DIGITAL IDENTIFICATION A POWERFUL ENABLER OF FINANCIAL INCLUSION
12 Apr 2019

Your Excellencies, Madame, Distinguished Guests, Ladies and Gentlemen,

Good afternoon, everybody.

I’m delighted to be here today. I’m happy to hear such rich discussions on how to harness digital identification for financial and economic inclusion. We just heard how important digital IDs are for mobility, security, dignity, connectivity and access to rights.

Unique biometric digital identification can be a powerful enabler of financial inclusion. It can do this in two main ways.

First and foremost, digital ID systems can positively impact KYC compliance for account openings.

It helps the 20 percent of financially excluded adults in low- and middle-income countries who are unable to access financial services because they lack the required documents to prove their identity.

Digital identification also supports ongoing AML/CFT monitoring. It better identifies, for example, who people are, from where a transaction is conducted, and, which funds are being used—all to ensure more robust financial integrity. Something that is very important.

Second, digital IDs allow the identification of recipients for G2P subsidies and enables beneficiaries to receive digital payments in a much easier way. This can reduce fraud in social programs, reduce cost and give support to people that need it and not to the middlemen.

The Government of India, for instance, has saved more than $9 billion from fraud elimination in its beneficiary lists across multiple programs after they leveraged their unique ID system for government to person payments.

However, opportunities surrounding digital ID systems are accompanied by privacy risks. Security breaches, such as through cyberattacks on databases or during data transfer, as well as facilitating surveillance on people, are threats that must be considered.

Digital technological advances can also amplify privacy risks. Instant and automated data processing can heighten exposure to fraud and identity theft. Digital ID databases with massive amounts of personal data create rich targets for hackers. And, the ability to bring digital ID databases together and combine them with other technologies, such as facial recognition, increase the opportunities for surveillance.

The consequences of privacy violations are serious. It could lead to discrimination, persecution, unjust treatment, and more.

Public trust in digital financial services can erode without strong data privacy. As you know, in financial services, trust is everything. Inaccurate or biased information might result in a person's loan applications being rejected erroneously or improperly. Or the selling of personal information to third-party data brokers can turn a person into a target of abusive marketing practices.

***

There are numerous strategies that can be utilized to mitigate these risks and still reap the benefits of digital
identification for financial inclusion. As Minister Ingabire just mentioned, a privacy-by-design approach builds privacy as the default setting into digital ID systems. This method brings together legal, organizational, and technology controls.

Importantly, a successful privacy-by-design approach requires an array of considerations.

When handling personal data, both the public and private sector can encrypt it, anonymize it, and use pseudonyms and tokens. These tactics help to:

- Firstly, limit the processing of personal data to the minimum necessary;
- Secondly, hide personal data and the interrelationships of the data points from plain view, so an individual's data points are not linked or easily observed;
- Thirdly, separate and distribute the processing of personal data to avoid the ability to make complete profiles of individuals;
- And fourthly, aggregate personal data when processing at the group level to limit privacy risks to a specific individual.

Companies and governments can also provide more control to individuals. They can ensure individuals are informed when, and why, their data is processed. Additionally, people should be provided the tools to control the processing of their data, along with the ability to correct it and challenge inaccuracies. This is very important.

If well designed, digital ID systems have the potential to be more secure and privacy-centric than traditional paper-based alternatives. Encryption, consent and control can improve security and transparency—it enables people to understand how and when their data is used by a third party. And they can also be notified in the event of a data breach.

Digital identification is also capable of protecting personal information via machine-readable credentials, such as smart cards and QR codes, so that only the pieces of necessary personal information are shared. We can bear in mind the important question “Is this something that is nice to know or something we need to know?”

Governments considering creating digital foundational ID systems could learn from the experiences of other economies which have taken a privacy-by-design approach. Peru and the EU are two good examples.

And of course, establishing international and open standards, as well as global principles will be essential to help countries further, in the design and implementation of their own digital ID systems.

***

Now, I know Kristalina is eager to offer her closing reflections as well.

So I would like to conclude by saying, how important it is that we discuss these issues and that we help each other; so that we can harness the potential of having digital identities, while we empower citizens to use them to their benefit and avoid abuse.

I wish you much success. As the World Bank focuses on this key public goods, which my work relies on, I both wish and need your success.