Briefing Note | **DataTalk** 12

Digital Identity

March 2022

Reliable and trustworthy digital identity (DI) services are a crucial enabler for integration into the digital economy. The technology holds great promise in contributing to financial inclusion, financial crime prevention, and improved customer onboarding experiences. It also presents financial institutions (FIs) with a unique opportunity to leverage their existing positions as trusted data custodians and their large KYC investments. Moving forward, it will be vital to make DI "smart", and stakeholders from both the official and private sectors will need to prioritize creating standards that enable interoperability across sectors and borders. This note provides a summary of the key themes from the discussion, respecting that the conversation was conducted under the Chatham House Rule and comments are unattributed.

Identity is a digital asset. Verifying consumers' identities and keeping that information safe and secure is more important than ever as digital activity accounts for an ever-growing share of the economy and cybersecurity risks multiply. Individuals today commonly manage dozens of passwords, which is increasingly frustrating for consumers, costly for companies, and poses security risks for all parties. Institutions can create solutions by considering DI as a strategic business opportunity rather than just a technological problem to solve. High trust services that enable people to carry their identities with them and exercise greater control over their data can promote economic growth and inclusion, enhance privacy and security, and strengthen customer relationships.

FIs, especially banks, are well placed to play a leading role. Their core competencies include helping customers execute transactions, protecting assets, and managing risk, all of which can be applied directly to DI as a new asset class. The prospect of decentralized services and Web3 will likely increase demand for DI, especially one that is recoverable rather than lost if the user misplaces their wallet or private key. Banks are likely to face strong competition from technology companies and telecom operators, and competitive forces may frustrate attempts at cooperation. It's possible that one institution will take the lead on identity services and other banks will seek to become fast followers because of the potential to create new revenue streams and monetize existing investments in identity verification technology to fulfill their KYC obligations.

DI has to be smart. Plenty of identity credentials have a digital component such as a driver's license or passport. To get the full benefits of digital ID, there needs to be a way for the user to only share information that is necessary for a particular purpose—for example, verifying compliance with COVID protocols like vaccination status or providing proof of age. Digital ID needs to provide value-added services to the end-user and to relying parties in order to gain traction in the market. For banks that already hold strongly proven identities of their customers; the challenge is to add other attributes. That can make a smart DI more valuable than a government-issued ID card.

Informed user consent is critical for success. Digital ID services need to gather information in ways that protect privacy and with the informed consent of the end-user. That's essential to building and maintaining trust at the core of the system because it gives users control over what data is shared and with whom. The IIF recently published Principles for Digital Trust Networks to recommend key development points such as user-centricity. The IIF also joined the Global Assured Identity Network (GAIN) to advocate for these principles in action across verification networks.

Interoperability and standardization are essential to avoid a fragmented landscape. The digital economy may be global but legal and liability standards on identity and privacy vary by jurisdiction. The European Union is taking a regulatory approach that could make its acceptance of digital ID effectively mandatory while countries like Australia and Canada, which don't have national identity cards, are adopting a trust-based approach that may play to banks' strengths. Cooperation is vital to ensure that these different approaches can work together, and we don't end up with islands of identity. The IIF is collaborating with the OpenID Foundation and others on the Open Digital Trust initiative, which aims to promote interoperable technical standards and a market-based mechanism for reconciling legal and liability issues.