see the Monetary Authority of Singapore's various notices and guidelines on AML/CFT, *available at* http://bit.ly/2p5BgJX; for Australia, see *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).
[14] See the standards provided by the Financial Action Task Force (FATF), http://bit.ly/2f1TJAA. The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system. The FATF is, therefore, a "policy-making body" that works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. The FATF framework is composed of the 1) FATF Recommendations 2012, 2) international anti-money laundering and combating the financing of terrorism and proliferation (AML/CFT) standards, and 3) FATF Methodology to assess the effectiveness of AML/CFT systems 2013.
[15] For the E.U., see Article 25 of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments, OJ L 173, 12.6.2014, p. 349–496.

for SMEs represents some USD 1.6 trillion.[16] This is key as SMEs provide 80% of employment and economic growth for most countries.

In addition, financial institutions, corporates, and individuals in emerging and developing markets are often seen as "high risk" and hence subject to "de-risking" (including much of Asia, Africa and South America),[17] particularly by financial institutions from Western developed markets.[18] This issue has become sufficiently significant to be a focus of the G20,[19] the Basel Committee on Banking Supervision,[20] the Financial Stability Board ("FSB"),[21] and the Financial Action Task Force ("FATF"), among others, with one solution being to adjust standards in order to reduce the disproportionate impact on correspondent banks in emerging and developing markets and their customers.[22]

Beyond SMEs and correspondent banking, the G20 (particularly through its focus on digitally inclusive finance)[23] and the United Nations (UN) (in particular through the UN Sustainable Development Goals)[24] have made financial inclusion a central policy objective, on equal footing with financial stability and integrity. In this context, in addition to de-risking, AML/CFT/CDD requirements often make it difficult for underserved segments of society to access the formal financial system, particularly the poor and rural residents. Financial inclusion is seen as central to supporting economic growth and reducing poverty and inequality, as it empowers individuals to improve their circumstances by using financial services, and particularly digital financial services delivered through mobile and smart phones.

Because of the sometimes conflicting objectives and regulatory frameworks of transparency, privacy, financial integrity, revenue collection, financial inclusion, economic growth, and financial stability, identification and identity pose particular challenges in the context of finance.

3 The Evolution of Identification and Identity: Analogue to Digitalized to Digital

Just as the financial services industry has changed significantly with the progressive introduction of technology from the 1970s onwards, the concept of identity has evolved over time. Starting with the creation of the first passport in 1414 in the UK[25] it has reached the point

[16] See Global trade finance gap reaches US$1.6 trillion, SMEs hardest hit (ADB) last accessed 5th June 2018, available on: https://www.adb.org/news/global-trade-finance-gap-reaches-16-trillion-smes-hardest-hit-adb.
[17] International Finance Corporation (2017) p 13.
[18] For instance, the Hong Kong Monetary Authority (HKMA) issued a circular on de-risking and financial inclusion on September 8, 2016 (http://bit.ly/2Im1cJv) to banks operating in Hong Kong: the HKMA observed months of media reports on the plight of some customer groups who were excluded from banking services. The HKMA warned about the dangers of screening out too many potential customers, because the resulting de-banking or financial exclusion of some customer groups could harm Hong Kong's economy and its reputation as one of the world's leading international financial centers. As a follow up, on 11 October 2017 the HKMA, Securities and Futures Commission (SFC), and Insurance Authority (IA) each relaxed their respective requirement to verify addresses in the context of AML (see Ref. B10/1C, http://bit.ly/2FByORK).
[19] See Global Partnership for Financial Inclusion (2017); International Finance Corporation (2018).
[20] See International Finance Corporation (2017) p 12, International Finance Corporation (2016) p 2.
[21] See World Bank (2018) p 1.
[22] See 'Outcomes FATF Plenary, 21-23 February 2018', FATF, http://bit.ly/2EMkwRT.
[23] GPFI, 2016, "Updated G20 financial inclusion indicators focus on digital financial services," G20 Financial Inclusion Indicators, August 10, http://bit.ly/2FvXkrI.
[24] UNCDF 'Financial Inclusion and the SDGs," United Nations Capital Development Fund, http://bit.ly/2DkTBap.
[25] See, A brief history of the passport (The Guardian) last accessed 5th July 2018, available on https://www.theguardian.com/travel/2006/nov/17/travelnews.

that in some instances one is dealing with a new definition of identity rather than merely a modernized version of an old process of identification.

3.1 Typology of Identification

The present discussion needs to be understood in the broader context of the datafication of society – sometimes referred to as the 4th Industrial Revolution.[26] This fourth stage of industrialization since the 18th century is characterized by an additional use of technologies that is blurring the lines between the physical, digital, and biological spheres, collectively referred to as cyber-physical systems.[27] As with understanding any major economic shift, a multi-disciplinary approach is needed. We have previously argued that a forward-looking regulatory framework is only achievable if one simultaneously considers three separate issues: digital identity, data management and financial regulation.[28]

This section, therefore, focuses on the first issue by providing a taxonomy and definition of identity.

Starting with a definition, someone's identity can take one of four different forms and be in one of two states: static or dynamic.[29] The four different forms include:

- *Physical identity* will be an element such as fingerprint, IRIS or DNA.
- *Legal identity* will be documents such as passports, national ID cards or driving licence.
- *Electronic identity* is composed of social media accounts such as Twitter, WeChat, etc.
- *Behavioural identity* captures the unique way you walk, talk or even hold a phone.

Representing this in a table visually is the following matrix:

State	Static Identities	Dynamic Identities
Form	Physical	Electronic
	Legal	Behavioural

Figure 1: Identity Topology

[26] Klaus Schwab, *The Fourth Industrial Revolution* (World Economic Forum, 1st ed, 2016).
[27] Idem.
[28] Arner, Barberis and Buckley (2017).
[29] See The global identity Dilemma – static biometrics are not the answer (Gartner), last accessed 2nd July 2018 available at: https://blogs.gartner.com/avivah-litan/2016/09/16/the-global-identity-dilemma-static-biometrics-are-not-the-answer/.

Forms of static identification have been relied upon historically to prove an individual's identity to, say, a bank. These are *analogue* forms which require physical documents, or some kind of physical marker like a finger print, and record information used to establish someone's individuality: identity is established by the form of identification. By their nature these forms change very little over time. *Digitized* forms of identity rely on the same limited kinds of information but put them into a digital form which can be more readily used in different contexts, for example in opening a bank account over the internet using scanned versions of otherwise analogue identification documents, or broadcasting one's own features via the internet to an identification clerk who performs background checks by asking questions the answers to which only that person could know.[30] The next stage in the evolution of identity is concerned with the shift to new forms of *digital* identity, in which the concept of "identity" is broadened to include dynamic behavioural characteristics that reflect an individual's distinct personality, for example, by collecting data from social media profiles and analysing patterns of searching and of consumer and other behaviour on the internet. The number of data points assembled that way together makes it very likely that the user is the person s/he claims to be.[31]

These characterizations apply not only to individuals but also to legal entities, which require in most cases some form of legal authorisation (e.g. company registration) in order to exist. That identity can be physical or digital. In many cases today, an entity may be mainly digital.

3.2 Traditional vs. Non-Traditional KYC

Relating the above to the financial services industry, a bank will perform its "legal KYC" when a client opens an account and provides an identity document, such as a passport or company registration. After that, as the banks get to know their customer from a transactional standpoint, this can be extended by capturing payment, insurance or investment data. These touch points represent the bank's principal opportunities to better understand their customer. Whilst the passport provides identification data, the transaction data helps create a profile of a person, including their creditworthiness – an identity which is more than merely identification, fundamental particularly in the context of business and other legal entities.

However, in the second stage banks seem to be at a disadvantage compared with their more tech-driven counterparts such as TechFins[32] or FinTech[33] start-ups. These entities capture both behavioural and overall business data, and also often use safer authentication options. For instance, a datafied firm could capture the way a person holds a phone, or brings it to their ear, using an in-built gyroscope or how (and how often) that person enters a password. Such things can act as second-factor authentication methods. In a similar way, user data from an online persona can result in a better assessment of a customer risk profile. For instance, whether a customer tends to cancel orders frequently, whether s/he engages in risky activities, in general (e.g. paragliding, high mountain engineering, cave diving), or whether the user's lifestyle involves certain risks (such as consumption of unhealthy fast food, ownership of a dangerous dog, or close friendship or kinship with people with infectious diseases). All of

[30] Examples include the online identification performed by German, Luxembourgish and Swiss financial services providers. Infra, at IV.D.
[31] International Bar Association Legal Practice Division Working Group (2015) p. 11.
[32] Zetzsche, Buckley, Arner, & Barberis (2018).
[33] Arner, Barberis, and Buckley (2016).

this information is generated by online devices (i.e. smart phones, fitness monitors, etc) or social media data.[34]

Therefore, unless customers have an account and frequently perform transactions, banks are at a disadvantage, compared to tech companies, in having a comprehensive view of their client. For instance, an average person checks their online bank accounts less than 10 times per month[35], which is to be compared with the hundreds of visits to a social media platform[36] or thousands of messages[37] sent on average on a messaging app over the same period. Less data means less informed decisions, for example in the context of loan origination. In the industry, this is known as having a "thin credit file" limiting banks capacity to assess credit profile of a client and therefore the capacity to (appropriately) sell them a financial product such as a loan.However, consumers do not necessarily have control over this wide-ranging digital identity. The individual might not know who exactly has access to their information, or to what extent, for example if privacy policies are overly complex or otherwise left unread. If the definition of "identity" is limited to only what is considered to be "personally identifiable information" (which may not extend to behavioural data), then the reality of our expanding digital identities cannot be fully appreciated or dealt with.[38] In response to these concerns, the argument has been raised that ownership of this information should instead rest with the person the information is about, rather than with whatever entity is collecting the information.[39] It is therefore important that any dynamic information which banks seek to incorporate into their assessment of a prospective customer's identity has been obtained with consent.

A particular example arises in the context of small and medium businesses (SMEs) who increasingly in the US and China in particular may run the majority of their actitivities through major platforms such as Amazon or Alibaba. Such firms acquire a much more comprehensive picture of the activities of these businesses, in many cases essentially a real time cashflow based picture including linkages to major customers and suppliers. Such data provide an advantage over the traditional data possessed by a financial institution. At the same time, if such cashflow data were combined with financial institution data (e.g. payments to staff) then one would be in a very good position to know the customer and the funds, as well as to provide services, perhaps on an automated basis. This is the TechFin model.

3.3 The Case for E-IDs in Emerging Markets

Rethinking and implementing new digital identity approaches will have a disproportionate benefit in emerging markets precisely because so many people there fail the first hurdle to access to financial services: the provision of a valid ID document.[40] Presently, some 1.5 billion individuals lack a formal, legal form of identity.[41] In other words, 1 in 6 people globally cannot be banked, receive remittances, or access the financial services industry.

[34] For details see our previous works in Zetzsche, Buckley, Arner, & Barberis (2018) and Arner, Barberis, and Buckley (2016).
[35] See, Want Mobile Banking Users? Eliminate login (Bank Innovation) last accessed 2nd July 2018, available on: https://bankinnovation.net/2017/03/want-mobile-banking-users-eliminate-the-login/.
[36] See, 74 Facebook statistics and facts (DMR) last accessed 5th July 2018, available on: https://www.wordstream.com/blog/ws/2017/11/07/facebook-statistics.
[37] See, 65 what's app statistics and facts (DMR) last accessed 5th July 2018, available on: https://expandedramblings.com/index.php/whatsapp-statistics/2/.
[38] International Bar Association Legal Practice Division Working Group (2015) pp. 5-6.
[39] Id. at 7-8.
[40] Klosters (2018),
[41] World Bank, (2018a).

Even where users have a bank account, they use it very rarely. This lack of financial engagement can either be self-imposed (i.e. by cultural or geographical factors) or externally-imposed (i.e. customer fails KYC or risk criteria). As a result, financial exclusion relates not only to the capacity to have a bank account, but also to access financial products that can smooth liquidity constraints (i.e. micro-loans) or protect households from unexpected, or at least unfortunate events (i.e. insurance).

The benefit-risk trade-off in emerging markets makes for a much stronger case of reform, and indeed this is where a lot of the activity has occurred to date, such as the Aadhaar roll out in India (discussed in Part 4). Whilst in the West the development of alternative credit scoring mechanisms using social media[42] represents a marginal improvement to the data-sets available to inform an origination decision, in developing countries this is often the only method to start forming a customer profile. As a result, M-Pesa and use of air-time re-loading history as a proxy for one's monthly income became a successful alternative approach to knowing a customers' (risk) profile. Similarly, in India, the fact that one in five people 10 years ago did not have formal ID documents supported calls for new ways of identification. It also raises issues such as should a country only issue paper-based documents or leapfrog identification and authentication standards by combining legal and physical characteristics?

3.4 Three Concerns

The benefits of reforming the identity approaches in finance do not only accrue to individuals in emerging markets. The consequences of such reform are economy-wide and include stakeholders ranging from banks to tech companies and from governments to supra-national organizations. The breadth of beneficiaries strengthens the policy justification for these reforms.

For example, banks will fall short in their multi-billion digitization transformation programs if they do not rethink KYC processes. Technology companies, ahead of their full entry into financial services, will gain from leveraging external KYC utilities to make-up for the shortfalls in their pre-existing customer identification details. Governments will be able to decrease the cost of paying out benefits to, and collecting taxes from, citizens. Supra-national organizations will be equipped to advance financial inclusion especially for the poor and rural residents.[43] Individuals will gradually gain access to a broader array of financial services, made possible by the providers leveraging a comprehensive set of data about them.

The combination of these potential gains, and today's technological capacity, makes the current framework for both identification and identity outdated. What defines a person can no longer be limited by a static legal document (such as a passport or identity card).

However, the collection and use of dynamic identities, being behavioural or electronic, is not issue-free either. Three concerns are of particular importance.

Firstly, is the issue of fake IDs. Nationally issued legal documents are assumed legitimate because they are issued by states, administered on an apparently bullet-proof centralized

[42] See, Your social networking credit score (Slate) last accessed 5th July 2018, available on http://www.slate.com/articles/technology/future_tense/2013/01/wonga_lenddo_lendup_big_data_and_social_networking_banking.html?via=gdpr-consent.

[43] See, Aadhaar based e-KYC Services – the much needed change for financial inclusion (Microsave) last accessed 5th July 2018, available on http://blog.microsave.net/aadhaar-based-e-kyc-service-the-much-needed-change-catalyst-for-financial-inclusion/. On details, see Arner, Buckley, Zetzsche (2018).

ledger and have built-in security features. In contrast, electronic identities can be tampered with. This can have two dimensions. Existing identities could be amended, or non-existing ones invented. Practically if a person's legal identity, such as a passport, is stolen, a replacement can be ordered. However, if their physical, behavioural, or electronic identity is compromised (for example, their fingerprint, voice patern, or online history), then a part of them has been taken. These cannot readily be replaced, for example because of the fixed number of fingerprints, or because of the difficulty in rebuilding a social media account with all previous friend connections and data.

The second area of concern is loss of privacy. Electronic identities are much more complete and therefore raise privacy questions, especially in the event of data breaches. A number of governments and non-government organisations have nominated principles which could guide the treatment of dynamic digital identities in light of these risks, such as the user control principle (that individuals can choose whether or not, and to what extent, to disclose their information), the transparency principle (that data processors must justify why they are collecting data), and the data minimisation principle (that only the minimum data required for a certain purpose be collected).[44]

Third is the issue of monopolization and the risk of abuse from market power. In the data business, size matters, and this is not only true in terms of business size (where it raises antitrust/ competition law concerns), but also in the number of data points a data firm holds on an individual. The more data points a tech firm holds the better are its identification services, understood as "true identity". It is highly likely that datafied firms can find out the truth about a person's character, and put this knowledge to use, for instance, by charging extra fees for non-fee sensitive individuals, and by adding pictures of little children for certain individuals (such as new grandparents) to get them into a spending mood.

A simple comparison reveals a striking difference: A bank holding a passport or identity card of a customer will know the following: holder's name, date of birth, nationality, photograph, signature, and depending on national passporting customs sometimes also height, eye colour, religion, place of birth, issue date, nationality, maiden name, special features (such as scars), children and some academic degrees (such as Dr). These comprise roughly a dozen data points[45] and need to be contrasted with the 20,000 data points typically held by social credit scoring systems, such as Sesame Credit in China.[46] This shows a tension emerging. Dynamic identities are more complete than their static counterparts, because of the larger data-set gathered on individuals. Of course, the bank will have more data points than those provided by the passport / ID card, as when the customer looks for a certain service such as credit, he or she will provide income-related and expenses information as requested by the bank. The principle is nevertheless true: data businesses know far more about their customers than most customers comprehend. This increased understanding of a person's (digital) identity comes at the risk of being perceived as (too) intrusive by customers or by society at large. Until the

[44] See e.g. International Bar Association Legal Practice Division Working Group (2015);
Mike Bracken, *Identity and Privacy Principles*, UK Government Digital Service (April 24, 2012), https://gds.blog.gov.uk/2012/04/24/identityand-privacy-principles/.

[45] Naturally, the bank will have more data points than those, simply by the fact that the customer looks for a certain service (such as credit), and provides income-related information requested by the bank.

[46] See, Your online, mobile, and social behaviour are now data-points used by fintech start-ups and governments in scoring credit-worthiness, (E27) last accessed 5 July 2018, available at https://e27.co/online-mobile-social-behaviour-now-data-points-used-fintech-startups-governments-scoring-credit-worthiness-20170504/ or See, Your Facebook Page Or Your Credit Score: What's More Important For Getting A Loan? (Fit Small Business) last accessed 5th July, available at https://fitsmallbusiness.com/facebook-credit-score/.

trade-off between data provided and services rendered is made clear, and data protection frameworks are actively enforced or IT solutions[47] to privacy concerns become globally implemented, the acceptance of digital identity as a standard for financial services will be delayed.

3.5 From Analogue to Digital

A *legal identity* is external and personal and *summarizes* who someone is. By contrast, a physical or *behavioural identity* is internal and interactive and *defines* who someone is. Finally, electronic identity, while external and not a natural characteristic of a person, is increasingly internalized by people as they spend more time online and can provide a relatively complete picture of their persona and preferences. Said differently, people have less difficulty providing their passport details to a third party, then their social media credential, as the latter is more intrusive in someone's life.[48]

In this context, two paths exist to solving the identity challenge found in financial markets: Developed markets will probably tend to digitize pre-existing infrastructure while emerging market countries may tend to leapfrog and adopt full digital identities.[49]

Yet if one was to take a global approach, the path of least resistance (from a political, legal, personal and technological standpoint) is to focus on digitizing analogue identities. This would be the first step of a broader and sequenced reform process which would later address enhancing digitized identities to create a full digital identity. However, this second step requires a discussion that goes well beyond finance, as it will entail rethinking privacy standards and achieving a global consensus on existing notions such as data sovereignty,[50] and developing new frameworks that treat data as an economic right.[51] As a result, it may well be easier on a global basis to focus on entities (such as companies) in the first instance and leave individual identification to domestic sovereigns.

[47] For such an approach, see Thomas Hardjono, David Shrier, Alex Pentland, *Trust::Data: A New Framework for Identity and Data Sharing*, MIT Press.
[48] See, US proposes reviewing social media of nearly everyone seeking entry (The Guardian) last accessed 5th July 2018, available on https://www.theguardian.com/us-news/2018/mar/30/us-immigration-social-media-visas.
[49] This geographical distinction as likewise been found in the context of how FinTech has evolved differently in developed markets (i.e. A reaction to the crisis) and developing economies (i.e. a reform mechanism). See Arner Barberis and Buckley (2016).
[50] For details, see Weigegnd (2017).
[51] See Lanier (2014).

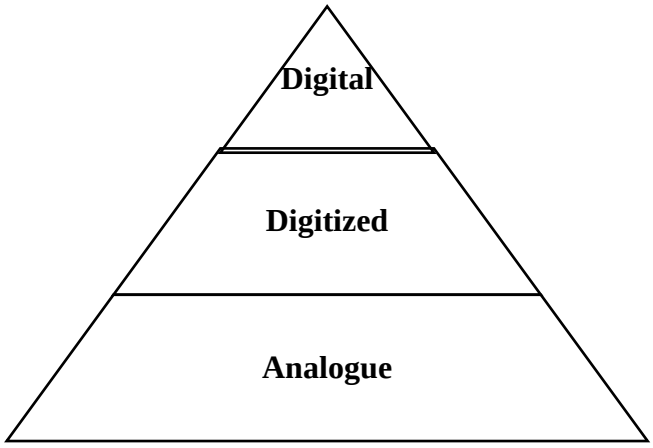

Figure 2: Evolution of identity pyramid

3.6 Windhover Principles

One step in this direction is taken by the Windhover Principles.[52] The Windhover Principles seek to articulate a set of guidelines concerning the management of online identities.[53] They provide that individuals should have control over their digital identities and personal data. Furthermore, they argue that new and evolving digital technologies make it possible to protect an individual's privacy while providing government access to consumer identification. Overall, adherents to the Windhover Principles "pledge to authenticate users' online identity whilst giving customers control over their personal data and allowing them to move it between organisations."[54]

Theoretically, the Windhover Principles can be applied so that: a customer signs up with a digital currency exchange integrated with open source platform and creates an account with all necessary information. The open source platform will then send the identity information to a trusted third party that independently verifies the information. Regulators can access the information via an access token as long as certain procedures are satisfied. [55]

Currently, the Windhover Principles are supported by organisations such as BitPay, Coinsetter and Ripple Labs[56] and have influenced public policy such as New York's bitcoin regulation, the Bitlicence.[57] Considering the Windhover Principles are largely aspirational, its influence has already been significant.

Needless to say that neither one-dimensional approach is meeting practical demands. If all data generated by industry is owned by the clients, industry will stop producing applications

[52] See Lanier (2014).
[53] Token Commons Foundation, *The Windhover Principles for Digital Identity, Trust, and Data* (2014) <http://tokencommons.org/Windhover-Principles-for-Digital-Identity-Trust-Data.html>.
[54] Sarah Todd, 'Manifesto Vows to Give Consumers Control of Digital Identities', *American Banker* (Online) 20 October 2014 <https://www.americanbanker.com/news/manifesto-vows-to-give-consumers-control-of-digital-identities>.
[55] John Clippinger, 'A Proof of Concept Pilot for A Decentralised Autonomous Authority (DAA) For KYC Compliant Decentralised Identity and Authentication Services', (Research Paper ID3, MIT Media Lab), available at <http://financelawpolicy.umich.edu/wp-content/uploads/sites/26/2016/09/Clippinger-A-Proof-of-Concept-Pilot-for-A-Decentralized-Autonomous-Authority4.1.16.pdf>.
[56] Pete Rizzo, 'Why 20 Bitcoin Companies Are Baking a New Deal for Digital Identity', *Coindesk* (online) 21 October 2014 <https://www.coindesk.com/20-bitcoin-companies-backing-new-deal-digital-identity/>.
[57] Ibid.

beneficial for the clients. If on the other hand industry is assigned data property, the privacy implications are severe and unacceptable for liberal-democratic societies. As a third dimension, social welfare demands sharing of *some* data among industry and the state– where the delineating line is, in detail, will be the most important question to answer in the next decade – and most likely this question will be answered differently in the US where data protection and privacy is of lesser importance than in the EU but where at the same time the involvement of the state in the context of identification is far less politically acceptable than in the EU (i.e. it is unlikely that the US will adopt any form of national ID – digital or otherwise – in the near future whereas almost all EU member states now have various forms of national IDs, the UK being an exception pending Brexit).

The remainder of this paper, and in particular Part 4, focuses on digital identity as understood in the context of digitization of static identities. This forms the basis of eID and eKYC frameworks and utilities today, which are discussed in Part 5.

4 Solving the Identity Challenge: Designing Infrastructure for Digital Identification

Financial technology, and in particular "regulatory technology" (RegTech), [58] present opportunities to reconsider existing systems and to build the necessary infrastructure to balance market integrity, financial inclusion, and economic growth, while at the same time meeting commitments to international financial standards including those set by the FATF, Basel Committee, FSB, and the UN. The foundation of this infrastructure will be new forms of digital identification.

In considering systems of digital identification, it is necessary to differentiate between those for people, those for other things, and those for legal entities. Within each of these categories, the system of identity could be established by the sovereign, regulated by the sovereign (perhaps on a monopoly basis), or be private in nature. Such systems can be mandatory (such as a national identity card) or voluntary (as passports are in many countries). If voluntary, they may be encouraged or incentivized through a range of measures, for instance in the context of companies (registration of which is necessary to acquire the entity attributes) and legal entity identifiers (which are now mandatory for entities dealing with EU counterparties under MiFID2 – whether in the EU or otherwise – but are voluntary in many other countries outside of the OTC derivatives context).

In considering identification, it is important to separate both base identity (generally a sovereign function for individuals and corporates) and digital identity. Base and digital identity can be merged, as in Aadhar and Iris Guard; or separate, as in the eIDAS Regulation in the EU and in systems developed by Alibaba and Tencent in China (see infra, at 4.1 to 4.3).

Perhaps the best example of the potential of a comprehensive digital ID system built upon biometrics is Aadhaar in India. This is a national system and has been so strongly encouraged as to be practically mandatory. The other end of the spectrum can be seen in countries without mandated forms of national identification, such as Australia, the US, the UK or Canada. There are also particular challenges in the cross-border context, where there are increasing efforts to use digital identification in the context of border control or more broadly for business purposes, with the EU as perhaps the leading example.

[58] Arner, Barberis, and Buckley (2017).

4.1 Aadhaar in India

India's Aadhaar system is operated by the Unique Identification Authority of India (UIDAI), and involves issuing a 12-digit randomized number to all residents of India to be used to access government services, subsidies, social benefits, banking, taxation, and insurance, among other services. Enrolment to obtain an Aadhaar number is free, and a process of biometric de-duplication seeks to ensure that only one number is generated for each individual. The Aadhaar number issued acts as a proof of identity, but is unrelated to citizenship rights, and does not identify people's caste, religion, or income. To be issued with an Aadhaar number, an individual must satisfy the UIDAI verification process, which requires various demographic and biometric data to be provided, including the individual's name, date of birth, gender, address, mobile number, email address, ten fingerprints, two iris scans, and a facial photograph.[59]

The Aadhaar system also provides for a number of methods of updating data. As the Aadhaar number can be linked to a growing number of services, this is important. Biometric data can, for example, be updated as children grow, or in the case of accidents or diseases, or as the quality of technology improves. Such updates can be undertaken online, using a login consisting of the individual's Aadhaar number and registered mobile number, and uploading the requisite supporting identification documents, or by visiting a permanent enrolment centre in person.[60]

The Aadhaar system is subject to a hotly debated constitutional challenge in the Supreme Court of India at the time of writing. It is being argued that the system is a breach of privacy, and that data are being collected by third-party contractors hired by UIDAI without proper safeguards in place. It is also argued that the biometric identification techniques, fingerprinting and iris scanning, are susceptible to misuse and fraud.[61] In related proceedings in mid-2017, a nine-judge bench of the Supreme Court of India held that Indians have a right to privacy, however, declined to rule on the constitutional validity of the system.[62]

Aspects of the Aadhaar system subject to critique include that the *Aadhaar Authentication Regulations 2016* provide for transaction data to be archived for five years from the date of transaction. Aadhaar has even been described as "mass surveillance technology".[63] However, Aadhaar has also proven beneficial. For example, billions of rupees of financial benefits previously lost annually through fraud and corruption are now finding their way to the intended recipients. The Indian government claims this alone has saved an estimated US$5 billion.[64] In some states of India, before Aadhaar and associated financial services, up to 45% of government welfare payments were failing to reach their intended recipients due to "leakage".

There have indeed been many problems in Aadhaar's implementation, many of which would appear to have arisen because the implementation was rushed, perhaps for political reasons; and information on the system's apparently many practical shortcomings has not been

[59] *About Aadhaar*, Unique Identification Authority of India, http://bit.ly/2HsyzJd.
[60] *Aadhaar data update*, Unique Identification Authority of India, http://bit.ly/2xoDhG4.
[61] Live Law News Network India, 2018, "SC constitution bench to begin final hearing on validity of Aadhaar cards tomorrow," January 16, http://bit.ly/2p866kw.
[62] *Puttaswamy (Retd.) & Anor v Union of India & Ors* (Civil) No 494 of 2012.
[63] Abraham, S., R. S. Sharma and B. J. Panda, 2017, "Is Aadhaar a breach of privacy?" The Hindu, March 31, http://bit.ly/2BpbVyx.
[64] The Economist, 2016, "Indian business prepares to tap into Aadhaar, a state-owned fingerprint-identification system," December 24, http://econ.st/2FyB0hb.

forthcoming. However, difficulties and sloppiness in implementation should not be allowed to detract from the potential of a national biometrically-based identification system to underpin an entire digital financial ecosystem.

4.2 Digital Identification Without a National ID: The Australian GovPass project

Australia lacks any form of national identity card, in part because earlier attempts to introduce such an initiative proved to be highly problematic politically. Identity in Australia today is generally established by reference to documents ranging from passports to drivers' licenses, and by numbers issued for tax purposes or access to Medicare. In response, the Australian Government Digital Transformation Agency (DTA) has produced the Trusted Digital Identity Framework (TDIF), a draft of which was released for public feedback in November 2017, and which is under development at the time of writing. The Framework was prompted by the final report of the 2014 Financial System Inquiry, which recommended that "a national digital identity strategy will help to streamline individuals' engagement with government and provide efficiency improvements."[65] The DTA is also undertaking a project, currently in its beta stage, to produce a digital ID for individuals to easily and securely prove their identity to government services online – the Govpass. Essentially, the technology involves using an "exchange" as a mediator between government departments and a verifier vouching for a user's identity. Once a user receives a "tick of approval" from an accredited verifier, they will be able to access available government online services. In 2018, the DTA is testing TDIF and Govpass frameworks.[66]

In October 2017, the Council of Australian Governments (COAG) reached an agreement that a national scheme should be introduced allowing for biometric identification and matching "to promote the sharing and matching of identity information to prevent identity crime … while maintaining robust privacy and security safeguards."[67] The *Identity-Matching Services Bill 2018* (Cth) was introduced to the Australian parliament in February 2018, and it is currently under consideration by the Parliamentary Joint Committee on Intelligence and Security.[68] If passed, the bill will authorize the Department of Home Affairs to facilitate communication between agencies with the creation of five identity-matching services.[69] The bill also establishes the NDLFRS (National Driver Licence Facial Recognition Solution) and an interoperability hub to act as a "router", matching requests with facial image databases operated by the various services above.[70]

While there is a great deal of activity, therefore, around identity in Australia, the issue remains contentious politically and it would not surprise, in time, to find that many of these worthy initiatives have failed to progress.

---

[65] Australian Government, *Improving Australia's Financial System: Government Response to the Financial System Inquiry*, AUSTRALIAN TREASURY (2015), https://static.treasury.gov.au/uploads/sites/1/2017/06/Government_response_to_FSI_2015.pdf.
[66] *Govpass*, Australian Government Digital Transformation Agency, http://bit.ly/2Go0z1C.
[67] COAG, 2017, "Intergovernmental agreement on identity matching services," Council of Australian Governments, October 5, http://bit.ly/2p5g5YO.
[68] *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018*, PARLIAMENT OF AUSTRALIA, https://www.aph.gov.au/Parliamentary_Business/CommitteesJoint/Intelligence_and_Security/IMSBill.
[69] These include the FIS (face identification service), FRAUS (facial recognition analysis utility service), FVS (face verification service), IDSS (identity data sharing service), and OPOLS (one person one license service).
[70] *Identity-Matching Services Bill 2018* (Cth) s 7(3).

4.3 Interlinking Domestic Digital ID Systems in the EU

In contrast to Australia, Canada, and the US,[71] identity cards with a chip embedded and common security features including the EU-wide use of biometrics are widely spread and used in EU/EEA member states and shared among member states' authorities. In most EU/EEA countries, ID cards have replaced passports and driver licenses for ID purposes.

Initially, this was also true for the UK, where resistance against a pan-European standardized ID card was traditionally fierce. In fact, the UK Presidency of the EU Council in 2005 advanced EU-wide ID card standards, data retention, and intelligence sharing to fight terrorism, following the bomb attacks on the London subway system on 7 July 2005.[72] Following repeal of the British Identity Cards Act by the Identity Documents Act 2010,[73] the British ID cards introduced only in 2006 were cancelled. Since then, only foreign nationals from outside the EU have been required to have an identity card, thereby returning the UK to a state similar to that of Australia, Canada, and the US.

At the same time, a focus of European policy is on promoting cross-border business transactions. European policy actions since the mid-1990s have been focused on trying to ensure that digital signatures and documents signed with such signatures are recognized across borders. A 1999 EU Directive has sought to ensure that advanced electronic signatures based on a qualified certificate and created by a secure-signature-creation device were valid signatures under the laws of each Member State, in the same manner as a handwritten signature, regardless of electronic form; in particular, digital signatures have been admitted as evidence in legal proceedings.[74] However, while good in theory, in practice the e-signature received little recognition. Achieving the e-signature certificate was burdensome, few recipients had the technology to identify the certificate, and after more than a decade the technology underlying the directive was outdated. Further, the directive did not deal with authentication and trust services, two pillars of real importance in today's online markets.

The failure of these initiatives is particularly evident in cross-border transactions, where EU cross-border online services represented a meager 4% of online sales, compared to national online trade which represents 42% of sales, and US-based online services which represent a surprising 54%. This is seen as a real barrier to completing the European internal market; and highlights how enterprise-made identification systems dominate the European online economy.[75] As a response to such trends, European regulators adopted the eIDAS Regulation (eIDASR)[76] in 2014 with a view to reducing the costs of transacting online, be it in commerce or financial services, and enhance competition.

The eIDASR provides "a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities."[77] The underlying

[71] See on the U.S., Quarmby (2003).
[72] See eGovernment news – 14 July, 2005 – E.U. and Europe-wide – Identification & Authentication/Justice and Home Affairs, http://bit.ly/2FDfWSi.
[73] See http://bit.ly/2FJybsP.
[74] See Article 5 of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13/12 of 19 January 2000.
[75] See Government of the Grand Duchy of Luxembourg, Countdown to eIDAS, http://bit.ly/2FOlUmU.
[76] Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), OJ 257/73 of 28 August, 2014.
[77] European Commission, http://bit.ly/2p9FH5P.

rationale is that legal certainty on eID services will assist businesses and citizens to use digital interactions as their natural way of interaction.

Rather than introducing a pan-European ID card system, which would double the work for Member States, the eIDASR seeks to ensure that people and businesses can use their own national eIDs to access public services in other EU countries where eIDs are available. The goal is to create an European internal market for eTrust Services by ensuring that eIDs work across borders, and have the same legal status as traditional paper based processes.[78] Use cases include submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, setting up a business in another member state, authenticating internet payments, and bidding for tenders.

Prior to the adoption of the eIDASR many different national standards of eIDs, independent from coordinated EU policy, were developed within EU member states. Rather than harmonizing those standards, the eIDASR focuses on the technical interoperability of all existing eID standards. By mandating liability on member states as well as the eID provider for meeting certain identification obligations (including that the person identification data uniquely represents the person to which it is attributed and that online authentication is available)[79], the eIDASR creates trust in the eIDASR-based cross-border identification.

The eIDASR is a role model among the eID projects since it provides, in principle, an open standard not limited to EU jurisdictions. Every national ID system that is willing to connect to the eIDAS system could do so. Connecting to the eIDASR does not require a reform of national eID standards. Rather, by defining nodes (so-called eIDAS connectors) that provide the cross-border links between other countries' systems and one own's system any country could link to the eIDAS identification system in the EU/EEA, resulting – potentially – in a global eID network.

While adopted in 2014, the implementation of the eIDASR took some time, with public eID systems taking the lead. However, in November 2017 the first private sector-run national eID scheme was notified to the European Commission by Italy, connecting all eIDs created by that private enterprise to the European eID network. This enables Italian citizens and businesses to use their Italian eID credentials to access public services in other Member States.[80]

The eIDASR lays the foundation for a *service-oriented ID base*. The European Commission's Consumer Financial Services Action Plan,[81] aiming at "better products and more choice for European consumers", pledges to "work with the private sector to explore how they could use electronic identification and trust services for checking the identity of customers." Action Item 11 states: "The Commission will facilitate the cross-border use of electronic identification and know-your-customer portability based on eIDAS to enable banks to identify customers

[78] European Commission, http://bit.ly/2p9FH5P.
[79] See Article 11 of the eIDAS Regulation.
[80] European Commission, First private sector eID scheme pre-notified by Italy under eIDAS, 7 December 2017, http://bit.ly/2DmVQtV, online http://bit.ly/2DmVQtV.
[81] European Commission, *Consumer Financial Services Action Plan: Better Products, More Choice*, March 2017, online https://ec.europa.eu/info/publications/consumer-financial-services-action-plan_en (last access 20 June 2018). The Action Plan draws on previous work, such as a commissioned study asking for connection eIDAS and the consumer financial services sector, see CEPS/UCC/LIST, Study on the role of digitalisation and innovation in creating a true single market for retail financial services and insurance, 1 July 2016, online https://ec.europa.eu/info/publications/study-impact-digitalisation-eu-single-market-consumer-financial-services_en (accessed on 20 June 2018).

digitally." The Action Plan draws on the results of a commissioned study asking for better connecting eIDAS and the consumer financial services sector.[82]

In particular, by the facilitation of on-line relations with customers and establishing fully digital customer relationships, the Action Plan seeks to abolish offline "in office" identification and the need for handwritten signatures on contracts. The European Commission seeks to piggy-bag on new ways of identifying and authenticating customers, in order to further remote identification and tackle fraud issues. In the words of the European Commission,

> [t]he use of electronic identity schemes, as set out in eIDAS, would make it possible to open a bank account on-line while meeting the strong requirements for customer identity proofing and verification for know-your-customer or customer due diligence purposes. The legal certainty and validity of qualified eSignatures, as provided for under eIDAS, could also enhance the security of electronic transactions. This should work across borders and across sectors, and it should have the same legal effect as traditional paper based processes.[83]

The first steps in that direction have been undertaken by the European 4th Anti-Money Laundering Directive in accepting electronic identification systems under eIDAS as tools to meet customer due diligence requirements. As well as creating a common EU-wide identity repository for the public sector,[84] the European Commission encourages Member States to ensure that the schemes they are preparing for notification under eIDAS will also be available for the private sector. Further, the European Commission intends to open the Connecting Europe Facility subsidy scheme[85] for tests relating to the cross-border use of electronic identification by financial institutions. It will also introduce an implementation plan and information system architecture solutions with the objective of progressing towards an eBanking foundation that will meet all the requirements for remotely identifying bank customers.

4.4 Synthesizing the Lessons

Identity, and in particular digital identity, is potentially transformative in finance and the digital economy more broadly. This is a particular challenge in developing countries and emerging markets where often substantial proportions of the population lack any form of formal identification documents. At the same time, this shows where the greatest gains can be made, with the example of Aadhaar (the foundation of the India Stack infrastructure strategy) in India illustrating the potential, as well as a number of related challenges particularly in the context of data security and privacy. Likewise, the UN/Jordan experience of Iris Guard shows the potential for biometric digital identification systems to be implemented in the most challenging circumstances and – like Aadhaar – the transformative impact these can have.

---

[82] Cf. CEPS/UCC/LIST, Study on the role of digitalisation and innovation in creating a true single market for retail financial services and insurance, 1 July 2016, online https://ec.europa.eu/info/publications/study-impact-digitalisation-eu-single-market-consumer-financial-services_en (accessed on 20 June 2018).
[83] European Commission (March 2017).
[84] See European Commission, proposal for Regulation (…) on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), COM (2017) 794 final.
[85] The Connecting Europe Facility (CEF) is a key EU funding instrument to promote growth, jobs and competitiveness through targeted infrastructure investment at European level. It supports the development of high performing, sustainable and efficiently interconnected trans-European networks in the fields of transport, energy and digital services. CEF investments fill the missing links in Europe's energy, transport and digital backbone. See https://ec.europa.eu/inea/en/connecting-europe-facility (last access 20 June 2018).

4.4.1 e-ID vs Substitutes

While compromises between digital and physical services are necessary for progress, they do not represent the "end of history". Identification is important. In theory, it is the basis for any other digital-only activity. In practice, physical identification often substitutes for e-ID where e-ID is too complex, and once physical identification occurs, intermediary-made substitutes for identification such as PIN/TAN codes distributed to smart phones and fingerprint and iris scans reduce the importance of an efficient e-ID. Hence, e-ID can be bypassed at little cost.

Digital ID, however, is necessary if the subsequent parts of the digital financial ecosystem are to rest upon a solid foundation. The various other parts of the ecosystem that can be built upon such a foundation include four more elements: (1) sophisticated and advanced payments infrastructure, (2) streamlined account opening procedures, (3) an ecosystem that supports the payment of government benefits and other payments into accounts, and (4) a financial system that provides credit to individuals and SMEs on the basis of credit scores compiled from diverse and accurate data. We have explored this in detail elsewhere.[86]

[86] Arner, Buckley & Zetzsche (2018).

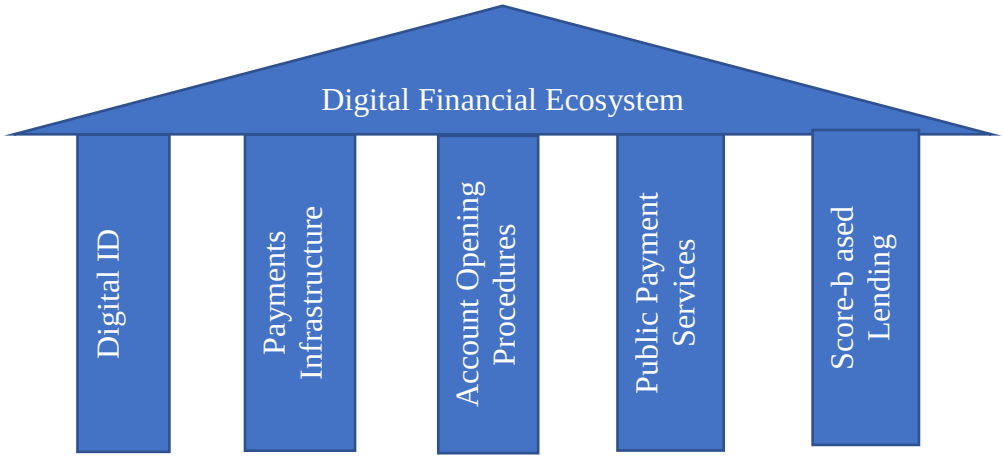

Figure 3: Elements of a Digital Financial Ecosystem

Such a comprehensive digital financial ecosystem will provide for many benefits. For instance besides the obvious ones – financial inclusion, enhanced service, greater choice to consumers and – if rightly designed – effective consumer and client protection[87], it will increase social welfare. For instance, it will transform government tax collection and thereby better fund government investments in education, health, roads and other infrastructure. Such an ecosystem will likewise transform the payment of government welfare and other benefits, dramatically reducing the losses in such payments due to corruption that bedevil many developing countries today. Such an ecosystem will also be able to allocate credit in such a way that SMEs, the principal employers of people in most countries, can thrive.

At the same time, such systems – while technically feasible – may not be politically feasible in many countries. In these cases, systems of optional digital identity separate from national / sovereign identification systems hold the greatest transformative potential, with the EU eIDAS Regulation showing one framework, and systems developed by Alibaba and Tencent in China representing other approaches.[88]

Many choices will have to be made in building such systems. For instance, additional information to be embedded for financial services providers into a customer's LEI or new smart ID card. These identifiers could include information on links to exposed political persons (1 = yes, 0 = no, plus country identifier) and the range of financial services deemed suitable for the entity (10 = all, 9 = complex derivatives to 0 = state bonds only). This data would be machine readable and determine which client relationships would be subject to additional checks. Once established, the receiving financial institution would tap into the KYC utility only to check whether new information is available; and these types of checks could also be fully automated, superseding manual processes. The information embedded in the transaction code will not always be collected by the same entity. For instance, the payment service provider that accepts the client's money for the first time within a jurisdiction may review the AML questions, while the first investment firm selling the client investment products may add information on suitability. As accountability is vital, records of who has added which information and when

[87] Arner, Buckley & Zetzsche (2018), at 7, 12, 17.
[88] For a comprehensive discussion see Arner, Buckley & Zetzsche (2018), at 13.

are essential, which, once again, suggests some form of blockchain system as a potentially suitable underlying architecture. For details on approaches, see infra at 5.3.

4.4.2 Base vs Business IDs

These ID systems are, from a sectorial perspective, neutral instruments**.** Financial services were not the centre of attention, nor was their necessity considered, when agreeing on standards and developing technologies. For instance, the European e-IDASR tackles the issue of ensuring that a person claiming an identity is the person they say they are, with a particular focus on cross-border identification. No further information is forwarded and certified than that necessary for identification. Examples of information that is not forwarded include whether the person is a politically exposed person under money laundering legislation, or whether the person is a sophisticated or non-sophisticated investor.

Further, the specific focus on identification (i.e. Base ID) may ignore the needs of businesses who are interested in immediate identification and authorization to link their clients to on-boarding systems. In some markets, this has led to additional (partially digital) solutions for online businesses, such as the online identification process whereby German, Luxembourg, and Swiss financial regulators allow an agent to check the identity of retail clients connected to them via a screen camera,[89] while corporate clients must have a LEI when entering into financial services contracts.[90]

4.4.3 Balancing the objectives

Different data are important for for different use cases. In fact, a sole Business ID may work well for sectorial use even if it provides less, or entirely different data than the Base ID. For instance, for financial services it is not relevant wether a client is born on 1 or 8 of July 1965, or whether the client was born in Malawi or Mosambik. At the same time, it is relevant that the identification features are unique and that data is stored through which the client can be identified and contacted today; for AML/CFT purposes business and private connections may also matter. The data points necessary for financial services may very well differ from those stored in the Base ID, and come from different sources (e.g. social media, shopping and telco platforms). At the same time, age and origin matter for health insurance (through genetic predisposition) as well as for travel (consider the origin-related issuance of passports in some countries).

This example demonstrates that for financial inclusion purposes only, we may start with a Business ID and remanufacture the Base ID one by one, with additional use cases being added over time. For that purpose a national/regional consensus of minimum requirements is necessary. For instance, the respective central banks / financial regulators could declare that fingerprints and iris scans together with network-related information on relatives, occupation, friends and land ownership (if any) suffice for low amount payment accounts in the lowest risk category. The data generated through this Business ID could then be linked via the central bank

[89] The technique was first introduced in 2015 and 2016 and clarified in later regulatory releases. See for Germany Bundesanstalt für Finanzdienstleistungsaufsicht, Circular 3/2017 (GW) - video identification procedures, Ref. GW 1-GW 2002-2009/0002, Date: 10 April 2017, online http://bit.ly/2x17fAS; for Luxembourg, CSSF, FAQ on AML/CTF and IT requirements for specific customer on-boarding/KYC methods, Version of 8 March 2018, http://bit.ly/2GlsP4M; for Switzerland see FINMA circular No. 2016/7 on video and online identification, 3 March 2016.

[90] See Article 26 of the Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (MiFIR).

/ financial regulator and/or the authority in charge of the Base ID. This would not only go a long way in bringing in the 1.7 billion unbanked individuals around the world into the financial system, it would also build a Base ID system over time that is in fact highly efficient and effective – and even more so if the same and additional data are linked to the Base ID authority in other sectors (e.g. payments to and from government, health registration cards etc.). It is however very important to learn one of the core lessons of Aadhaar: an identification system should not become a centralized storage location for disparate information. Rather, technology allows the interconnection of various pools of golden source data which are in fact stored and maintained separately: this is far more robust from the standpoint of both cybersecurity and data protection. An example can be seen in the systems being adopted in Australia or in the EU eIDASR.

Regardless of structure, it is central from the standpoint of building infrastructure to consider how base digital ID can extend to as much of the population as possible in order to maximize efficiencies in the context of other systems. Beyond individuals, similar systems can also be considered for corporates (for example based on the LEI system) and other types of entities, in particular as these interact with business registration and tax systems. As noted above, from the international standpoint, corporate ID based on LEI combined with CRS (Common Reporting Standards for tax information sharing) and benefitical ownership requirements may be far more politically acceptable than systems focusing on individuals (where privacy and security concerns arise much more readily than in the corporate context).

Such systems in turn can move beyond mere digital identification to proof of digital identity, particularly in the context of KYC requirements and related systems.

5 From Digital Identification to Digital Identity and KYC Hubs

5.1 Financial Law Prerequisites

Performing and verifying customer identity and carrying out Know Your Client ("KYC") due diligence, both on acceptance of a new customer (on-boarding) as well as on an ongoing basis are fundamental pre-requisites for the maintenance of market integrity.[91] In particular, customer identification and due diligence are essential tools in maintaining confidence and trust in the financial system and reducing the likelihood of criminal or terrorist access to financial services.[92] These are embodied in a wide range of AML/CFT/CDD requirements (anti-money laundering / countering the financing of terrorism / customer due diligence), based on internationally agreed approaches.[93] In addition, they are the basis of understanding customer needs and are essential to providing financial services in an appropriate manner, often coming under the umbrella of suitability and related KYC requirements.[94]

[91] See Financial Action Task Force (2018) p 8.
[92] See Basel Committee on Banking Supervision (2016).
[93] See FATF Recommendations online: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf; for Europe, see Article 10-29 of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73–1 ("4TH AMLD").
[94] See for Europe, Art. 25 of DIRECTIVE 2014/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, OJ L 173/249, 12.6.2014 ("MiFID II").

Base identity is essential in and of itself for many purposes, plus it also provides the fundamental element of the KYC process. Particularly when linked electronically with other golden source data (such as telephone, utility, tax and address information, usually collected for other independent purposes), it provides the basis of a simple eKYC system which can dramatically reduce costs in account opening while at the same time addressing concerns regarding market integrity (e.g. anti-money laundering – AML – and related considerations). The core objective is to make it as simple and inexpensive as possible for the vast majority of the public to open accounts, including SMEs. This should allow resources to instead be focused on higher risk customers, thereby not only supporting financial inclusion, but also better protecting market integrity. Such approaches also offer the potential to reduce the role of the shadow or underground economy, with potentially wide-ranging beneficial effects.

At the same time, however, these requirements also restrict access to financial services in some cases and therefore must be balanced against objectives of financial inclusion, overall customer experience, financial competitiveness and economic growth. Technology presents opportunities to reconsider existing systems and to build the infrastructure necessary to balance market integrity, financial inclusion and economic growth in order to support each, while at the same time meeting commitments to international financial standards including those set by the Basel Committee on Banking Supervision, FATF, FSB and United Nations Sustainable Development Goals.[95]

5.2 Towards KYC Hubs

As a result, in addition to systems of digital identification, an increasing range of eKYC and other digital identity systems are being developed to better achieve financial sector objectives.

Financial institutions, FinTech startups and technology firms engaging in financial services face a key challenge in the time-consuming and complex client on-boarding process required to meet CDD regulatory requirements. CDD data are also only useful if reliable, from a trustworthy source, and up-to-date. Financial institutions must spend a lot of time and resources refreshing and re-verifying their client information, making transactions expensive for institutions and inconvenient for clients. This is all the more inefficient if, as in the case of Luxembourg as a global hub for collective investment schemes that are distributed on a cross-border basis, the same client will often be checked by several Luxembourg entities more or less simultaneously and later ongoing when the client purchases units of different investment funds based in Luxembourg.

In addition, from the standpoint of the overall objective of protecting market integrity, data analytics from regulatory authorities and others are most effective when applied to comprehensive pools of data. As a result, not only are existing systems expensive, inefficient, and inconvenient, they are also often not overly effective in achieving the actual regulatory objective of preventing criminal or terrorist use of the financial system. In some cases, CDD requirements could even drive legitimate businesses and financial activities out of the formal financial system and into the informal financial system.[96]

[95] See references *supra*, at II. and III.

[96] For instance, in the context of much-needed remittances in the Pacific, see RL Stanley and RP Buckley, "Protecting the West, excluding the rest: The impact of the AML/CTF regime on financial inclusion in the Pacific, and potential responses" (2016) 17(1) *Melbourne Journal of International Law* 1.

A sector-wide e-ID KYC utility is a potential solution to these challenges and, unsurprisingly, the idea of a centralized KYC utility ("KYC Hubs") is gaining real traction globally.[97] This does not require standardizing e-ID, a task which will face insurmountable challenges in practice. Rather a network based on national identification system similar to the European eIDAS Regulation (supra, at 4.3), but focused on Business IDs is most suitable.

5.2.1 Private Service (South Africa)

One approach to KYC compliance, that does not rely upon digital biometric identification, has been taken in South Africa, where three major financial institutions and Thomson Reuters have partnered to create a central web-based database of KYC information, to be available to participating financial institutions free of charge. Essentially, the service collects the KYC information from the customer, verifies it once, and then distributes it to all of the customer's chosen institutions. Customers control who can access and view their information, and the UK data centers which support the database are subject to strict European Union data privacy laws. The centralized database avoids document duplication and streamlines account opening procedures for the customer at no cost.[98] The benefits of this system are not yet fully apparent as not all financial institutions have chosen to participate. Yet, as Samuel van Kiekerk of Standard Bank has said, it has "already delivered a win-win situation", as customers only need to provide their information once, and client-facing staff in banks no longer need to perform the task of information gathering.[99] As adoption levels increase, so should the efficiency benefits.

5.2.2 Public Service (India)

As another example, as part of India Stack, and based on the Aadhaar digital identity system discussed above, India has developed a paperless e-KYC service to instantly establish the identity of prospective banking customers. Provided customers expressly consent to their identity being made available by the e-KYC service, the service provides a non-repudiable proof of identity to service providers, including address, date of birth, gender, mobile number and email address. The India Stack e-signature layer also interacts with e-KYC.[100] This allows prospective banking customers to electronically sign contracts and other documentation without being physically present at a branch, and without any physical documentation. The digitization of identity authentication streamlines the account opening process for customers and allows all prospective customers who give their consent to easily access both digital and traditional financial services.[101]

Axis Bank was the first bank to offer an e-KYC account opening facility in late 2013. As its chief executive Shikha Sharma said simply at its launch: "Anybody can walk into a branch, give his finger prints and walk out with a bank account." This service reduced the turnaround

[97] LexisNexis, 2016, "Banks willing to collaborate on shared KYC utility," Finextra, September 28, http://bit.ly/2dyGiYp.

[98] *The South African KYC Service*, Thomson Reuters Africa, https://africa.thomsonreuters.com/en/products-services/risk-management-solutions/kyc-as-a-service.html.

[99] Sibongakonke Fumba, *Innovative KYC Compliance Sculpted in Africa*, Thomson Reuters (Nov. 14, 2017), https://blogs.thomsonreuters.com/financial-risk/know-your-customer/innovative-kyc-compliance-sculpted-in-africa/.

[100] Sasi Desai and Nipun Jasuja, *India Stack: The Bedrock of a Digital India*, Medium (Oct. 27, 2016), https://medium.com/wharton-fintech/the-bedrock-of-a-digital-india-3e96240b3718.

[101] At the time of writing, these sandboxes include AuthBridge, Digio, Aadhaar Bridge, eMudhra, OnGrid, Aadhaar API and Syntizen Technologies: see *About EKYC API*, IndiaStack, http://indiastack.org/ekyc/.

time for opening a bank account from 7 – 10 days to just one day.[102] Today, many traditional banks in India offer bank accounts which can be opened and used instantly using e-KYC authentication, including savings and everyday accounts.[103]

The system is also utilized by licensed payments banks, of which there are two currently in full operation, PayTM and Airtel Payments Bank.

PayTM is an e-wallet provider which has really struggled, as its business has scaled, to comply with the KYC requirements imposed by the Reserve Bank of India. However, since the implementation of Aadhaar, 87 percent of PayTM's KYC checks have come to rely on the e-KYC system. In order to upgrade customers' accounts to the highest value wallet, agents can now go into the field with biometric devices to instantly authenticate the identity of customers, and then instantly upgrade their wallet.[104] Customers are not required to attend at a branch or provide any physical documentation.

Airtel has also had difficulties, centering more on whether they have properly obtained express customer consent before using e-KYC information to open accounts. UIDAI recently barred Airtel from conducting SIM identity verification of payments bank clients using Aadhaar-based e-KYC because it had opened payments bank accounts without obtaining "informed" customer consent. Airtel's payments bank had been verifying its KYC information using Airtel's own telecom business. In response, on 20 February 2018, the Reserve Bank of India issued a new directive on KYC norms for payments banks requiring verification of KYC information by third parties,[105] and CEO Shashi Arora has resigned over the issue.

India Post Payments Bank is becoming India's third full-fledged payments bank as it is rolled out nationwide from April 2018 onwards. It is expected to become the largest network promoting financial inclusion in the country, providing digital payment services to both rural and urban areas, and using e-KYC to ease account opening procedures.[106]

5.3 Designing eKYC Infrastructure

5.3.1 From simple to complex

The costs savings expected from eKYC are greatest when most financial institutions participate. This statement is unlimited, in geographic terms. From an efficiency perspective, therefore, the probably politically unachievable optimum would be one global KYC utility with a full, up-to-date register of all clients within the regulated banking system.

---

[102] *Axis Bank Introduces a Paperless, eKYC Based A/c Opening*, India Infoline News Service, https://www.indiainfoline.com/article/news/axis-5875391291_1.html.

[103] For example, AXIS Bank (https://www.axisbank.com/accounts/savings-account/axis-asap/axis_ASAP.html); RBL Bank (https://abacus.rblbank.com/); and HDFC Bank (https://www.hdfcbank.com/htdocs/digital-campaign/instantaccounts.html).

[104] *See How PayTM Is Using Aadhaar EKYC to Upgrade Their Wallet Customers*, IndiaStack (Dec. 14, 2016), http://indiastack.org/see-paytm-using-aadhaar-ekyc-upgrade-wallet-customers/.

[105] Amrit Raj, *RBI Issues New KYC Norms for Payments Banks*, Live Mint (Feb. 21, 2018), https://www.livemint.com/Industry/lMRk8xGt0uMzMGvkhGWRVL/RBI-issues-new-KYC-norms-for-payments-banks.html.

[106] ET Bureau, *India Post Payments Bank Will Begin Nationwide Rollout in April*, The Economic Times (Feb. 10, 2018), https://economictimes.indiatimes.com/industry/banking/finance/banking/indian-post-payments-bank-will-begin-nationwide-rollout-in-april/articleshow/62861636.cms.

Small improvements in this field can yield significant benefits. For instance, assume five entities each invest 3 staff hours in on-boarding the same client. If a KYC utility is (in addition to the one-time technical set-up costs) able to reduce the needed efforts to 3 hours invested by only one entity, the overall cost savings approach 80%. With ten members; putting the cost of the technology aside, the cost saving would be 90% if a customer deals with all ten entities, 10% greater than those of the utility with five members. That additional 10% will be partially offset by the additional costs of coordinating the additional five members. The calculated savings materialize only when participating institutions serve the same client. If we assume that all participants serve the same number of clients, the likelihood that this will be the case increases with the number of participants in the KYC utility. In other words, under these conditions, the larger the utility in terms of members, the greater the efficiency gains. Nevertheless, agreeing on governance features and standards is far easier with fewer rather than more members, and so transaction costs may be a good reason to start small and grow over time.

Many issues will need to be addressed in building a KYC utility. Some sample questions include:

1. **Which technological platform?** A centralized ledger or a distributed ledger?[107] Ensuring simultaneous access is the strongest argument in favor of using distributed ledgers, while data privacy, governance concerns and technical complexity may tip the tide in the direction of more concentrated ledgers.[108] If a distributed ledger is chosen, the next question will be public or permissioned, although this admits of an easier answer as it is very difficult to see the need for a public ledger. These are of course not exclusive: best practice today may suggest centralized stores for individual forms of golden source data but a decentralized structure linking these together – so that for instance you only have to change your address once and it is immediately confirmed for all other linked systems. It is thus important to understand at the outset the technological options – and not assume any particular structure.

2. **Who shall participate and how?** Answers will depend on the sophistication of technology required for participation, access to hyper-fast data streams, and reliability when performing CDD.

3. **What type of information will be shared?** Options include the synthesized result (i.e., "client is clean: yes/no") or variants of additional information on the client. The answer to the responsibility question raised below will be influential in determining how much information will be shared.

4. **How often will the information be updated, and by whom?** Options range from centralized data maintenance to member-based maintenance. The answer will depend on the answers to question 2. The more reliable the members, the more acceptable is member-based data maintenance. At the same time, there may still need to be some sort of golden source certification for data that are declaratory in nature, for instance as is often the case in company registries.

[107] See on distributed ledgers Zetzsche D A, Buckley R P, and Arner D W, 2017, "The distributed liability of distributed ledgers: legal risks of blockchain," University of Illinois Law Review, 2017-2018, Forthcoming; Available at SSRN: https://ssrn.com/abstract=3018214 or http://dx.doi.org/10.2139/ssrn.3018214.
[108] See idem.

5. **How will liability be shared if, and when, things go wrong?** Options range from locating liability in one entity to joint liability. Again, this answer depends on that to question 2. The more reliable and financially stable the members, the more acceptable is joint liability. If only the largest institutions underwrite to the KYC utility, the argument for joint liability lies in incentivizing all members to invest in the maintenance and further development of the utility (precisely as stock exchange participants, by virtue of joint liability, are incentivized to maintain the AAA-rating of the central counterparty since its AAA rating reduces the costs of all trading partners).

6. **Which standards will be used for data sharing?** Options include an open standard or a standard designed specifically for participants.

Legal factors may influence complexity. For instance, regulated entities are easier to include than non-regulated ones, individuals raise different questions than legal entities, and foreign financial institutions are more difficult to integrate than domestic ones, in particular foreign institutions from jurisdictions with different legal systems.

A sector-wide eKYC solution might best first aim at digital identification of domestic licensed financial intermediaries, then be extended to locally incorporated companies (relying on LEIs) and subsequently be used for non-face-to-face on-boarding of individuals. Internationalization, including foreign institutions, is perhaps the final step to be tackled.

5.3.2 Responsibility

One issue facing the one-stop-shop concept for eKYC, including CDD and other financial services information, is who should be responsible for compliance. While financial institutions may rely upon an intermediary to perform any part of the CDD process, the ultimate responsibility for ensuring CDD requirements are met remains with the financial institution.[109] If a financial institution relies on CDDs performed by other intermediaries, the *respective rules of each jurisdiction are burdensome*. For instance, Article 27 of the European AML Directive requires that when financial institutions rely upon information from a third party for meeting any part of the CDD requirements, the financial institution take "adequate steps to ensure that the third party provides, immediately, upon request, relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner."

However, the restrictions are somewhat loosened, by one AML CDD being able to serve many banks, if a particular amount enters a bank account and then only circulates within a regulated banking system where all participants are subject to the same AML rules. *Example*: Money enters the EU banking system from a bank account in the Cayman Islands. The first EU bank needs to apply full CDD. In the absence of new information, banks that receive payments from that first EU bank can categorize those transactions as "low risk", i.e., they can in principle trust that the CDD applied by the first E.U. bank led to accurate results, and that the money is "clean".[110] The same logic could be utilized for a sector-wide KYC utility. This logic only works in closed systems, from which money or assets cannot leak in or out.

[109] See, for instance, Article 25 (1) of the European 4th AML Directive (above n 13).
[110] See Joint Committee of the European Supervisory Authorities, Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk

5.3.3 Governance

Governance is key. This is true for any company, and particularly true for a KYC utility. Because knowledge means power, concentrating knowledge concentrates power. Take for instance, Luxembourg, which is the largest global distribution center for investment funds, with its funds offered in more than 70 countries around the world.[111] A sector-wide AML/KYC tool that truly covered all client relationships would provide enormous synergies, but also pose new risks for clients globally. At the same time, an interlinked system of golden source company data from certified jurisdictions around the world based on LEIs would be of immense benefit to all legitimate interests but without the risks of centralizing data in any single location.

How to address these risks requires careful thinking that takes into account legal factors (such as property rights, liability, competition and antitrust concerns, and also applicable data privacy rules, such as GDPR)[112] together with non-legal factors (such as the technology used – with blockchain a natural candidate)[113], the cyber-security risks incurred, and the need to build a networked infrastructure to which hundreds, if not thousands, of entities can be linked.

From a governance perspective, the following legal questions are of particular importance, all of course premised on the technological and other choices highlighted in the preceding paragraphs:

1. Should the KYC utility be a *public or private enterprise*? A public enterprise offers public risk control, but probably also public tardiness, while a private enterprise may provide less of a long-term sustainability solution. If a private entity is providing the service, given its social welfare function it should be licensed and regulated.

2. Should the KYC utility be a *for-profit entity or an association* acting on behalf of its members? The answer will depend in part on how the utility is to be financed. User fees could provide ongoing maintenance costs, but up-front costs will be substantial. Given the utility will function as a monopoly, a for-profit entity with closed membership will prompt antitrust concerns (which is another reason for regulating it).

3. Who should run the *day-to-day business of the utility*? This may include decisions on technical standards and the further development of the utility in light of changing technical and legal conditions.

4. Shall the users or members have *participation rights, and if so, how*? Those with the greatest interest in the functioning of the utility may well have the greatest say. Voting rights could be assigned by (1) how often a member updates KYC data (if any), (2) how often a member requests KYC data, (3) a mix of the two, or (4) how much liability for the utility a member bears.

5. Who decides upon *membership applications*? The decision could be granted to an expert committee, the KYC utility's board (if any), the membership assembly, or a state institution

associated with individual business relationships and occasional transactions - The Risk Factors Guidelines -, JC 2017/37 of 26 June 2017, at Title III, Ch. 1 (Sectoral guidelines for correspondent banks), No. 81, 83.

[111] See ALFI, 2018, "Global fund distribution," http://bit.ly/2pagnwC.

[112] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), O.J. L119/1 of 4 May 2016.

[113] Zetzsche, Buckley and Arner (2017).

(such as the financial regulator). Given that the reliability of members affects the utility, and the utility's financial capacity influences all members' costs, a multi-step approach requiring the recommendation of an expert committee before membership being approved could be a good process.

While research into how to set up a KYC utility is in its infancy, we believe that such utilities, to a large extent, pose similar questions to stock exchanges in the 19th century, since both are set up to reduce the costs of information asymmetries, and both entail a degree of influence on market participants. The different rules for stock exchanges around the world suggest that a one-size-fits-all answer to the questions above is impossible, and that every jurisdiction interested in KYC utilities must answer these questions for itself in light of its traditions, legal structure, and the risks its members are willing to assume.

6 Conclusion: Addressing the Identity Problem in Finance

In addressing the identity problem in finance, this paper identified and considered two different aspects which must be addressed strategically. These are (1) Digital ID infrastructure, and (2) eKYC infrastructure.

Across both aspects, the paper considered two different contexts that must be addressed as part of the strategy: (1) individuals; and (2) entities (especially companies). Within these two contexts, the strategy must also address: (1) local; and (2) non-local individuals and entities, and also (1) physically present; and (2) non-physically present individuals and entities. In each case, infrastructure and utilities could be built by the government, the private sector, or by way collaboration.

Likewise, in each case, systems and utilities could be exclusive (for example, sovereign identity sources from sovereigns) or open (for example, a system of licensing for competitive providers), or something in between (for example, a licensed single provider).

This matrix lays out the central elements of a digital ID / eKYC strategy for putting in place the necessary financial infrastructure to meet objectives of financial integrity, financial inclusion, and financial competitiveness. It then proposed a three-part framework covering best practices, design and governance aspects of eKYC utilities. Over time, such systems could potentially be extended to suitability and other functions as well.

While primarily intended to benefit national policymakers and regulators, this research also should assist industry players. Both of these stakeholders can benefit from efficiency gains, whether in the form of compliance cost reductions, an increase in industry competition, or an improved user experience provided by this new online infrastructure. Customers, and the economy more broadly, should both likewise gain. Over time a network of national eKYC utilities could increase speed and service level in financial services. Standardising e-IDs beyond the level already achieved by FATF measures and work of international bodies such as IOSCO and the FSB is not a functional precondition; rather a network approach similar to the EU's eIDAS Regulation, but with a focus on Business IDs could better achieve FATF objectives while at the same time enhancing efficieny and reducing costs for participants. This is the fundamental promise of RegTech: designing systems which are capable of achieving regulatory objectives better than existing systems while at the same time increasing efficiencies and reducing costs for market participants.

While no single solution will address all the various issues identified, jurisdictions can nonetheless develop a strategic approach based on a clear understanding of existing regulation and infrastructure, international requirements, and the potential of solutions from both a technological and regulatory standpoint to address objectives, problems, and challenges. Any such strategic approach must be structured according to the needs and individual characteristics of each jurisdiction. Three steps are of particular importance.

First, where an economy is implementing new digital identification solutions (such as a new smart national ID card for individual digital identification purposes, or the LEI required under MiFID for financial transactions), it is advisable to think further ahead and link such identity devices to AML/KYC checks, by ensuring that complementary technology is implemented on the side of users and that sufficient data points exist in the storage devices (in the case of LEI, this could mean that the number for the LEI is larger to include AML/KYC scores). The same is true if, as is desirable for financial inclusion purposes in countries without a comprehensive Base ID system, regulation focuses first on Business IDs and remanufactures Base IDs from the former, particulary through networking existing golden data sources.

Second, 100 percent digital identification and eKYC coverage is neither feasible nor likely in the short term and aiming at 100 percent coverage from the beginning will either increase the risk of disruption or delay any synergies from sector-wide eKYC systems for the foreseeable future. Thus, complexity should shape which steps are taken and in which order. For instance, complexity tends to be higher on a cross-border basis and lesser on a domestic basis, and it is more difficult to include non-regulated entities than regulated ones that regularly use financial services. A sector-wide eKYC solution could first aim at digital identification of licensed domestic financial intermediaries, then include locally incorporated companies (relying on LEIs) and then next be utilized for non-face-to-face on-boarding of individuals and finally address the challenges posed by foreign institutions.

Third, from the beginning, a great deal of attention needs be given to the governance of the sector-wide eKYC tool. Knowledge is power, and the more knowledge, the more power. In particular, in global financial centers, a sector-wide AML/KYC tool that covers all client relationships will provide enormous synergies, but also pose new risks. How these risks might best be addressed requires careful thinking that takes into account legal factors (such as property rights, liability, competition, and antitrust concerns, and also applicable data privacy rules) and non-legal factors such as the technology used (with blockchain being a natural candidate), the cyber-security risks incurred, and the need to ensure the further technological evolution of a networked infrastructure to which thousands of entities may need to be linked.

More importantly, to focus on only identification, and ignore sector-specific needs and use cases, misses many of the potential opportunities an eKYC system could provide. In an ideal digital financial services world, identification would not only proceed smoothly, but every step necessary for client-onboarding and back-up checks would be done simultaneously, and only once per client for all kinds of services and intermediaries. Only when this is achieved will financial intermediaries benefit from the full potential of a sector-wide eKYC system.

Reference List

Aadhaar data update. Unique Identification Authority of India. https://uidai.gov.in/enrolment-update/aadhaar-enrolment/aadhaar-data-update.html.

About Aadhaar. Unique Identification Authority of India. https://uidai.gov.in/your-aadhaar.html.

About eKYC API. IndiaStack. http://indiastack.org/ekyc/.

Abraham S, Sharma RS, Panda BJ (2017) Is Aadhar a breach of privacy? The Hindu, 31 March 2017. https://www.thehindu.com/opinion/op-ed/is-aadhaar-a-breach-of-privacy/article17745615.ece.

Arner DW, Zetzsche DA, Buckley RP (2018) Fintech for financial inclusion: designing infrastructure for financial transformation – A Report to the Alliance for Financial Inclusion. https://www.afi-global.org/sites/default/files/publications/2018-09/AFI_FinTech_Special%20Report_AW_digital.pdf

Arner DW, Barberis J, Buckley RP (2016) The evolution of FinTech: a new post-crisis paradigm? Georgetown Journal of International Law 47(4).

Arner DW, Barberis J, Buckley RP (2017) FinTech, RegTech and the reconceptualisation of financial regulation. Northwestern journal of international law and business 37: 371-414.

Asian Development Bank (2016) Global trade finance gap reaches $1.6 trillion, SMEs hardest hit. Asian development bank news release. 7 September 2016.

Association of the Luxembourg Fund Industry (2018) Global fund distribution. http://www.alfi.lu/sites/alfi.lu/files/Poster-GFD-2018-web-BAT.pdf.

Australian Government Govpass. Digital Transformation Agency, Canberra. https://www.dta.gov.au/what-we-do/platforms/govpass/.

Australian Government (2015) Improving Australia's financial system. Department of Treasury, Canberra. https://static.treasury.gov.au/uploads/sites/1/2017/06/Government_response_to_FSI_2015.pdf.

Axis Bank introduces a paperless, eKYC based a/c opening. India Infoline News Service, 26 February 2014. https://www.indiainfoline.com/article/news/axis-5875391291_1.html.

BaFin Federal Financial Supervisory Authority (2017) Circular 3/2017 video identification procedures. 10 April 2017. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html.

Basel Committee on Banking Supervision (2016) Guidelines: Sound management of risks related to money laundering and financing of terrorism. February 2016. https://www.bis.org/bcbs/publ/d353.pdf.

Benedictus L (2006) A brief history of the passport. The Guardian, 18 November 2006. https://www.theguardian.com/travel/2006/nov/17/travelnews. Accessed 5 July 2018.

Bracken M (2012) Identity and privacy principles. UK Government Digital Service, 24 April 2012. https://gds.blog.gov.uk/2012/04/24/identityand-privacy-principles/. Accessed 5 July 2018.

Carse D (2000) Future of banking in Hong Kong – The impact and implications of internet banking. Hong Kong. https://www.hkma.gov.hk/eng/key-information/speeches/2000/.

Clippinger JH (2015) A proof of concept pilot for a decentralized autonomous authority (DAA) for KYC compliant decentralized identity and authentication services. MIT media lab. http://financelawpolicy.umich.edu/wp-content/uploads/sites/26/2016/09/Clippinger-A-Proof-of-Concept-Pilot-for-A-Decentralized-Autonomous-Authority4.1.16.pdf.

COAG (2017) Intergovernmental agreement on identity matching services. 5 October 2017. http://bit.ly/2p5g5YO.

Commission de Surveillance du Secteur Financier (2018) Frequently asked questions on AML/CTF and IT requirements for specific customer on-boarding/KYC methods. http://www.cssf.lu/fileadmin/files/LBC_FT/FAQ_LBCFT_VIDEO_IDENTIFICATION_080318.pdf.

Council of Australian Governments (2017) Intergovernmental agreement on identity matching services. 5 October 2017. https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf.

Desai A, Jasuja N (2016) India stack: the bedrock of a digital India. Medium, 27 October 2016. https://medium.com/wharton-fintech/the-bedrock-of-a-digital-india-3e96240b3718.

Donnelly G (2017) 74 super useful facebook statistics for 2017. Wordstream, 7 November 2017. https://www.wordstream.com/blog/ws/2017/11/07/facebook-statistics. Accessed 5 July 2018.

ETBureau (2018) India post payments bank will begin nationwide rollout in April. The Economic Times, 10 February 2018. https://economictimes.indiatimes.com/industry/banking/finance/banking/indian-post-payments-bank-will-begin-nationwide-rollout-in-april/articleshow/62861636.cms.

European Commission Connecting Europe Facility. https://ec.europa.eu/inea/en/connecting-europe-facility.

European Commission Framework for interoperability between EU information systems (police & judicial cooperation, asylum & migration). https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-794_en.

European Commission (2016) Study on the impact of digitalisation on the EU single market for consumer financial services. 1 July 2016. https://ec.europa.eu/info/publications/study-impact-digitalisation-eu-single-market-consumer-financial-services_en. Accessed 20 June 2018.

European Commission (2017) Consumer financial services action plan. 23 March 2017. https://ec.europa.eu/info/publications/study-impact-digitalisation-eu-single-market-consumer-financial-services_en. Accessed 20 June 2018.

European Commission (2017) First private sector eID scheme pre-notified by Italy under eIDAS. 7 December 2017. https://ec.europa.eu/digital-single-market/en/news/first-private-sector-eid-scheme-pre-notified-italy-under-eidas. Accessed 20 June 2018.

European Parliament (1999) Directive 1999/93 on a community framework for electronic signatures OJ L 13/12.

European Parliament (2014) Directive 910/2014 on electronic identification and trust services for electronic transactions in the internal market OJ 257/73.

European Parliament (2014) Directive 2014/65 on markets in financial instruments OJ L 173.

European Parliament (2015) Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing OJ L 141.

European Parliament (2016) Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC OJ L 119/1.

Financial Action Task Force Who we are. http://www.fatf-gafi.org/about/.

Financial Action Task Force (2018) Outcomes FATF plenary, 21-23 February 2018. 23 February 2018. http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-february-2018.html.

Financial Action Task Force (2012) International standards on combating money laundering and the financing of terrorism & proliferation. February 2012. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

Financial Stability Board (2017) Financial stability implications from FinTech: supervisory and regulatory issues that merit authorities' attention. 27 June 2017. http://www.fsb.org/wp-content/uploads/R270617.pdf.

Fumba S (2017) Innovative KYC compliance sculpted in Africa. Inside Financial & Risk, 14 November 2017. https://blogs.thomsonreuters.com/financial-risk/risk-management-and-compliance/innovative-kyc-compliance-sculpted-in-africa/.

Global Partnership for Financial Inclusion (2016) Updated G20 financial inclusion indicators focus on digital financial services. 10 August 2016. https://www.gpfi.org/news/updated-g20-financial-inclusion-indicators-focus-digital-financial-services.

Global Partnership for Financial Inclusion (2017) G20 financial inclusion action plan (FIAP) 2017. July 2017.

Government of the Grand Duchy of Luxembourg (2016) Countdown to eIDAS. 19 April 2016. https://www.isaca.org/chapters2/Luxembourg/Documents/201604%20AGM/eIDAS_ISACA_v1_PUBLIC.pdf.

Hardjono T, Shrier D, Pentland A (2016) Trust::Data: A new framework for identity and data sharing. Visionary Future LLC, Massachusetts.

Hong Kong Monetary Authority (2016) De-risking and financial inclusion. 8 September 2016. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160908e1.pdf. Accessed 2 July 2018.

IDABC (2005) European e-Government news roundup. http://ec.europa.eu/idabc/servlets/Docd548.pdf?id=21269.

Indian business prepares to tap into Aadhaar, a state-owned fingerprint identification system. The Economist, 24 December 2016.

International Bar Association Legal Practice Division Working Group (2015) Digital identity: principles on collection and use of information. https://www.ibanet.org/Document/Default.aspx?DocumentUid=2E931F85-C5D0-4952-A6E6-6EA48C593155.

International Finance Corporation (2016) De-risking by banks in emerging markets – effects and responses for trade. November 2016. https://www.ifc.org/wps/wcm/connect/3dc1cc57-2ab3-4eab-8018-f93203d5a00b/EMCompass+Note+24+De-risking+and+Trade+Finance+11-15+FINAL.pdf?MOD=AJPERES. Accessed 28 July 2018.

International Finance Corporation (2017) De-risking and other challenges in the emerging market financial sector. 1 September 2017. http://documents.worldbank.org/curated/en/895821510730571841/De-risking-and-other-challenges-in-the-emerging-market-financial-sector-findings-from-IFC-s-survey-on-correspondent-banking. Accessed 28 July 2018.

International Finance Corporation (2018) Increased regulation and de-risking impeding cross-border financing in emerging markets. January 2018. https://www.ifc.org/wps/wcm/connect/9e5b33c0-63a2-4ab4-bf54-b87c539538d4/EMCompass_Note_48_R2.pdf?MOD=AJPERES.%20Accessed%2028%20Jul%202018. Accessed 28 July 2018.

Joint Committee of the European Supervisory Authorities (2017) Joint guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions. European Banking Authorities, 26 June 2017. https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf.

Kirova M (2016) eIDAS regulation. eIDAS observatory, 28 June 2016. https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014.

Klosters D (2018) Digital identity: on the threshold of a digital identity revolution. World Economic Forum White Paper, January 2018. http://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf.

Kulp P (2017) Facebook quietly admits to as many as 270 million fake or clone accounts. Mashable, 3 November 2017. https://mashable.com/2017/11/02/facebook-phony-accounts-admission/#3Jg1dt85kPqZ.

Kumar L, Pathak A (2014) Aadhar based e-KYC service – the much needed change catalyst for financial inclusion! MicroSave, July 2014. http://blog.microsave.net/aadhaar-based-e-kyc-service-the-much-needed-change-catalyst-for-financial-inclusion/. Accessed 5 July 2018.

Lanier J (2014) Who owns the future? Simon & Schuster, New York.

Legislative Council of Hong Kong (1989) Drug trafficking (recovery of proceeds) ordinance cap.405.

Legislative Council of Hong Kong (1994) Organized and serious crime ordinance cap.455.

Legislative Council of Hong Kong (2002) United Nations (anti-terrorism measures) ordinance cap.575.

Legislative Council of Hong Kong (2011) Anti-money laundering and counter-terrorist financing (financial institutions) ordinance cap.615.

LexisNexis (2016) Banks willing to collaborate on shared KYC utility. Finextra, 28 September 2016. https://www.finextra.com/pressarticle/66294/banks-willing-to-collaborate-on-shared-kyc-utility.

Litan A (2016) The global identity dilemma – static biometrics are not the answer. Gartner Blog Network, 16 September 2016. https://blogs.gartner.com/avivah-litan/2016/09/16/the-global-identity-dilemma-static-biometrics-are-not-the-answer/. Accessed 2 July 2018.

Live Law News Network (2018) SC constitution bench to begin final hearing on validity of Aadhaar cards tomorrow. Live Law, 16 January 2018. https://www.livelaw.in/sc-constitution-bench-begin-final-hearing-validity-aadhaar-cards-tomorrow/.

Monetary Authority of Singapore Notices and guidelines. http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism/Notices-and-Guidelines.aspx?sc_q=all%20financial%20institutions&sc_type=Filter%20by%20category&sc_p=1.

Morozov E (2013) Your social networking credit score. Slate, 30 January 2013. Accessed 5 July 2018.

Noto G (2017) Want mobile banking users? Eliminate the login. Bank Innovation, 30 March 2017. Accessed 5 July 2018.

Parliament of Australia (2006) Anti-money laundering and counter-terrorism financing act Act.169/2006.

Parliament of Australia (2018) Review of the identity-matching services bill 2018 and the Australian passports amendment (identity-matching services) bill 2018.

https://www.aph.gov.au/Parliamentary_Business/CommitteesJoint/Intelligence_and_Security/IMSBill.

Parliament of Australia (2018) Identity matching services bill (cth).

Pesin I (2017) Your online, mobile, and social behaviour are now data-points used by fintech startups and governments in scoring credit-worthiness. E27, 4 May 2017. https://e27.co/online-mobile-social-behaviour-now-data-points-used-fintech-startups-governments-scoring-credit-worthiness-20170504/. Accessed 5 July 2018.

Prakash P (2015) Your Facebook page or your credit score: What's more important for getting a loan? Fitsmallbusiness, 4 September 2015. https://fitsmallbusiness.com/facebook-credit-score/ . Accessed 5 July 2018.

Puttaswamy (Retd.) & Anor v Union of India & Ors (Civil) No 494 of 2012.

Quarmby B (2003) The case for national identification cards. Duke Law and Technology Review 1, 1-10.

Raj A (2018) RBI issues new KYC norms for payment banks. LiveMint, 21 February 2018. https://www.livemint.com/Industry/lMRk8xGt0uMzMGvkhGWRVL/RBI-issues-new-KYC-norms-for-payments-banks.html.

Reuters (2018) US proposes reviewing social media of nearly everyone seeking entry. The Guardian, 31 March 2018. https://www.theguardian.com/us-news/2018/mar/30/us-immigration-social-media-visas.

Rizzo P (2014) Why 20 Bitcoin companies are backing a new deal for digital identity. Coindesk, 20 October 2014. https://www.coindesk.com/20-bitcoin-companies-backing-new-deal-digital-identity/.

Schwab K (2016) The fourth industrial revolution. World Economic Forum, Geneva.

See how paytm is using Aadhaar eKYC to upgrade their wallet customers. IndiaStack, 14 December 2016. http://indiastack.org/see-paytm-using-aadhaar-ekyc-upgrade-wallet-customers/.

Smith C (2017) 65 amazing WhatsApp statistics and facts. Expanded Ramblings, 1 July 2017. https://expandedramblings.com/index.php/whatsapp-statistics/2/. Accessed 5 July 2018.

The South African KYC Service. ThomsonReuters. https://africa.thomsonreuters.com/en/products-services/risk-management-solutions/kyc-as-a-service.html.

Stanley RL, Buckley RP (2016) Protecting the West, excluding the rest: the impact of the AML/CTF regime on financial inclusion in the Pacific, and potential responses. Melbourne Journal of International Law 17(1) 1.

Todd S (2014) Manifesto vows to give consumers control of digital identities. American Banker, 20 October 2014. https://www.americanbanker.com/news/manifesto-vows-to-give-consumers-control-of-digital-identities.

UK Parliament, Identity documents bill. https://publications.parliament.uk/pa/cm201011/cmbills/001/2011001.pdf.

United Nations Capital Development Fund. Financial inclusion and the SDGs. http://www.uncdf.org/financial-inclusion-and-the-sdgs.

Weigend A (2017) Data for the people. Ingram Publisher Services, Pennsylvania.

The windhover principles for digital identity, trust, and data. Token Commons, 21 September 2014. http://tokencommons.org/Windhover-Principles-for-Digital-Identity-Trust-Data.html.

World Bank (2018a) Principles of identification for sustainable development: toward the digital age. http://documents.worldbank.org/curated/en/213581486378184357/ pdf/112614-WP-REVISED-PUBLIC.pdf. Accessed 28 July 2018.

World Bank (2018b) The decline in access to correspondent banking services in emerging markets: trends, impacts, and solutions. http://documents.worldbank.org/curated/en/552411525105603327/pdf/125422-replacement.pdf. Accessed 28 July 2018.

Zetzsche DA, Buckley RP, Arner DW, Barberis JN (2018) From fintech to techfin: The regulatory challenges of data-driven finance. New York University Journal of Law & Business 14(2) 393. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959925.

Zetzsche DA, Buckley RP, Arner DW (2017) The distributed liability of distributed ledgers: legal risks of blockchain. European Banking Institute Working Paper series 14.

Address

European Banking Institute eV.

Mainzer Landstrasse 251

60326 Frankfurt am Main

Germany

For further information please visit our website www,ebi-europa.eu or contact us at info@ebi-europa.eu

www.ebi-europa.eu

The European academic joint venture for research in banking regulation

www.ebi-europa.eu