

THE IDENTITY CHALLENGE IN FINANCE: FROM ANALOGUE IDENTITY TO DIGITIZED IDENTIFICATION TO DIGITAL KYC UTILITIES

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

www.ssrn.com/abstract=3224115



RESEARCH UNIT

Who are we?



- We ourselves know who we are
- Digital Identity is about how to
 - ✓ provide evidence to others that we are who we say we are ('identification')
 - ✓ ensure useful data sharing while retaining privacy
 - \checkmark balance costs for society, tax budgets and individuals



'Identity' Generators

 With sufficient data points a person may be identified as unique ('digital DNA')



Today's Topic

Identity is fundamental in finance. Knowledge of clients' identities is essential to protect against fraud and crime. From a risk management and regulatory standpoint, identity is essential to market integrity.

But identification and KYC rules can be **major barriers to accessing financial services**. We argue that **technology can solve this challenge** through the development of **digital KYC Utilities**. The establishment of digital KYC utilities requires addressing design questions such as registration methods, data availability and cross-jurisdiction recognitions. Yet, 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.



Four (Old) Issues of Digital Identity to which eKYC could provide the answer

- How to uniquely identify someone digitally? Can a pin code / data code replace a "wet signature"?
 - Ethical/legal limits vs. Certainty of Identification
- Multiplication of IDs (cards, PIN/TANs, widges)
 - User friendliness, Cost efficiency
- Cross-border & Third Party Recognition? If services can be rendered digitally/ globally how to onboard customers remotely?
 - Interoperability
- Unauthorized & 'Unwanted' use (google, amazon etc.)?
 - Re-Privatization of digital identity



OVERVIEW

- A. Introduction $\sqrt{}$
- B. The Identity Challenge in Law & Finance
- C. Solving the ID Challenge: Infrastructure for Digital ID
- D. Towards KYC Utilities
- E. Conclusion & Theses

RUL



B. The Identity Challenge in Law & Finance



Balancing Objectives

- Customer Due Diligence (CDD) ensures trust and confidence in the financial system; combatting crime, tax fraud and terrorism
- CDD rules exclude some poor individuals and small firms from financial services
- \Rightarrow Hampering growth, innovation and development
- \Rightarrow Asia: SMEs lack USD 1.6 trillion in funding; but generate 80% of the jobs



Conflicting Objectives

- Customers in the Global South often see as 'risky' for lack of documentation
- Derisking strategies apply (i.e. financial exclusion)
- \Rightarrow At odds with financial inclusion strategies
- \Rightarrow Identity at the core of the issue: 1.5 billion people (1 in 6 globally) lack valid ID.
- \Rightarrow Ensure identity \Leftrightarrow fight financial exclusion



New Solutions to Old Challenges

- Digital footprint ⇔ Traditional (Legal) ID?
- Introduce physical, electronic and behavioural ID factors
- From summary to definition of oneself
- Consider risks
 - Fake IDs
 - Loss of privacy
 - Monopolization and risk of abuse
 - \Rightarrow ID-ed individuals banked but imprisoned in the digital data tower?
 - \Rightarrow Substitute financial inclusion for digital intrusion?



Solving the ID Challenge: Infrastructure for <u>Digital ID</u>



RUL

Examples

- Aadhaar in India: biometrics as basis of personal identifier
- Digital ID without national ID: Australia, UK
- Identity plus-solutions: credit registers in Tunisia
- Solving the cross-border issue: Interlinking Domestic ID systems in Europe
- \Rightarrow Three lessons learned



Lesson 1: Balancing commercial, public and private interests

- Fully commercial IDs are « exclusive » since non-customers are out in the cold
- Fully public IDs are potentially too small in terms of data points to meet demands of innovation
- Fully private IDs do not recognize the investment by private enterprises



Lesson 2: Base vs. Business ("Pseudo") Identity

- Base: raw data, confirmation of « who you are »
- Business: additional profile data, confirmation of « how you are »
- ⇒ Client suitability requirements, financial sophistication, credit history, bank accounts etc.



From Base to Business ID: Multiple Pseudo Identity (access arrangement by necessity)



Lesson 2: Base vs Business ID

- First identification essential for onboarding, but not for operations
- FS institution can create substitutes (biometric data)
- FS institutions can foward those substitutes to centralized database (run by the CB) and remanufacture a centralized ID system
- \Rightarrow Business ID: objective focused (avoid multiplication of identities)
 - other data than Base ID
 - better data than Base ID?



- Can integrate upsides of layered identity man't ("reprivatisation")
- Minimum parts of private "base ID" to be defined by legislature

Universal Access, Global Reach

- Requires only agreement on biometric raw data
- Results in multiple additional customized datasets
- Global Ident & Access Man't (Standardization)
- Connection of ID systems: eIDAS Regulation (EU) as a starter?



Lesson 2: Base vs. Business ("Pseudo") Identity

 \Rightarrow But: multiple powerful business / « pseudo » IDs

- create privacy challenges
- add to the monopoly of large incumbents (« own ecosystem »)
- provide barrier to entry for small and innovative firms
- enhance cyberrisk due to single point of failure
- \Rightarrow necessitates Identity Risk Management



Lesson 3: Connectivity is crucial

Connectivity

- disrupts ID monopoly of private business ID holders
- spurs innovation
- allows for regional and provider diversification
- \Rightarrow Connection of ID systems: eIDAS Regulation (EU) as a starter?



EU eIDAS Regulation – interlinking ID systems

- safe access to services and (cross-border) online transactions online in just "one click"
 - \Rightarrow higher security
 - \Rightarrow more convenience for any online activity
- Examples:
 - ✓ submitting tax declarations
 - ✓ enrolling in a foreign university
 - ✓ remotely opening a bank account\
 - ✓ setting up a business in another Member State
 - ✓ authenticating for internet payments
 - ✓ bidding to online call for tender



- Open technical standards, ready for expansion towards a global identity network based on mutual recognition
- Country specific identification can be maintained and connected
- Public and private sector
- What works between countries can work between financial institutions; eIDAS open for private connectors
- \Rightarrow understand financial institutions as
 - recipients as well as providers of business identity and
 - providers of base identity



RESEARCH UNIT

D. Towards E-KYC Utilities





The KYC-AML Hub as horizontal integration









<u>Q1: Public or Private Initiative?</u>

- Private services available (e.g. Thomson Reuters in South Africa, Clarient, SWIFT, Fenergo, etc.)
 - Information markets: natural monopoly => avoid data privatization
 - Data sensitivity => data protection => avoid dispersion of data
 - International private actors vs. national supervisors
- Public services available (e.g. India Aadhaar system; LEI administration in Europe)

 - Large private entities will be unwilling, small private entities unable to do it.
 - Innovation vs cybersecurity: public risk control, but also public tardiness
 - \Rightarrow Public purpose entity or cooperative most suitable



<u>Q2: Scope => From Simple To Complex, Local to Supra-National</u>

- 1st stage: introduce KYC Utility in closed systems (for instance, regulated credit institutions only)
- 2nd stage: open for other sectors => additional information, additional members, additional complexity
- 3rd stage: Achieve highest level of efficiencies => include various sectors, intermediaries and entities



<u>O3: Number of participants</u>

- 5 participants = 80% ./. 20% of set-up costs + coordination costs↓
- 10 participants = 90% ./. 10% of set-up costs + coordination costs[↑]
- \Rightarrow start small
- \Rightarrow use open standards, formats and neutral priorities
- \Rightarrow prepare for growth
 - Contractually: simple, transparent, open language
 - technically: bandwidth, data points, system design etc.



RESEARCH UNI

Q4: Which technological platform? [centralized or distributed ledger? Simultaneous access vs privacy/ governance]

Q5: Who shall participate, when and how? (technology sophistication, access to hyper-fast data streams, CDD reliability).

Q6: What type of information will be shared? (synthesized result, i.e. "client is clean: yes/no" vs. variants of additional information).

Q7: How often will the information be updated, and by whom? (centralized data maintenance to member-based maintenance).

Q8: How will liability be shared if, and when, things go wrong? (one entity or joint liability; joint liability acceptable only if members are financially stable) RESEARCH UNIT



<u>Q9: Responsibility</u>

- Responsibility remains with outsourcing entity.
- Within closed systems CDD can be delegated to KYC Utility (only) if KYC Utility is well governed and supervised.
- \Rightarrow Consider additional legislation to ensure governance and supervision of KYC Utility.



Q10: Governance

- Knowledge means power => concentration of knowledge means concentration of power.
- KYC Utilities ⇔ Stock Exchanges: both are
 - information intermediaries
 - generators of transaction costs, and as such subject to expectation of low / zero cost service
 - generate and host very valuable, business relevant information; in turn no single financial market participant want another participant (nor government) to rule over the KYC Utility
 - \Rightarrow Similar governance questions apply



1. For-profit entity or an association acting on behalf of its members? (Arg: financing? Up-front costs, user fees; antitrust concern? Profit vs. transaction costs)

 \Rightarrow Public purpose entity or association

2. Who should run the day-to-day business of the utility?

- \Rightarrow legal and tech managers with adjudication skills
- \Rightarrow independent from any large incumbent participant



3. Users' or members' participation rights?

- \Rightarrow Those with the greatest interest in the functioning of the utility shall have the greatest say.
- ⇒ Voting rights by number of (1) updates of KYC data, (2) requests of KYC data, (3) a mix of (1) and (2), or (4) liability?
- \Rightarrow mix of the former. For user-related questions (1) to (3), for financing and risk-oriented decisions (4).



4. Who decides upon membership applications?

Options: expert committee, the KYC utility's board (if any), the membership assembly, state institution (such as the financial regulator)

- \Rightarrow Multi-step approach.
- \Rightarrow Expert committee or regulators to review tech sophistication and governance of new member and to provide recommendation.
- ⇒ Membership assembly or board entitled to reject application with reasoned opinion only



RESEARCH UNIT



Conclusion & Thesis





<u>THESES</u>

1) The present focus on identification, while ignoring sector-specific needs, misses many potential opportunities an eKYC system could provide. Economies implementing new digital ID solutions (e.g. smart national ID card or LEI) should **link such identity devices to AML/KYC checks and other business ID data**, by ensuring that adequate technology is implemented and sufficient data points exist in storage devices.

2) **100% digital ID and eKYC coverage is neither feasible nor likely in the short term**. Complexity should determine which steps are taken and in which order. Small numbers generate (already) impressive efficiency gains.

3) E-ID for small amount transactions can be created from ad-hoc collected data (biometrics). It does not have to be centralized prior to service. No passport etc system necessary.

4) For sector-wide AML/KYC tools **governance is key.** Addressing these risks requires careful thinking that takes into account legal factors, non-legal factors (such as technology), the cyber-security risks incurred.

5) ID management is a sensitive matter. Take Care. Start small. Grow slowly. Learn from

TechFin / Data-driven Finance

www.ssrn.com/abstract=2959925



Regulatory Sandboxes www.ssrn.com/abstract=3018534



Recommended Readings on FinTech

Digital ID/KYC Utilities www.ssrn.com/abstract=3224115



ICO Goldrush

www.ssrn.com/abstract=3072298

Distributed Ledgers / Blockchain www.ssrn.com/abstract=3018214



Against Hard Interest Rate Caps and Pro FinTech / RegTech <u>www.ssrn.com/abstract=3159202</u>







RUL RESEARCH UNIT



Thanks!

Prof. Dr. Dirk Zetzsche, LL.M. ADA Chair in Financial Law / Inclusive Finance University of Luxembourg Dirk.Zetzsche@uni.lu www.ssrn.com/author=357808

RESEARCH UNIT

RUL



