CAPCO

JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

SECURITY

Digital ID and AML/CDD/KYC utilities for financial inclusion, integrity and competition

DIRK A. ZETZSCHE | DOUGLAS W. ARNER
ROSS P. BUCKLEY

DIGITIZATION

#47
04.2018

JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

ORGANIZATION

CURRENCY

SECURITY

Digital ID and AML/CDD/KYC utilities for financial inclusion, integrity, and competition

DIRK A. ZETZSCHE | Professor of Law, ADA Chair in Financial Law (Inclusive Finance), Faculty of Law, Economics and Finance, University of Luxembourg, and Director, Center for Business and Corporate Law, Heinrich-Heine-University, Düsseldorf, Germany

DOUGLAS W. ARNER | Kerry Holdings Professor in Law, University of Hong Kong

ROSS P. BUCKLEY | King & Wood Mallesons Chair of International Financial Law, Scientia Professor, and Member, Centre for Law, Markets and Regulation, UNSW Sydney

ABSTRACT

Customer identification is key to protecting market integrity. The know your customer, anti-money laundering, and counter-terrorism financing rules all work to this end. However, these strict rules can limit access to financial services, particularly by small and medium enterprises and poorer individuals. Global interest in e-identity is growing, with multiple countries either establishing, or having already established, national e-identity systems. The potential of centralized identity databases to simplify the experience of accessing both government and financial services is clear. Efficient e-identity services also hold great potential for international financial centers. This article sets out three measures to which such centers must pay particular attention in building their e-identity systems.

1. THE CHALLENGE OF E-ID: SQUARING THE CIRCLE

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.[1] From the standpoint of an international financial center (such as Hong Kong, Luxembourg, or London), competitiveness derives from balancing these objectives and providing the necessary infrastructure for financial markets to function well.

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),[2] based on internationally agreed approaches.[3] 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.[4]

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 and innovation, and reducing, or in some cases eliminating, their access to finance has important consequences for growth, innovation, and development. In addition, financial institutions, corporates, and individuals in emerging and developing markets (such as most of Asia) are often seen as "high risk" and hence subject to "de-risking," particularly by financial institutions from Western developed markets.[5] This issue has become sufficiently significant to be the focus of the G20, the Basel Committee, and 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 (particularly Asia) and their customers.[6]

Beyond SMEs and correspondent banking, the G20 (particularly through its focus on digitally inclusive finance)[7] and the United Nations (U.N.) (in particular through the U.N.'s Sustainable Development Goals)[8] 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 in rural and urban areas. 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.

Financial technology (fintech),[9] and in particular "regulatory technology" (regtech),[10] 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

---

1 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.

2 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).

3 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.

4 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.

5 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 October 11, 2017 the HKMA, Securities and Futures Commission (SFC), and Insurance Authority (IA) each relaxed their respective requirements to verify addresses in the context of AML (see Ref. B10/1C, http://bit.ly/2FByORK).

6 See "Outcomes FATF Plenary, 21-23 February 2018", FATF, http://bit.ly/2EMkwRT.

7 GPFI, 2016, "Updated G20 financial inclusion indicators focus on digital financial services," G20 Financial Inclusion Indicators, August 10, http://bit.ly/2FvXkrI

8 UNCDF "Financial Inclusion and the SDGs," United Nations Capital Development Fund, http://bit.ly/2DkTBap

9 Arner, D. W., J. Barberis, and R. P. Buckley, 2016, "The evolution of FinTech: a new post-crisis paradigm?" Georgetown Journal of International Law 47:4, 1271-1319

10 Arner, D. W., J. Barberis, and R. P. Buckley, 2017, "FinTech, RegTech and the reconceptualisation of financial regulation," Northwestern Journal of International Law and Business 37, 371-414

by the FATF, Basel Committee on Banking Supervision, Financial Stability Board (FSB), and the U.N. In this article, we examine how financial centers could make use of technology in the context of digital identity and electronic AML/KYC requirements.

This article identifies and considers three different aspects which must be addressed strategically:

- Digital ID infrastructure
- eKYC infrastructure
- Suitability infrastructure

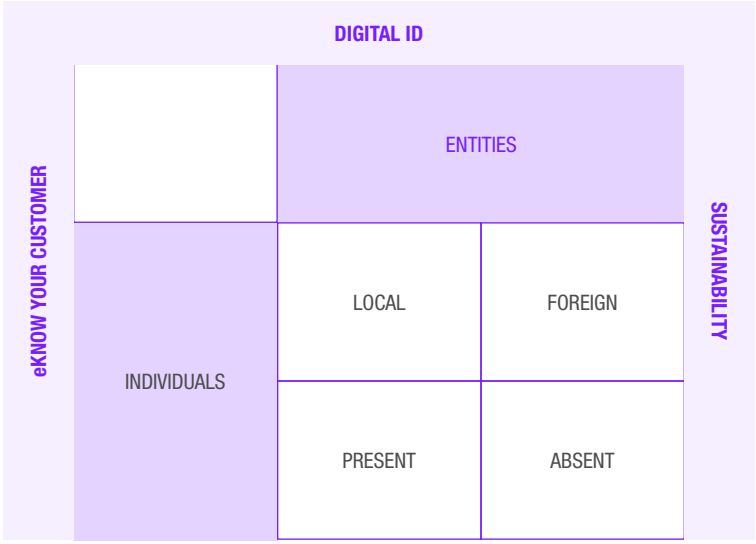
Across each of these aspects, the article considers two different contexts that must be addressed as part of the strategy: (1) individuals and (2) entities (especially companies). Within these two contexts, the strategy must also address: (1) local and (2) non-local individuals and entities, and also (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 in some form of 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 strategy for putting in place the necessary financial infrastructure to meet objectives of financial integrity, financial inclusion, and financial competitiveness, with the following sections addressing each of digital ID, eKYC utilities, and suitability in turn.

2. THE ROLE AND BENEFITS OF SECTOR-WIDE E-ID SYSTEMS

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 on refreshing and re-verifying their client information, making transactions expensive for institutions and inconvenient for clients. 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

Figure 1: Digital client on-boarding matrix



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. A sector-wide e-ID KYC utility is a potential solution to these challenges and, unsurprisingly, the idea of a centralized KYC utility is gaining traction globally.[11]

The next section analyzes the connection between KYC utilities and digital identification systems.

2.1 E-ID on the rise

Ensuring that all steps of identification for an E-identity can be performed online and from any location is an important objective of law makers around the globe. Examples addressing each pain point in the identification network include the Aadhaar in India, probably the most up-to-date and ambitious top down eID project, the GovPass in Australia, which connects existing ID devices and turns them into an eID system, as well as the E.U. e-IDAS Regulation, which seeks to solve the issue of how to provide cross-border eID.

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

2.1.1 Creating digital identity from scratch – the Indian Aadhaar system

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. Enrollment 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 information 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.[12]

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, indeed, 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 enrollment center in person.[13]

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 identity cards are a breach of privacy, and that data is 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; and there have indeed been many problems in Aadhaar's implementation.[14] 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.[15]

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."[16] 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 U.S.$5 billion.[17]

2.1.2 Linking identity databases – 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 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.[18]

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."[19] The Identity-Matching Services Bill 2018 (Cth) was introduced to the Australian parliament

[12] About Aadhaar, Unique Identification Authority of India, http://bit.ly/2HsyzJd
[13] Aadhaar data update, Unique Identification Authority of India, http://bit.ly/2xoDhG4
[14] 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
[15] Puttaswamy (Retd.) & Anor v Union of India & Ors (Civil) No 494 of 2012.
[16] Abraham, S., R. S. Sharma, and B. J. Panda, 2017, "Is Aadhaar a breach of privacy?" The Hindu, March 31, http://bit.ly/2BpbVyx
[17] The Economist, 2016, "Indian business prepares to tap into Aadhaar, a state-owned fingerprint-identification system," December 24, http://econ.st/2FyB0hb
[18] Govpass, Australian Government Digital Transformation Agency, http://bit.ly/2Go0z1C
[19] COAG, 2017, "Intergovernmental agreement on identity matching services," Council of Australian Governments, October 5, http://bit.ly/2p5g5YO.

in February 2018. If passed, the bill will authorize the Department of Home Affairs to facilitate communication between agencies with the creation of five identity-matching services.[20] 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.[21]

2.1.3 Towards cross-border digital identity: The European e-IDAS regulation

In contrast to Australia, Canada, and the U.S.,[22] identity cards with a chip embedded and common security features including the E.U.-wide use of biometrics are widely spread and used in E.U./E.E.A. member states and shared among member states' authorities. In most countries, ID cards have substituted passports and driver licenses for ID purposes.

Initially, this was also true for the U.K., where resistance against a pan-European standardized ID card was traditionally fierce. In fact, the U.K. Presidency of the E.U. council advanced E.U.-wide ID card standards, data retention, and intelligence sharing to fight terrorism in 2005, following the bomb attacks on the London subway system on 7 July 2005.[23] Following the epeal of the British Identity Cards Act by the Identity Documents Act 2010,[24] the British ID cards introduced only in 2006 were canceled. Since then, foreign nationals from outside the E.U. have been required to have an identity card, thereby turning the U.K. into something of a pre-ID state similar to that of Australia, Canada, and the U.S.

At the same time, a focus of European policy is on ensuring cross-border business transactions. European policy actions since the mid-1990s have been focused on trying to ensure that digital signatures and related declarations of will are recognized **across borders**. Since then, member states had to ensure that advanced electronic signatures based on a qualified certificate and created by a secure-signature-creation device were deemed valid signatures under the laws of each member state, in the same manner as a handwritten signature, regardless of its electronic form; in particular, digital signatures were admitted as evidence in legal proceedings.[25] 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

[20] 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).
[21] Identity-Matching Services Bill 2018 (Cth) s 7(3).
[22] See on the U.S., Quarmby, B., 2003, "The case for national identification cards," Duke Law and Technology Review 1, 1-10.
[23] See eGovernment news – 14 July, 2005 – E.U. and Europe-wide – Identification & Authentication/Justice and Home Affairs, http://bit.ly/2FDfWSi
[24] See http://bit.ly/2FJybsP
[25] 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.

deal with authentication and trust services, two pillars of eminent importance in today's online markets.

These issues have become particularly evident in cross-border transactions and were seen as barriers to completing the European internal market: national online trade (42%) as well as U.S.-based online services (54%) relying on enterprise-made identification systems dominate the European online economy, where E.U. cross-border online services represented a meager 4% of online sales.[26] The European regulators adopted the **eIDAS regulation (eIDASR)**[27] in 2014 with a view to reducing the costs of changing one's online relationship, be it in commerce or financial services, and enhancing competition.

The eIDASR shall provide "a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities."[28] The underlying rationale is that legal certainty on eID services will assist businesses and citizens to use digital interactions as their natural form of interaction. Rather than introducing a pan-European ID card system, which would double the efforts for member states, the eIDASR seeks to ensure that people and businesses can use their own national eIDs to access public services in other E.U. countries where eIDs are available 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.[29] Use cases include the submission of 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 online calls for tender.

Prior to the adoption of the eIDASR, many different national standards of eIDs were developed within the E.U. member states, independent from coordinated E.U. policy. Rather than harmonizing those standards, the eIDASR focuses on technical interoperability of all existing eID standards. By mandating the liability of 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),[30] 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 E.U. 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 E.U./E.E.A.

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 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.[31]

2.1.4 Sector neutrality

These ID systems are, from a sectorial perspective, neutral instruments. Financial services were not the center 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 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

[26] See Government of the Grand Duchy of Luxembourg, Countdown to eIDAS, http://bit.ly/2FOlUmU
[27] 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
[28] European Commission, http://bit.ly/2p9FH5P
[29] European Commission, http://bit.ly/2p9FH5P
[30] See Article 11 of the eIDAS Regulation.
[31] 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.

to them via a screen camera,[32] while corporate clients must have a Legal Entity Identifier (LEI) when entering into financial services contracts.[33]

2.2 Synergies and scale economies of sector-wide e-ID utility

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.

More importantly, focusing on only identification, and ignoring sector-specific needs and use cases, misses many of the opportunities an e-ID system could provide. In an ideal digital services world, not only would identification proceed smoothly, but every step necessary for client-onboarding and back-up checks would be done simultaneously, and only **one time per client for all kind of services and intermediaries**. Only if this is achieved will financial intermediaries benefit from the full potential of a sector-wide e-ID system.

For instance, additional information to be embedded for financial services providers into, let's say, the LEI or a new smart ID card, 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 also determine which client relationships will 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 can also be fully automated, rendering manual intervention unnecessary.

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 (let's say the E.U. or Hong Kong) may review the AML questions, while the first investment firm selling the client investment products may add the information on suitability. As accountability is vital, records of who has added which information and when are essential.

2.3 Responsibility

One issue facing the one-stop-shop concept for e-ID, including CDD and other financial services information, is who must take responsibility for compliance. While financial institutions may rely upon an intermediary to perform any part of the CDD measures, the ultimate responsibility for ensuring CDD requirements are met remains with the financial institution.[34] Even if a financial institution relies on CDDs performed by other intermediaries, the **respective rules of each jurisdiction are burdensome**. For instance, under Hong Kong law, the financial institution must obtain written confirmation from the intermediary that it agrees to perform the role and that it will provide, upon request and without delay, a copy of any document or record obtained in the course of carrying out the CDD measures on behalf of the financial institution. The financial institution must also ensure that the intermediary will comply with the AMLO record-keeping requirements, and if requested by the financial institution within a period of six years following the end of any business relationship with a customer, provide a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out CDD as soon as reasonably practicable after receiving the request. In the same vein, 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 as one AML CDD can serve many banks, if a respective amount enters a bank account and only circulates within a regulated banking system where all participants are subject to the same AML rules. For example, money enters the E.U. banking system from a bank account in the Cayman Islands. The first E.U. bank needs to apply full CDD. In the absence of new information, banks that receive payments from that first E.U. bank can categorize those transactions as "low risk," i.e., they

[32] 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.

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

[34] See, for instance, Article 25 (1) of the European 4th AML Directive (supra note 2).

can in principle trust that the CDD applied by the first E.U. bank led to accurate results, and that the money is "clean."[35] The same logic could be utilized for a sector-wide e-ID plus system (or KYC utility). Note that this logic only works in closed systems, from which money cannot leak in or out.

3. TOWARDS "E-ID PLUS": SETTING UP A KYC UTILITY

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

3.1 The complexity issue

However, those who seek too much will achieve nothing. Any KYC utility project must necessarily start small. This is because hundreds of small questions must be answered to build it. Some sample questions illustrate what may be required to build a well-functioning KYC utility:

1. Which technological platform? A centralized ledger or a distributed ledger?[36] Ensuring simultaneous access is the strongest argument in favor of using distributed ledgers, while data privacy and governance concerns may tip the tide in the direction of concentrated ledgers.

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 above (II.3.) 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 Question 2. The more reliable the members, the more acceptable is member-based data maintenance.

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 the KYC utility, the argument for joint liability lies in incentivizing all members to invest in the maintenance and further development of the utility (similarly to how stock exchange participants together, 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).

[35] 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 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.

[36] See on distributed ledgers Zetzsche, D. A., R. P. Buckley, and D. W. Arner, 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

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

3.2 Efficiency curve

Small improvements in this field can yield significant benefits. For instance, assume that five members each invest two staff hours in 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 two hours invested by only one entity, the overall cost savings approach 80%. Compare this with ten members: putting the cost of the technology aside, the costs saving would be 90%, but only 10% greater than those of the utility with five members. Those additional 10% will be partially offset by the additional costs of coordinating the additional five members. However, the calculated savings materialize only when participating institutions serve the same client. If we assume that all participants serve the same number of regional distribution of clients, the likelihood that this will be the case increases with the number of participants in the KYC utility. Under the conditions set out, the larger the utility in terms of members, the greater the likelihood of efficiency gains. Nevertheless, agreeing on governance features and standards is far easier with fewer rather than more members.

Thus, financial centers should aim to start small with a KYC utility, and plan for it to grow over time.

3.3 Reducing complexity

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 e-ID solution could first aim at digital identification of domestic licensed financial intermediaries, then include locally incorporated companies (relying on LEIs) and finally be utilized for non-face-to-face on-boarding of individuals. Internationalization, including foreign institutions, is perhaps the final step to be tackled.

4. GOVERNANCE OF E-ID SYSTEMS

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, the largest global distribution center for investment funds, with its funds offered in more than 70 countries around the world.[37] A sector-wide AML/KYC tool that truly covers all client relationships will provide enormous synergies, but also pose new risks for clients globally.

How these risks could 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, such as GDPR)[38] together with non-legal factors (such as the technology used – with blockchain a natural candidate),[39] 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:

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.

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 for 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.

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 preconditions.

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

[37] See ALFI, 2018, "Global fund distribution," http://bit.ly/2pagnwC
[38] 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.
[39] See on Blockchain Zetzsche (2017), supra 36.

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 (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 certain 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 take on.

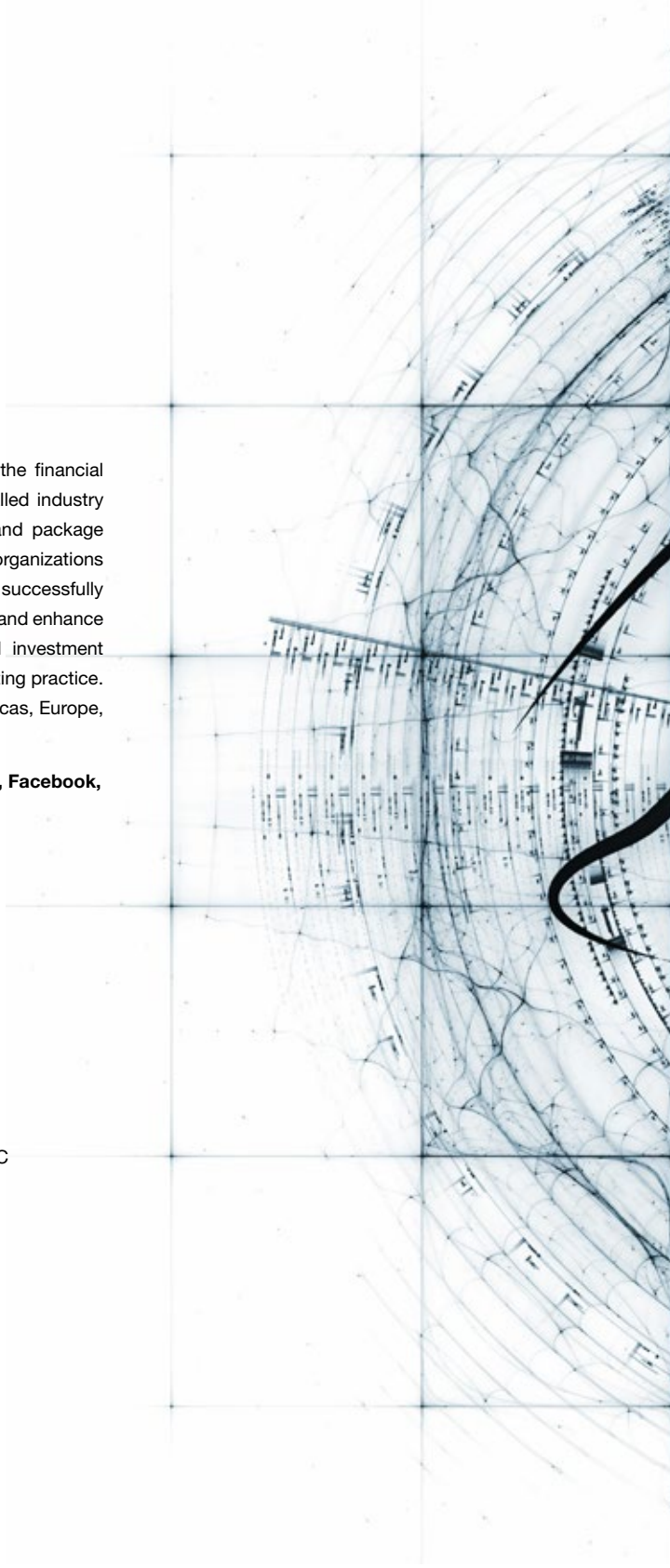
5. THREE STEPS TOWARDS A SECTOR-WIDE E-ID UTILITY

While no single solution will address all the various issues identified, financial centers 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 the center. Three steps are of particular importance.

First, where a financial center is implementing **new e-identity solutions** (such as the new smart Hong Kong 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).

Second, 100% e-ID coverage is neither feasible nor likely in the short term, and aiming at 100% coverage from the beginning will either increase the risk of disruption, or delay any synergies from sector-wide e-ID systems for the foreseeable future. Thus, **complexity should** determine which steps should be 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 e-ID solution could first aim at digital identification of licensed financial intermediaries, then include locally incorporated companies (relying on LEIs) and finally be utilized for non-face-to-face on-boarding of individuals.

Third, from the beginning, putting a great deal of attention into the **governance** of the sector-wide e-ID tool is of utmost importance. Knowledge is power, and where there is a lot of knowledge, there is a lot of 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, but also applicable data privacy rules, such as GDPR) and also **non-legal factors** such as the technology used (with blockchain being a natural candidate), the cyber-security risks incurred, and the need to ensure further technological evolution of a networked infrastructure to which thousands of entities may need to be linked.



ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward. Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, and finance, risk & compliance. We also have an energy consulting practice. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Xing.**

WORLDWIDE OFFICES

Bangalore
Bangkok
Bratislava
Brussels
Charlotte
Chicago
Dallas
Dusseldorf
Edinburgh
Frankfurt
Geneva
Hong Kong
Houston
Kuala Lumpur
London
New York
Orlando
Paris
Pune
São Paulo
Singapore
Stockholm
Toronto
Vienna
Warsaw
Washington, DC
Zurich

CAPCO.COM

CAPCO