# Dissolving Barriers:
## A Global Digital Trust Protocol

Based on a chapter of the same name written by Ankit Ratan, published in *The REGTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation* by Janos Barberis, Douglas W. Arner, & Ross P. Buckley.

SIGNZY

# The Problem

Due diligence for cross-border transactions takes months to complete. The time and cost to overcome business and compliance risk is high.

## Example

In a cross-border transaction taking place between two parties in the United States and India, the US party would hire a US law firm A and the Indian party will hire an Indian law firm A to ensure that the transaction complies with the local regulatory regime. Since the two parties do not trust each other, they will, in turn, hire lawyers in the other jurisdiction, i.e. the US law firm will hire an Indian law firm B, and the Indian law firm will hire a US law firm B.

- This illustrates how a single transaction now involves four law firms, resulting in time and cost escalations, which increasingly restrict such cross-border transactions.

SIGNZY

# A Solution

A global digital trust system allows multiple parties in different jurisdictions to transact through a single platform. It could ensure the transaction meets compliance for each jurisdiction.

Digital trust is important for the success of this solution. Building digital trust is a 3-part process:

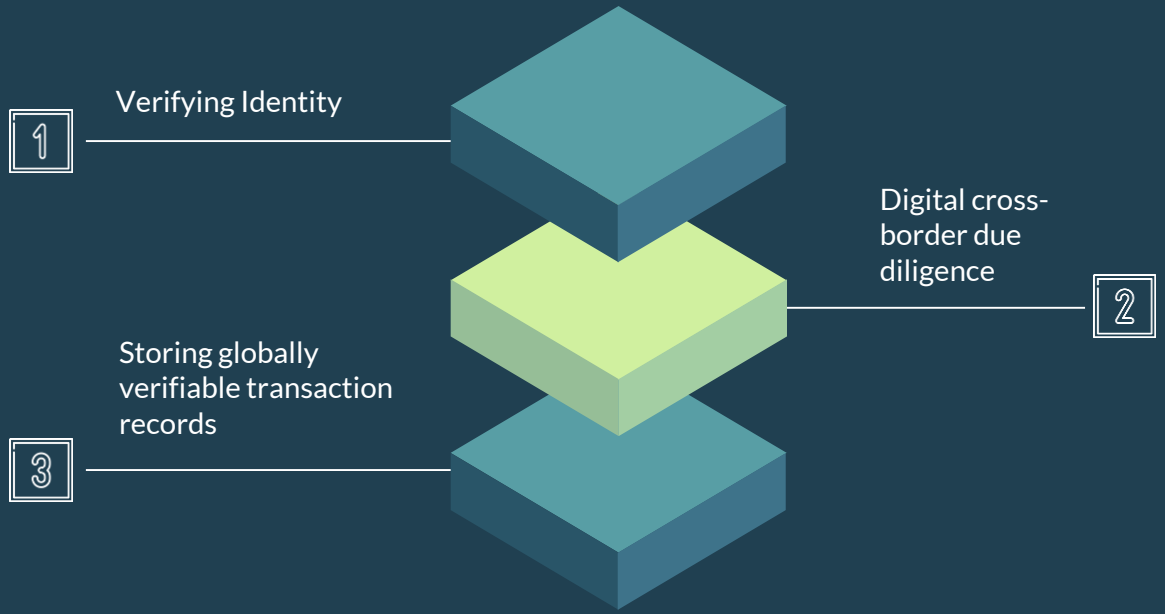
1. Authenticating unique identity
2. Getting to know more about this ID
3. Digital record of the transaction

Part 1 and 2 come under financial Know-Your-Customer (KYC).

SIGNZY

# What is needed to create this system?

To create a global digital trust system, one would need a global way of:




SIGNZY

# Attempts at unified global identity

1. Generic digital identities

**Example:** email as a login username, social media login as a digital profile (FB, Twitter)

- **Email** is insufficient from the regulatory standpoint since it does not uniquely identify the user.
- **Social profile**, however, is difficult to replicate. Data from timeline and network can identify fraudulent profiles.
- Facebook & Google are becoming the industry standard
    - Facebook has patent to use social network data for lending
    - Social profiles are being used to give creditworthiness scores (Lenddo)
    - Google is planning to use location and behaviour data to assess risk and do basic KYC checks

SIGNZY

## 2. Digital identities linked to unique physical identities

Companies are trying to link national identities to a global identity.
Possible approaches: verification using large human team, storing data on blockchain

**Key steps:**

i) verify the national ID
ii) verify the data on the national ID (if possible)
iii) prove person uploading ID is same as person creating the digital ID (biometric proof)

**Example of verifiable biometrics:** Aadhaar database in India for fingerprint/iris/face, available as an API for easy consumption

**The problem:**

- IDs are not global or equal in privileges
- ID frauds are prevalent
- No evidence to show frauds in offline will not translate to digital world

SIGNZY

# Due Diligence

KYC does not merely imply establishing identity. KYC implies knowing your customer beyond the person's name, date of birth, and PIN code. This is where negative lists come into the picture. Each country has a different regulator, and they have different negative lists based on differentiated criteria.

## Example

India: Industry regulators like RBI, SEBI, IRDA, Registrar of Companies publish lists. Administrative and policing agencies like NIA, CID, and Central Vigilance Commission publish names associated with AML or countering the financing of terrorism (CFT).

USA: A unique sanction list is published by the US Treasury Department

SIGNZY

# Due Diligence (Contd.)

Moreover, different regulatory bodies are recording and furnishing KYC information in different countries.

## Example

India: There are multiple entity types such as a private limited company, limited liability partnership, partnership firm, sole proprietorship firm, HUF, trust, and so forth. Each entity type is governed by a different regulatory regime, which prescribes ownership and identity documents and other proof of business.

USA: Each state has its own regulatory regime for incorporation of entities, and their identification and business proof documents. Each state also allows multiple types of such entities, therefore leading to multiple types of documents for KYC.

SIGNZY

# Beyond One-time KYC: Keeping Records

The other dimension of trust is history.

Storing and sharing historical data may involve sensitive information. This is therefore a sovereign sensitive subject. What is possible is putting all future global transactions on a record and using mere transaction party history itself, without revealing the nature of the transaction.

The creation of defaulter history has been one of the most critical regulatory processes within the banking domain.

**Issues:**

1. **Input** (how one can trust organizations that are inputting negative data
2. **Privacy** (collecting someone's past behaviour might not always be fully legal

SIGNZY

# Keeping Records (Contd.)

Current practice: To have special access to industry centralized databases.

Example: Credit Bureaus

Challenges: 1. Real-time updating of these databases
2. The critical sovereign aspect: cross-border data sharing

## Example

When people with current outstanding loans migrate from India to US, they have higher default rates.

Why? Credit scores in the US are unaffected by their credit history in India, as the US banks have no way to verify or link their Indian credit history.

SIGNZY

# Core Function of Compliance Can Be Replaced by an AI Platform

The context: In an increasingly digital world, real-time decision making is becoming an essential need of the business.

For example: Multiple FinTechs are effectively creating online loan processes that take under 5 minutes.

The need: All compliance checks also need to be concluded within this period and hence be done in real time. While compliance can also be done later in an offline mode, the speed of the digital world makes post-compliance a very risky affair. Hence, real-time compliance has become a core value required of the regulatory environment of the digital world.

SIGNZY

# More on the AI Platform

The flip-side: Risks in the digital world are much higher and severe damage can be done within hours.

The solution: A real-time system that makes checks as strictly as today's human-based processes. An AI-based KYC system itself is a need in a future digital world. This KYC system will have three key components:

1. ***Verification of identity:*** ability to link to a local identity system and authenticate person digitally.
2. ***Background check:*** ability to access local negative lists and databases, either public or industry-specific.
3. ***Regulatory decision engine:*** Make decisions based on current prevailing guidelines and outputs from 1 and 2.

SIGNZY

# [1] Verifying Identity

A human-based process requires the person to produce an ID document. An officer sees this, and then does the following three things:

- Establishes that this is a valid ID
- Establishes that the form details and ID details are same
- Matches the customer's face with the picture in the ID

The process is region agnostic. Companies (including Signzy) are performing these processes using COMPUTER VISION (a subset of the larger AI world) where the workflow is simple. The user does a video onboarding where they show ID documents. The algorithms in the background have the ability to make all the three judgements and let the case pass or not.

SIGNZY

# [2] Background Check

Even today background checks represent a fairly automated process. A simple ability to connect and update the data should be good enough. Additionally, an ability to crawl and update negative lists would be desirable.

# [2] Regulatory Decision Engine

Outputs from both these engines would have to be run through the particular case. This process will be an AI replica of a more manual process today, where risk teams using their understanding of compliance rules make a judgement in each case file. This engine can slowly evolve into a self-learning-based engine where digital frauds may throw up some interesting compliance best practices that have not been thought of today.

SIGNZY

# The Power of a Common Global KYC Platform

The power here lies in the common platform both parties rely on to do verifications. It may seem that the platform's advanced technological ability makes it acceptable. However, the real acceptance would be derived from two parties using the same platform to do local verifications.

Once Party A trusts this platform for its own local KYC, it's easier for Party A to trust the same for a global KYC check. Though this platform obviously has no single ID, it has a common intelligence layer. This layer decided, as an example, that it would use Aadhaar in India and SSN in the US.

SIGNZY

# Keeping Records Beyond KYC

In a digital world, you need a negative database that gets updated in real time and still is able to ensure basic global principles are met:

**(i)** privacy

**(ii)** quality of data

**(iii)** global accessibility

Proposed solution: Decentralized digital ledger. The protocol will carry the following two types of data:

1. Unique identity
2. Transacting parties and their trust rating

**Trust rating** would be a function of the number of past transactions. In this function, each transaction has weightage based on the trust rating.

SIGNZY

# Keeping Records Beyond KYC (Contd.)

## Example

Someone frequently transacting with low-trust parties might have a lower trust rating than someone with fewer transactions but with high-trust parties.

**Current situation:** Blockchain has become synonymous with a decentralized ledger. We already have globally decentralized ledgers with decent adoption.

**Future Possibility:** One or multiple blockchains can be used to record transactions between parties and create trust scores that are verifiable by anyone across the world.

SIGNZY

# Conclusion

The offline trust mechanism performs two functions:
(i) identify the person by look or feel
(ii) learn something about the person's behaviour.

This AI-based platform would be able to do these two important things needed to replicate the offline human and paper-based trust mechanism:

1. Establish a digital KYC using AI that meets or even supersedes today's local human-based processes, thus satisfying local regulators.
2. Create a reward/punishment mechanism based on future digital transactions by assigning trust scores.

Thus, even though this system creates neither a global digital ID nor a common negative list, it can create a platform for enabling digital trust globally. The system will also ensure compliance with different jurisdictions and the differentiated regulatory regimes. This, in turn, will lead to seamless cross-border transactions to enable a truly digital global economy.

SIGNZY

## For more information visit us at:

 : Signzy

 : signzy.com

 : @TeamSignzy

 : /TeamSignzy/

SIGNZY