Financial Inclusion and Cybersecurity[1]

FinCyber Conference on Cybersecurity and Financial Inclusion

December 10, 2020

Magda Bianco

Banca d'Italia and GPFI co-chair

Good morning, good afternoon and good evening to everyone. It is a pleasure to take part in this event, alas remotely. I am grateful to the Carnegie Endowment for International Peace, the International Monetary Fund, the World Bank and the World Economic Forum for their effort: with physical distancing as a constant reminder of the difficult times we are living, I believe the topic of today's discussion is absolutely central.

The unfolding pandemic is forcing our interactions – social and economic alike – away from the physical, and into the digital space. As we find comfort in our virtual connection, however, it is important to keep in mind that billions of people still do not enjoy safe access to digital services.

While we, a minority of the global population, can count on secure and reliable networks, secure and reliable devices, suitable regulatory frameworks, capable enforcement agencies, together with a sufficient degree of digital literacy – this is far from the norm.

The digital divide cements existing inequalities, while breeding new dimensions thereof.

[1] I would like to thank Claudia Biancotti and Michele Savini Zangrandi for their help in preparing this speech and Anna Zelentsova and David Symington for their comments. The responsibility for the content is my own.

The question I would like to focus on today is: in a world of increasing digitalization of financial services, how do we onboard the vulnerable while shielding them from additional risks, including those related to cyber threats? It is a question that has become even more central with the outbreak of Covid-19.

The rise of Digital Financial Services (DFS)

In trying to tackle this question, let me build the groundwork from a few, well established facts.

Simple access to financial services is a major determinant of both individual well-being, and of collective growth[2]. Recent work by the IMF[3] shows the positive relationship between financial inclusion and the reduction of inequalities, especially at the low end of income distribution. It had previously confirmed the positive impact of financial inclusion on economic growth, and recently, again, research by the IMF has shown the role that digital financial inclusion may play in reducing the economic (and social) impact of Covid-19.

In 2010, recognizing the importance of financial inclusion, the G20 established the Global Partnership for Financial Inclusion (GPFI): an inclusive platform committed to advancing financial inclusion globally, which in the next 3 years I will have the honour to co-chair with Anna Zelentsova.

In the ten years since, there has been enormous improvement in expanding access to financial services. One simple metric shows that between 2011 and 2017, 1.2 billion unbanked adults obtained access to financial services[4].

---

2 Financial Inclusion: What Have We Learned So Far? What Do We Have to Learn?, IMF (2020)

3 M. Čihák, R. Sahay. 2020. "Finance and Inequality." IMF Staff Discussion Note No. 20/02, International Monetary Fund, Washington, DC; R. Sahay, et al. 2015. "Financial Inclusion: Can It Meet Multiple Macroeconomic Goals?" IMF Staff Discussion Note No. 15/17, International Monetary Fund, Washington, DC. R. Sahay, 2020. "The Promise of Fintech. Financial Inclusion in the Post COVID-19 Era". IMF Staff Discussion Note No. 20/09, International Monetary Fund, Washington, DC.

4 The Global Findex Database 2017.

Digitalization has played a great role in this. The number of mobile money accounts almost tripled in low and middle income countries between 2013 and 2017[5], and by 2019 the number of registered mobile money accounts surpassed 1 billion, worldwide[6].

The impact of digitalization is only starting to show. As access to digital means expands, digital financial services will play an increasingly important role in reaching the underserved population.

The limits of DFS

Yet, as the advent of Covid-19 sparks a surge in the demand for digital financial services, it also lays bare the limits and the gaps in system.

Access is anything but universal. In some parts of the world, key digital and financial infrastructure is missing or incomplete. Where this is not a problem, the poor may still lack a connection to the internet or basic digital skills. Finally and importantly, jurisdictions with consumer protection frameworks that are appropriate for the online world (and actually implemented) are still few and far between.

Access also comes with increasing risks: cyber threats are getting more pervasive. As the pandemic accelerates digitalization, the attack surface widens. At the same time, as the value chain of digital financial services becomes more complex, it also becomes harder to supervise, leaving open gaps for malicious actors to exploit.

And it is especially vulnerable groups who bear the brunt of this risk. Covid-19 pushed online low-income households, the elderly, and other demographics where digital literacy is low, without giving them a chance to learn how to fend for themselves in the new environment. Low-income households are also more likely to access digital financial services from cheap and unsafe devices, from unstable networks, or from jurisdictions where data privacy and security frameworks are not well developed.

---

5 The Promise of Fintech: Financial Inclusion in the Post COVID-19 Era. IMF (2020)

6 State of the Industry Report on Mobile Money 2019, GSMA

Conceptually, these risks articulate along two dimension: a macro dimension and a micro dimension, in a complex web of interrelationships that I will take a few minutes to expand upon.

Fleshing out the risk

At the macro level, we have issues that affect all subjects within the same jurisdiction, regardless of their wealth or level of education. The problem here is one of technical and legal infrastructure. On one hand, IT infrastructure might be unreliable, or unsafe. On the other, regulatory frameworks – and enforcement capabilities – might be scarce, or missing.

Make no mistake, while digital financial services can thrive plenty good despite poor technical or legal infrastructure, the economic livelihoods of those that come to depend on them, might not. Lacking adequate safeguards, exposure to such services can be harmful – countless cases of fraud in unregulated new-generation ecosystems, such as Bitcoin, provide the most obvious warning.

The challenge lays in complexity: digital financial services require a diverse set of regulatory backstops to work properly. Different authorities are likely to be involved, and coordination challenges follow.

The first regulatory layer must address network security from a technical standpoint. Most advanced economies have extensive cybersecurity statutes aimed at strengthening core digital infrastructure, which include special provisions for the financial sector. This is not always the case in low-income jurisdictions.

The second layer should guarantee the stability and integrity of the financial system. One may be tempted to believe that digitalization *per se* does not change the game. Alas, this is not always the case. Some digital financial instruments are unlike their physical predecessors in ways and with risks that we still fail to understand completely.

The optimal regulatory framework for large-scale algorithmic lending, for example, is still very much a work in progress.

The third layer must build safeguards for consumer rights that are appropriate for the digital world. Malicious actors can pose as legitimate providers of financial services both offline and online – fraud and other varieties of misconduct, including unlawful exploitation of personal data, existed before the internet. New means, however, amplify the scope and speed of potential abuse, while sometimes making prosecution harder.

The macroscopic issues I have just highlighted are compounded by another set of issues that enter *at the micro level,* or at the edges of financial networks. Regardless of how closely we guard core infrastructure, low-income households face what we may call a "cybersecurity trap": a condition whereby they are disadvantaged from the start. Through no fault of their own, they end up introducing weak spots into the system.

Two elements contribute to the trap. First, the poor only have access to the cheapest devices, which also tend to be the most insecure. Second, they are also likely to lack awareness of security and privacy issues.

Averting risks: the case for public intervention

In the face of these daunting and overlapping levels of complexity, let me start drawing to closure by circling back to my original question. In a world of increasing digitalization of financial services, how do we onboard the vulnerable without saddling them with a host of new risks?

As economists say, let me start from first principles. Finance is tied to trust from the get go – that's why we say that people *entrust* their funds to financial institutions. Hence, we need to guarantee trust in digital financial services.

Trust starts with literacy, is reinforced by strong digital identification and travels through secure networks, devices and applications. Trust is a public good however, and

we know from large body of evidence on market failures that public goods are in structural undersupply.

It might be tempting to dismiss public sector intervention on the grounds of inefficiency and technological backwardness. Some may argue that leading technology companies are extremely efficient, and advanced, and should therefore be trusted to provide solutions in the form of the digital and financial infrastructure, the regulatory framework and the enforcement capacity that we sorely need. The capabilities of these actors, however, are not necessarily supported by the right set of incentives.

So how should we, as the public sector contribute?

At the macro level, we need to double up our efforts in building and supporting safe infrastructure, appropriate regulation and capable regulators. This entails enhanced cooperation, technical support and capacity building.

At the micro level, we have to start thinking how to harden the disadvantaged against new risks. Digital and financial education programs can go a long way in teaching how to avoid the most common pitfalls: we need to work together to develop a culture of cyber hygiene, first and foremost aimed at preventing online financial fraud.

At the same time, as digital business models come to rely on massive-scale data collection and monetization, financial education also needs to impart an understanding of the value of personal information. Users of digital financial services must know what their data rights are, and they must become the first line of defence against data abuse. Mitigating privacy risks for individuals eventually results in lowering security risks for entire countries.

Literacy and empowerment can go a long way, but not all the way. We also need to lay the groundwork for minimum agreed-upon device and app security standards. The guidelines for mobile security published by the European Union Agency for

Cybersecurity (ENISA) and the United States' National Institute for Standards and Technology (NIST) provide a useful starting point.

In doing this, we need to work together. Cybersecurity in financial services, and particularly in financial services for the more deprived, lies within the purview of four different communities – cyber experts, financial regulators, diplomats, and development agencies.

As the recently launched Carnegie Endowment's International Strategy to Better Protect the Financial System Against Cyber Threats clearly points out, however, there is a fundamental disconnect between such communities. While numerous actors count elements of this realm within their jurisdictions, it is central to none of them, with the result that the cybersecurity aspect of financial inclusion is often neglected.

The Italian presidency of the G20 and the GPFI

The GPFI and the Italian G20 Presidency are aware of this.

Setting Digital financial inclusion and SME finance as GPFI priorities for the years 2021-23, the overarching themes of the Italian G20 Presidency can be captured in three words: People, Planet, and Prosperity.

During the Italian G20 presidency, our work within the GPFI will be devoted to identifying and understanding the gaps in financial inclusion caused, or worsened, by the unfolding crisis, while developing a menu of options for a more inclusive and resilient society.

Our work will articulate in two complementary areas of intervention. The first is related to increasing digital and financial awareness and competences of individuals and firms (possibly also through digital means). We believe these are essential tools in fostering people's empowerment, active citizenship, financial inclusion, resilience and well-being. Households and businesses with higher financially literacy will be better able to cope with the income strains associated with crises, will be more resilient.

The second area of intervention is related to a more "inclusive" regulatory and supervisory framework, aimed at encouraging the development of inclusive and responsible digital financial services, while granting adequate protection to final customers, not least from cyber risk. What are the most effective approaches in terms of consumer protection to ensure digital financial inclusion? Again, digital instruments might be of help for supervisors as well.

We have the opportunity to build on a number of prior commitments and achievements, both at the international and at the domestic level.

Concluding remarks

While the opportunities that digitalization bring us should not be missed – we also need to ensure not to be saddled with the downsides of a mismanaged digital transition. I strongly believe that digital and financial literacy are key in fostering a responsible use of digital financial services by all individuals and firms, especially the most vulnerable ones. Education and awareness are a very strong shield against many risks that an increased digitalisation of services poses, not least cyber risk. At the same time, authorities should ensure that the regulatory and supervisory environment is fit for purpose to deal with all challenges digitalisation poses. The best practices that we aim for as deliverables of the Italian Presidency will hopefully help in this regard, by providing a menu of policy options, especially for developing and emerging counties.

Moreover, the GPFI will continue to engage with all relevant stakeholders and standard setting bodies to strengthen cyber risk policies that take into account also the needs of the most vulnerable and underserved to foster financial inclusion.

I thank you for your kind attention, and look forward to the discussion.