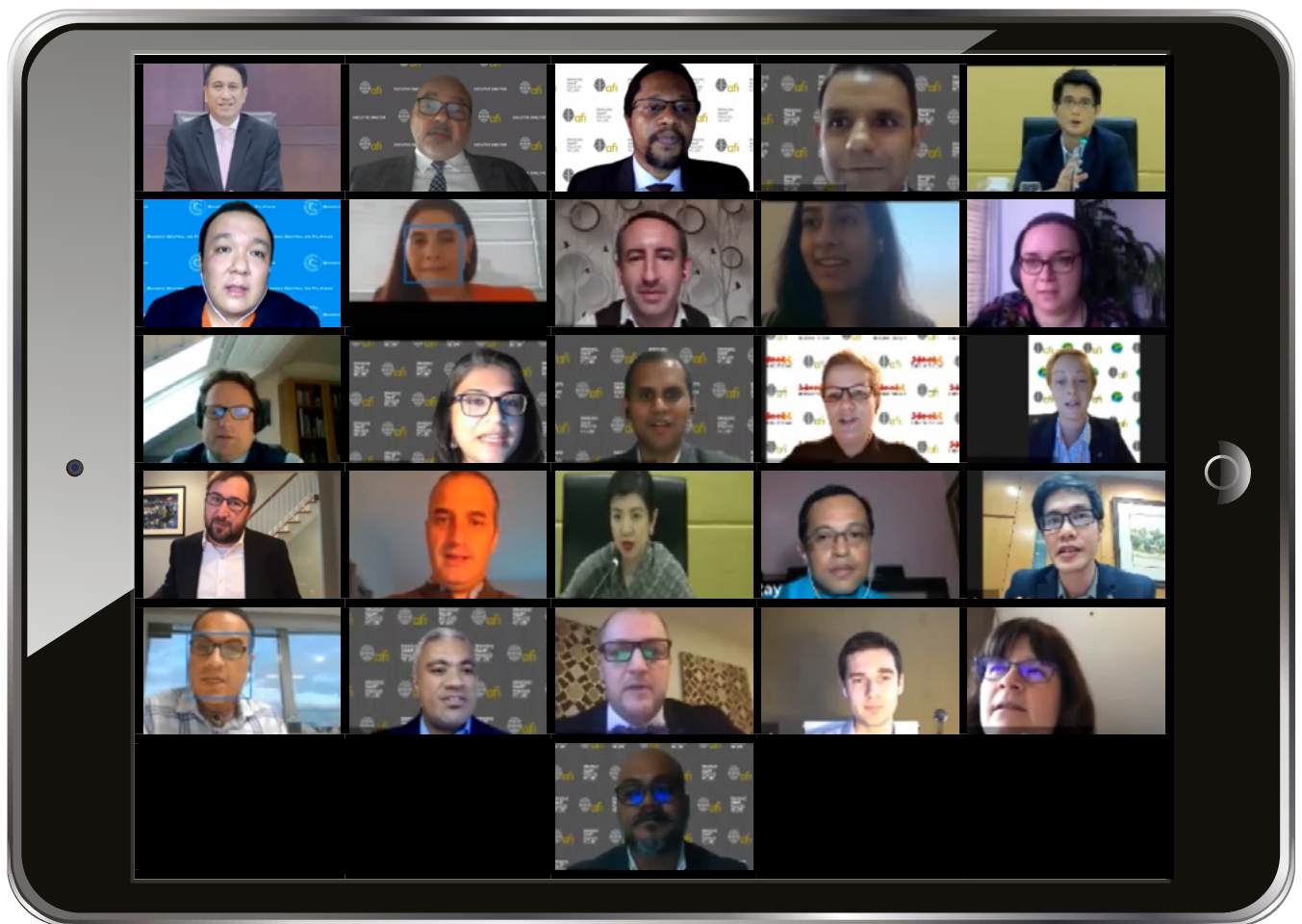




BANK OF THAILAND

# HARNESSING THE POTENTIAL OF FINTECH IN DEEPENING FINANCIAL INCLUSION: PRACTICAL REGULATORS EXPOSITIONS

1-3 December 2020



In partnership and participation of



BANK NEGARA MALAYSIA  
CENTRAL BANK OF MALAYSIA



COMISIÓN NACIONAL  
BANCARIA Y DE VALORES



中國人民銀行



Bank of Russia



បណ្ណាគារជាតិ កម្ពុជា  
NATIONAL BANK OF CAMBODIA  
Risk. Stability. Development.

WORKSHOP REPORT

# CONTENTS

BACKGROUND	3
OBJECTIVE	4
REPORT SUMMARY OPEN BANKING AND OPEN API	4
OPENING REMARKS:	8
Ronadol Numnonda (Deputy Governor, Bank of Thailand)	8
Alfred Hannig (AFI Executive Director)	9
CONTEXT AND OUTLINE OF PROGRAM	11
SESSION 1: STATE OF OPEN BANKING AND OPEN API	12
SESSION 2: OPEN BANKING AND OPEN API: OVERCOMING IMPLEMENTATION CHALLENGES	21
SESSION 3: OPEN BANKING AND OPEN API: REGULATORY APPROACHES	25
SESSION 4: THE ROLE OF DFS IN ADDRESSING THE IMPACT OF COVID-19	31
SESSION 5: IMPACT OF COVID-19 ON SDGS AND KEY RISKS IN COVID-19 DIGITAL FINANCIAL TRANSFER	40
SESSION 6: STATE OF E-KYC AND DIGITAL ID	43
SESSION 7: E-KYC AND DIGITAL ID: REGULATORY APPROACHES AND INNOVATION	51
WAY FORWARD: KEY POLICIES AND REGULATORY LESSONS, KEY ACTIONS AND SUPPORT	60
APPENDIX: AGENDA	61

## ACKNOWLEDGMENTS

This product is a deliverable under the Digital Financial Services & FinTech workstream.

Authors and contributors from AFI:

This report was developed and led by Jaheed Parvez (Technical Specialist), with contributions from Ritesh Thakkar (Senior Manager, EECA & Asia Region).

This report builds on knowledge exchange co-hosted by Bank of Thailand, in partnership and participation of AFI member institutions: Bank Negara Malaysia, Bangko Sentral Ng Pilipinas, Comisión Nacional Bancaria y de Valores, The People's Bank of China, Bank of Russia and National Bank of Cambodia.

We would like to thank AFI member institutions, partners and donors for generously contributing to development of this publication.

The knowledge exchange program was partially funded with UK aid from the UK government.

## BACKGROUND

Alliance for Financial Inclusion (AFI) member countries represent diversity in terms of geography, socioeconomic development, cultural context, and levels of financial inclusion. This necessitates a focused regional and country-based approach in coming up with policy solutions to address financial inclusion challenges. Member countries in their financial inclusion journey have complex challenges and priorities to be addressed and need innovative policy responses to advance their financial inclusion objectives.

Knowledge Exchange Program-2, organized jointly with the Bank of Thailand (BoT) was a follow-up to the first Knowledge Exchange Program organized in November 2019 in Malaysia. The Knowledge Exchange Program was originally conceptualized from the demand of AFI member institutions for a platform of cross-learning among the member institutions who have similar context, interest and priorities for developing policy actions on specific topic and issues through AFI's unique peer learning platform which supports in developing practical policy interventions.

Knowledge Exchange Program-2 facilitated cross-learning among participating member institutions on e-KYC and Digital ID, Open Banking and Open API, and Data Privacy and Protection. It focused on sharing learnings and experiences between developing and developed country financial regulatory policy-making institutions.

Knowledge Exchange Program-2 is aligned with the Sochi Accord on FinTech for Financial Inclusion, adopted by the AFI Membership in September 2018.<sup>1</sup> The accord calls for systematic dialogue among peers in developing and emerging countries as well as developed economies, showcasing policy learnings on issues of high shared priority, which include e-KYC processes and Digital ID. The 2020 event built on the outcomes of its inaugural edition of 2019, itself a follow up to the Prague on Global Dialogue on Regulatory Approaches for Inclusive Fintech, where Enabling FinTech Ecosystems was identified as one of the key areas of priority in the global 3D Workstream.<sup>2</sup>

---

1 Sochi Accord - FinTech for Financial Inclusion - Alliance for Financial Inclusion  
2 Global Dialogue on Regulatory Approaches for Inclusive FinTech

## OBJECTIVE

The overall objective of Knowledge Exchange Program-2 was to develop shared insights and knowledge on practical policy solutions to issues related to creating Enabling FinTech Ecosystems and the different approaches applied by developing and developed country financial regulators for Financial Inclusion.

Specifically, Knowledge Exchange Program-2 was organized to help member institutions to:

- > Develop a better understanding of the regulatory landscape from various jurisdictional contexts and peer exchanges for practical adoption of best practices on Open Banking and Open API.
- > Develop a better understanding of the regulatory framework to enhance implementation of practical policy solutions for Digital Identity Systems and e-KYC.
- > Equip member institutions with knowledge, best practices and standards in data privacy and protection laws, regulations, compliance frameworks, and needed collaboration with other relevant authorities (i.e. Competition and Data Protection authorities) in the changing landscape of Digital Financial Services.
- > Enhance the knowledge of member institutions for devising practical solutions to mitigate the impact of emergencies such as COVID-19 and potential solutions that can be considered in the pandemic's recovery phase by policymakers.

**Output:** Knowledge Exchange Program-2 is a platform for participating AFI member institutions and their financial regulator peers from developed countries to share knowledge and experiences to enhance capacity on innovative and enabling policy environments for Digital Financial Inclusion and, more particularly, for Enabling FinTech Ecosystems.

The event's key insights are synthesized in this report, presenting the key practical policy solutions discussed by the AFI member institutions and developed country financial regulatory institutions.

**Outcome:** The knowledge gained from participating in Knowledge Exchange Program-2 will be used to enhance existing policy solutions and the development of new policies in specific areas by participating member institutions.

## REPORT SUMMARY OPEN BANKING AND OPEN API

### DAY 1: OPEN BANKING AND OPEN API

#### SESSION 1: STATE OF OPEN BANKING AND OPEN API

- > This session gave an overview of Open Banking and Open API initiatives in Thailand, Philippines and Mexico.
- > Third-party service providers are disrupting the financial sector with digital financial services, posing hard questions to regulatory and supervisory authorities on their traditional roles.
- > Carefully designed Open Banking solutions can help overcome the challenges of limited access and usage of formal financial services provided by banks and non-bank financial institutions (NBFIs).
- > Open Application Programming Interfaces (APIs) enable third-party service providers to access customer transaction data of banks and NBFIs, which helps banks and NBFIs to better understand customers' financial behaviors and design appropriate products for them.
- > The API standard is thus a key enabler for the efficient, secure and cost-effective flow of data without which DFS cannot function.
- > Underlying Open Banking is the concept that customers own their financial and transaction data. Thus, this data should be shared only if the customers agree.
- > Open Banking also supports innovation by promoting competition in the market.

#### SESSION 2: IMPLEMENTATION CHALLENGES OF OPEN BANKING AND OPEN API

- > This session focused on how to leverage Open Banking initiatives to achieve financial inclusion. It showcased the experience of the UK, one of the first countries to have an Open Banking regime, for others to learn from its successes and challenges.
- > The UK adopted Open Banking after nine of its largest banks agreed to give authorized third-party providers (TPPs) access to personal financial data of customers who had consented to it.

- > The UK Competition and Markets Authority initiated Open Banking in February 2017 as part of its Retail Banking Market Investigation to increase competition.
- > The Open Banking Implementation Entity (OBIE) creates and maintains the Open Banking Standard and the Open Banking Directory, and monitors the nine banks involved.
- > OBIE provides implementation support for both banks and TPPs seeking to implement Open Banking standards.
- > Notably, OBIE prescribes user experience standards and operational guidelines in addition to technical standards.
- > The UK has three types of Open Banking business models: consumer products, business products and technical services (provision of software to help firms implement Open Banking APIs).
- > Two-thirds of UK consumers (in a June 2020 survey) had not heard of Open Banking; and less than eight percent viewed it as a good idea.
- > The majority were concerned about privacy, data loss or fraud. There must be greater industry clarity and action on security, privacy, accountability (in cases of data breach), and liability for loss.

## DAY 2: OPEN BANKING AND OPEN API

### SESSION 3: REGULATORY APPROACHES TO OPEN BANKING AND OPEN API

---

- > This session presented the European Union's experience of regulating Open Payments and Open API, as an incremental step toward Open Banking and then Open Finance.
- > The European Banking Authority approaches the regulation of Open Payments to further the goal of a single EU market for its 27 Member States: a level playing field, and equal levels of competition for all entities.
- > The EBA adopts guidelines and recommendations with a view to promoting the safety and soundness of markets and convergence of regulatory practice.
- > Open Payments is the only sector covered by the EU's Revised Payments Services Directive (PSD2) by which the EBA prescribes regulatory requirements for DFS related to Open Payments.

- > This specific (Open Payments only) legal approach rather than market self-regulation was necessary because of the sheer number and diversity of banks and third-party providers (TPPs) across the EU region.
- > TPPs are allowed to access only information related to payments accounts in respect of payment initiations or payments account information.
- > Some of the objectives of PSD2 necessarily compete with one another, and there is a need to strike a balance between them.
- > Innovation is assumed to encourage market competition for the best solution for the consumer: the most cost-efficient and user-friendly solution eventually survives competitive pressures.
- > Notably, financial inclusion was left out as an objective of PSD2 because the overall rate of financial inclusion is very high among EU member states and increases yearly.
- > To mitigate the challenges of greater competition, EBA has set up an Industry Working Group on APIs comprising nine banks, nine TPPs, and nine API scheme providers to present their viewpoints and seek clarifications, which are published.

### SESSION 4: THE ROLE OF DFS IN ADDRESSING THE IMPACT OF COVID-19

---

- > This session considered a broader view of DFS and weighed what a "better normal" post-COVID-19 scenario means in practice for financial inclusion.
- > Three perspectives could help inform recovery policy and frameworks — digital finance, gender-inclusive finance, and inclusive green finance.
- > The Philippines introduced a regulatory framework in 2009 to catalyze innovation and manage the associated risks founded on a robust digital infrastructure, digital skills, digital ID, and an enabling regulatory framework.
- > The Philippines' Digital Banking Exposure Draft approved in 2020 creates a distinct 'digital bank' category.
- > The national ID system (PhilSys) will enable Filipinos to access and utilize innovative digital financial products and services.
- > AFI's policy framework response to COVID-19 has seven pillars:
  - Promoting and incentivizing digital payments.
  - Secure and resilient digital payments and technology infrastructure.



- Enabling regulations (consumer protection, data privacy and digital financial literacy for those with increased vulnerabilities).
  - Regulations for responsive risk-mitigating innovations.
  - Agent and merchant operations ('last mile' transactions).
  - Facilitation of additional use cases (e-money, mobile money, online and offline payments).
  - Coordination among stakeholders.
  - Cross-cutting issues (environment, renewable energy for small businesses and individuals; assistance for women and other vulnerable groups).
- > Global financial inclusion gender gap: nearly a billion women remain financially excluded.
  - > In developing countries, the financial inclusion gender gap of nine percent has persisted since 2011.
  - > Advancing women's equality could add an estimated USD12 trillion to global GDP by 2025.
  - > Barriers include socio-cultural factors, lack of gender-sensitive policies, limited ownership or control of mobile technology, inadequate access to digital devices, and limits in financial literacy/capability.
  - > The lack of sex-disaggregated data hampers understanding of the true socio-economic impact of COVID-19 on women.
  - > A fully inclusive and gender-sensitive financial system must account for
    - Regulatory institutions.
    - MSMEs.
    - SME guarantee schemes.
    - Social Protection.
    - Gender-sensitive regulatory and legislative frameworks.
    - Gender-sensitive National Financial Inclusion Strategies.
    - Women's financial literacy strategy and national strategies for financial education.
  - > AFI's '4P' policy framework of inclusive green finance can be used for COVID-19 recovery (Provision, Protection, Prevention, Promotion).
  - > Disaster Risk Reduction policies (DRR) and emergency preparedness measures can provide a relative safety net for financial institutions that can enable them to help clients resume their economic activities.

- > The COVID-19 crisis can provide lessons for designing future DRR policies and responses to national disasters linked to climate change.
- > The two notable examples from the AFI network to date of a greening of the COVID-19 response include: the Green Transformation Fund of Bangladesh Bank and Bangko Sentral ng Pilipinas' Inter-Agency Working Group.
- > The Go Green Inclusive Financing Program of the Land Bank of the Philippines, while not COVID-related, is a concrete example of MSMEs linking together the inclusive, recovery and green elements.
- > Greening the COVID-19 response is not an act of charity; there is a clear business case for it.

## SESSION 5: IMPACT OF COVID-19 ON SDGS AND THEIR RISKS FOR DFS TRANSFER PROGRAMS

---

- > This session explored how advances in DFS can enable governments to mitigate the adverse effects of COVID-19 and sustain progress towards the 2030 agenda.
- > It also highlighted risks that have emerged in the DFS sphere during the pandemic, specifically in the use of digital transfers for vulnerable segments.
- > Financial inclusion is not a goal in itself but an opportunity to improve overall human and social development.
- > There is a growing base of evidence of how DFS has been used as a means for achieving better social and economic outcomes.
- > An MIT study found that the spread of mobile money in Kenya lifted roughly one million people out of extreme poverty from 2008-2014, equivalent to two percent of the population.
- > The Indonesian experience of digital finance inclusion saw 1.4 million recipients under the subsidized rice program move out of extreme hunger.
- > In Bangladesh, mobile money managed to get enough community health agents to register a million new mothers for maternal and health programs.
- > There is scope to document the progress in relation to financial inclusion targets, including through the Sustainable Development Goals reporting process for every country.
- > AFI members can encourage national bodies to report on financial inclusion indicators.

- > The Fintech and Digital Payments Office of the UNSGSA has collaborated with Better than Cash Alliance and the World Bank to publish a compendium of how DFS supports the progress of 13 of the 17 SDGs.
- > While there are many challenges with utilizing DFS and digital platforms, they can play key roles in supporting social and development outcomes related to education, health and work.
- > The pandemic has created a situation where making social welfare payments via digital means was not only good for inclusivity but essential given the challenges of limited mobility.
- > There are seven major risks and solutions that have been or could be implemented to address them:
  - Inadequacy of complaints feedback mechanisms.
  - Risk of financial and digital illiteracy.
  - Exclusion of either current beneficiaries under a cash program, or potential beneficiaries.
  - High transaction failure rates.
  - Lack of knowledge or information about the nearest cash help-point.
  - Overcharging fees for cash-out and transactions.
  - Overcrowding and health and safety risks at cash-out points.

### DAY 3: STATE OF E-KYC AND DIGITAL ID

#### SESSION 6: STATE OF E-KYC AND DIGITAL ID

---

- > Digital disruption of the financial sector is driving increased choice for consumers around the world and changing their behavior.
- > An increasingly customer-centric regulatory agenda is compelling institutions to leverage new technologies to give customers more control over their data and identity in the digital economy.
- > For a truly integrated digital ecosystem to work, businesses and individuals must be able to seamlessly navigate across ecosystems without repetitive authentication processes.
- > Developing efficient and effective e-KYC systems is a common industry objective and formidable regulatory challenge.
- > Harmonizing industry standards with risk appetites for new technologies is a frequent stumbling block to industry-wide KYC initiatives.

- > Providing a cross-industry, cross-sector, verified and enriched digital ID would eventually provide the foundation of a trust network in which customers participate and control their own data.
- > Such access to simplified digital products and services will be the key enabler to digital transformation.
- > Market players must adjust to a digitally enabled economy and regulators need to provide better outcomes for customers and manage the risks of a new ecosystem appropriately.
- > Thailand, Philippines, Malaysia and Mexico presented on their respective national ID schemes and the challenges processes by which they arrived at their regulatory approaches based on national priorities.

#### SESSION 7: REGULATORY APPROACHES TO E-KYC AND DIGITAL ID, AND INNOVATION

---

- > This session presented a detailed look at regulatory approaches used in the highly developed jurisdictions of Estonia and Luxembourg, and some flagship digital initiatives.
- > It also considered private sector perspectives of e-KYC regulations.
- > The presentations highlighted the importance of shifting mindsets and achieving buy-in to embark on, and roll out a sophisticated, national-level project with regional potential.
- > Matching organizational capacity with regulatory requirements is essential for engaging with private sector stakeholders.
- > In addition to AML/CFT standards, consumer protection, data privacy and security must be considered for e-KYC and digital ID.

TUESDAY, 1 DECEMBER 2020  
DAY 1 - OPEN BANKING AND OPEN API

## OPENING REMARKS

RONADOL NUMNONDA  
DEPUTY GOVERNOR, BANK OF THAILAND



After extending a warm welcome to the Alliance for Financial Inclusion's (AFI) Second Knowledge Exchange Program, the Deputy Governor of the Bank of Thailand commended AFI's efforts in continuing to build on the success of previous year's inaugural edition to facilitate vibrant conversations between member countries committed to shaping the future of financial inclusion. He thanked AFI and all the speakers for taking time out of their busy schedules to share new insights and experiences before saying a few words on the subject at hand.

Financial inclusion has always been at the forefront of policymakers. Technological advances and innovation account for the rapid changes in the current landscape have resulted in smart access and use of financial services. Ultimately, it is hoped, this will engage more people, particularly those under-served, to use financial services in a smart and cheaper way. To ensure that in moving forward it leaves no one behind, the Bank of Thailand sees FinTech as one of the building blocks with social and economic potential to become a force for good. The pandemic has changed customer behavior and hastened the adoption of technology-based services – there was an unprecedented growth of 85 percent in electronic payments and fund transfers in May 2020 – thus providing great opportunities for FinTech and Digital Financial Services (DFS).



In Thailand, such changes in demand and behavior were met by PromptPay, the national digital payment infrastructure launched a few years ago (which enables the receiving and transfer of funds using the citizen ID or mobile phone number). This allowed for the integration of DFS, particularly in government economic recovery programs, in the form of e-wallets targeting those affected by Covid-19. Roughly 10 million individuals were able to register online instead of having to be present at a government office, and subsidies were disbursed through e-wallet using e-KYC to complete registration and the opening of accounts.

The private sector and relevant parties have also worked on digital ID. Once this is fully developed, it will enable accounts to be opened through the secure National Digital ID platform<sup>3</sup>. These are some examples of how FinTech can be harnessed to assist people to conduct financial transactions without physical contact or leaving their homes, thereby achieving public health and personal hygiene whilst enhancing greater financial inclusion.

In pursuing DFS, equal emphasis must be paid to both the front- and back-ends. While the front-end of user experience and convenience play an important role in the widespread adoption of DFS among the public, the back end of integration and need for the development of standards should not be neglected, hence the focus on Open Banking and Open Application Program Interface (API) in this meeting. The infrastructure for digital services should be utilized to benefit consumers within a secure ecosystem.

There must be active cooperation from a broad range of stakeholders to ensure effective implementation, regulatory oversight, and the prevention of market fragmentation. The potential in financial innovation is huge but there have also been repeated cases of data breach and mis-selling of products and services often targeting the most vulnerable. Financial and digital literacy are the crucial enabler in deepening financial inclusion further.

**ALFRED HANNIG**  
EXECUTIVE DIRECTOR, AFI



The AFI Executive Director thanked the Deputy Governor and the Bank of Thailand for being a co-host of this second edition of the Knowledge Exchange Program (KX-2). He also acknowledged the bank's leadership and its role as a co-founding member of this platform together with the Bank of the Philippines and Bank Negara Malaysia.

The original idea for this platform, however, was generated by the Central Bank of Russia two years ago. After cultivating this further, it has reached the stage of having a systematic program. The Executive Director also acknowledged the participation of the People's Bank of China, the Comisión Nacional Bancaria y de Valores (Mexican banking and securities regulator), the Central Bank of Russia, and the National Bank of Cambodia.

<sup>3</sup> Thailand's National Digital ID (NDID) is the common, open and interoperable e-KYC platform that connects the parties to an e-KYC transaction in order to share information for identity verification and authentication.

Members of the AFI network are diverse in terms of geography, socio-economic development, cultural contexts, and levels of financial inclusion. Different approaches are thus required to devise policy solutions that address financial inclusion challenges in various jurisdictions. There are also some at different stages of the financial inclusion journey, some with more complex challenges and different priorities. Others are looking for very specific innovative policy responses to advance their financial inclusion objectives even further. There are also numerous requests for tailored exchange programs by AFI member institutions to learn from the experiences of other members.

It is in everyone's interest that financial inclusion moves forward. This is not just a developed country issue, it is an issue everyone is grappling with. On the one hand, there are efforts to enhance access, usage and quality of financial inclusion; on the other, there are countries focused on maintaining high levels of financial inclusion. The further along in this journey, the more the need to address demand-side issues around digital literacy, financial literacy, and the protection of consumers. The agenda is complex, and what brings everyone together is this convergence, a common understanding of solutions, challenges and commonalities.

Financial inclusion is the common denominator, and this is true within and outside the AFI network. AFI has co-created this program for members to learn and share on country-specific challenges. The Knowledge Exchange Program takes a thematic policy approach on Digital Financial Services (DFS) led by participating member institutions, as well as invited stakeholders and external knowledge partners who are experts in the field. The second edition of the knowledge exchange program has two main themes: the first is on Open Banking and Open API regulatory approaches and solutions to overcome implementation challenges; the second is on e-KYC and digital ID focusing on the current state, innovation and regulatory approaches.

This program follows on from the Sochi Accord: FinTech for Financial Inclusion, adopted by the AFI membership in September 2018, which calls for a systematic dialogue among peers in developing and emerging countries, as well as developed economies, showcasing learnings and policy issues, including digital KYC processes and biometric ID. It is also a follow-up to a global dialogue on regulatory approaches for inclusive finance held in Prague in 2019. This program here is even more relevant given that the Covid-19 pandemic has forcibly sped-up learnings related to DFS and regulatory solutions. As mentioned, the government's

implementation of social distancing in Thailand resulted in a tremendous uptake of DFS.

Learning since the last financial crisis in 2007/8 when financial institutions deemed too big to fail had to be rescued by public interventions, the financial sector today is far better capitalized and in a stronger position to survive and actively contribute to an inclusive recovery. This confidence comes from all the learnings, especially on the technology front in the past ten years. Financial inclusion is one of the ways to mitigate the impact of Covid-19, to build recovery and resilience. Solutions must be based on previous learnings.

Peer-to-peer (P2P) engagement is a valuable core of AFI services. It involves Technical Working Groups, capacity-building events, peer learning, exchange advisory, and in-country implementation program. From these, first data has been collected on how countries are responding to the pandemic. There is a Covid-19 policy response dashboard, webinars, publications, and enhanced support for countries through tailored interventions of in-country implementation activities. Given the digital transformation of member countries and the current pandemic context, innovative DFS solutions will be key to enhancing the usage and quality dimensions of financial inclusion.

This Knowledge Exchange Program is expected to provide an important platform for AFI member countries and peers and financial regulators from developed countries to share knowledge and experiences to enhance the policy environment for financial inclusion and enabling FinTech ecosystems.

TUESDAY, 1 DECEMBER 2020  
DAY 1 - OPEN BANKING AND OPEN API

## CONTEXT AND OUTLINE OF THE PROGRAM

### MODERATOR

**KENNEDY KOMBA**  
DIRECTOR, STRATEGY &  
FINANCIAL INCLUSION POLICY,  
AFI



The participants were taken through the agenda and provided with the background for the second edition of the Knowledge Exchange Program, a collaboration between the Bank of Thailand and AFI in a practical regulators' exposition to facilitate peer exchange, including practical solutions around FinTech and DFS on the themes of Open Banking and digital ID and e-KYC.

This was a follow-up to the 2019 Knowledge Exchange Program hosted by Bank Negara Malaysia, and before that, the 2018 Sochi Accord, the 2019 Prague global dialogue, and the 3D initiative of AFI that brought together regulators from developing and developed countries to discuss convergence topics.

The program aimed at surfacing practical insights based on regulatory and policy solutions so that peers could create enabling environments for FinTech ecosystems in their respective countries. It would showcase the different approaches of developing economies, developed country regulators and other field experts invited. Its specific objectives were to generate a clearer understanding of the landscape for peer exchange of best practices, tools, and regulatory supervisory frameworks on the two main pillars (Open Banking and APIs, digital identity systems and e-KYC). Attention would especially be given to data privacy and protection, and mitigating the impact of Covid-19 on financial inclusion through recovery measures. The intended output was a cross-pollination of ideas and coming up with practical solutions that could be contextualized or made country-unique.

This rich exchange, including the practical discussions that emerge, would be captured in a report. This was expected to serve as a systematic reference point for translating the solutions discussed to realities on the ground. The report would also contain new insights that are technical and practical for regulators to pilot and introduce as programs to enhance FinTech in their countries.

The presentation concluded with an outline of the three-day program where Day One focused on overcoming implementation challenges of Open Banking and Open APIs, Day Two on regulatory approaches, and Day Three on e-KYC and digital ID.

TUESDAY, 1 DECEMBER 2020  
DAY 1 - OPEN BANKING AND OPEN API

## SESSION 1: STATE OF OPEN BANKING AND OPEN API

### MODERATOR

**JAHEED PARVEZ**

Technical Specialist, Alliance  
for Financial Inclusion, AFI



Broadly, financial inclusion is about access to appropriate, affordable financial products and services. Evidence shows that carefully designed Open Banking solutions can help overcome the challenges of limited access and usage of formal financial services.

This is done by enabling third-party access to transaction data, which in turn helps financial institutions to better understand customers' financial behavior and design appropriate products for them. Open Banking also supports innovation by promoting competition in the market. The first session gave an overview of Open Banking and Open API initiatives in Thailand, Philippines and Mexico.

## STATE OF OPEN BANKING AND OPEN API: THE CASE OF THAILAND

**THAMMARK MOENJAK**

Director, Financial Institutions  
Strategy Department,  
Bank of Thailand



The Bank of Thailand (BoT) responded to the digital disruption of the financial sector by asking itself two questions: "What can we do as a regulator?" and "What should we do as a regulator?". Its previous focus on ensuring stability at all costs was no longer tenable in this new financial landscape. As such, it identified four guiding principles to support its vision of banks and non-banks leveraging the power of data and technology to serve customers with personalized financial services in a timely manner. This goal is still subject to financial stability, competitiveness, and customer protection requirements.

The four principles guiding the BoT's approach to the new financial landscape including what it does with Open Banking and API standards are:



1. **Customer centricity.** Encourage mass personalization of financial services via the use of financial and non-financial data such that these services are available to all segments of society.
2. **Financial stability.** Since there will be banks and non-banks competing, there must be proportionate supervision. Non-banks (which might fall outside the remit of BoT) are unable to be regulated to the same degree as banks.
3. **No anti-competitive behavior.** There must also be a level playing field given the different sizes and types of market players. Promoting this can prevent potential abuse of market power. For example, new players like FinTech platforms have less customer data than traditional banks.

#### 4. Market conduct and consumer protection.

To protect and educate customers new to DFS about their rights, including their right to privacy.

Regulations alone may not suffice if customers are to be well-served. There also needs to be digital and financial infrastructure where data sharing is key to financial services that can be personalized to different segments of the market. Thailand's digital financial ecosystem, the 'Thailand Stack', is built upon a vertical integration model that has three layers of infrastructure, each with enabling initiatives (see slide for illustration).

At the lowest layer is 'digital identity', important for on-boarding customers to the digital world, and subsequently letting them transact on financial platforms. For instance, once they are on-board the banking system, they can transact on financial platforms (the second layer) like PromptPay, a faster payment service that connects banks and non-banks through a mobile number. These transactions will also generate data which, with customer consent, can be stored and shared among financial institutions to provide customers with better products and services.

One initiative under this 'data storage and sharing' layer is the development of API standards. This is needed to generate more efficient competition and data usage, and relies on data portability.

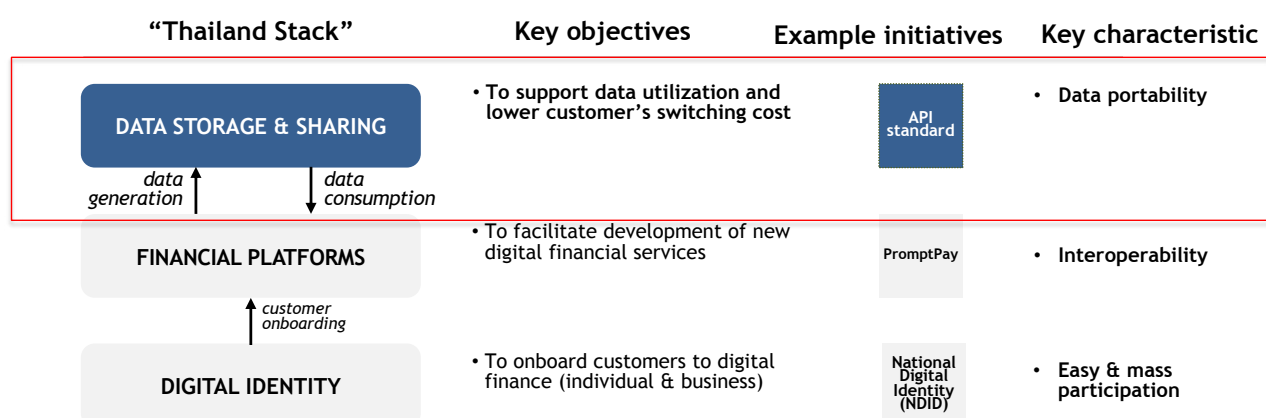
In a digital world, it is important for data to flow such that financial service providers can better fulfill the needs of customers in a personalized, timely and cost-effective manner. APIs that meet certain standards – cost-effectivity, reliability, automation, security, privacy, efficiency, speed – are the best ways to move data around. They serve the customer better because once data is machine-readable, it can be analyzed and shared seamlessly among financial services providers and offers can be made in real-time.

Customers would enjoy individualized and better quality products at a lower price, while providers would have reduced operating costs. Data sent through APIs are also more secure than the usual PDF mode which carries privacy and security risks.

The API standard is thus a key enabler for efficient, secure and cost-effective flow of data.

### Data sharing is one of the key engines in our drive towards digital finance.

Thailand's 'digital financial ecosystem' is built upon a 'vertical integration' of the 3-layer infrastructure that consists of several enabling initiatives.





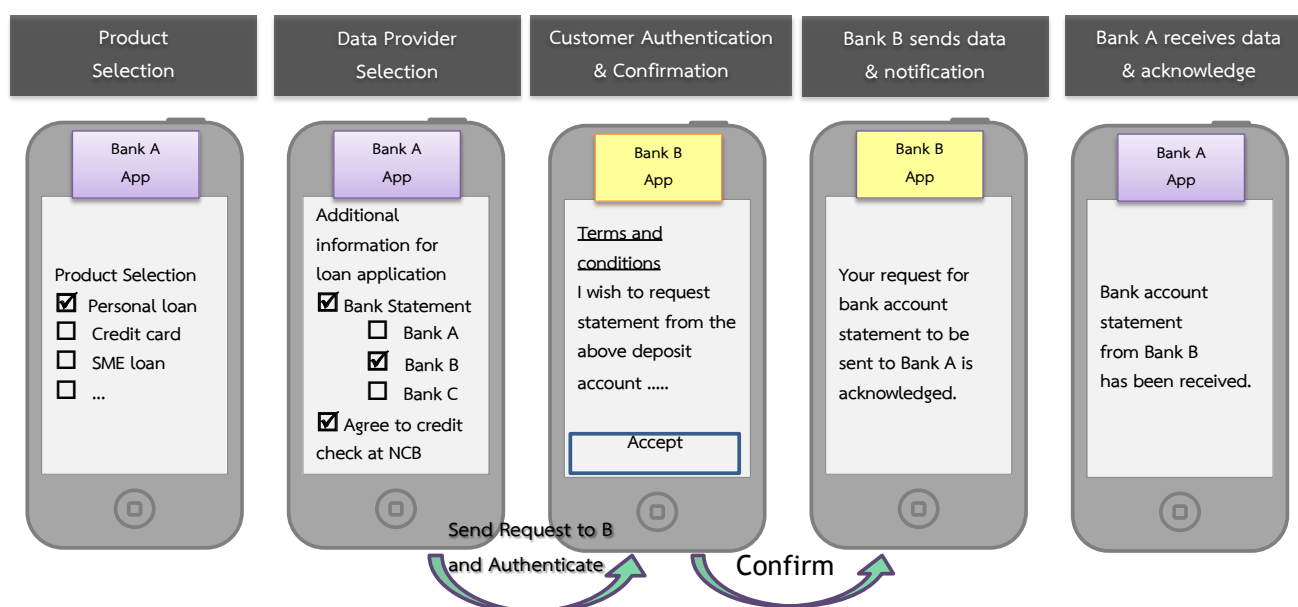
Financial institutions in Thailand understand that APIs are the future, so they have been competing to develop this for their market activities. However, it was clear from their feedback that they wanted the BoT to come in as a regulator to avoid market fragmentation given all the existing banks and non-banks would develop their own API standards for sharing data. A good way to think about developing APIs is the electricity plug example where different countries use different plug heads. Like with having many APIs, this creates duplication of resources and inefficiencies in usage.

The BoT is still quite a young player in the Open Banking industry. Unlike other countries that have mandated financial institutions to abide by certain API standards or allowed financial institutions to set theirs, it has not issued any Open Banking regulations. Banks were initially reluctant, fearing that they may lose their market share if there were common API standards and customers could freely switch from one provider to another. In the end, the BoT adopted a “think big, start small” approach to regulation. Based on ‘pain points’ identified by the banks, it stepped in to facilitate the design of an API for bank statements as well as its accompanying business rules.

This was chosen as the first-use case for a common API standard because in Thailand, bank statements are often used for financial services applications such as loans, as well as non-financial services like visa applications. Typically, one would request these at a certain branch. This involves a lot of manual work, including printing hard copies and then keying in the data from the statement into the system by an officer at another bank. This also carries the risk of fraud. For this process, the BoT invited different banks to a design thinking workshop and separated them into groups with a mix of technical and business representatives. One of the designs produced was for loan applications on a mobile banking app (see slide illustration, below). This showed how data could be sent in a more efficient, secure and safe manner.

A common API standard for bank statements will help pave the way for Open Banking, but there remain many challenges. The BoT does not want to take a strong stance on matters like business rules as it prefers the market to propose solutions.

### Example customer journey from Design Thinking Workshop





Still, there are four areas to consider as a regulator:

1. **Governance body and its composition:** APIs need ongoing development, maintenance and updating for more use cases over time. This calls for a governance body that is not only responsible and accountable for this but also oversees further coordination for different users.
2. **Participants of data sharing schemes:** APIs that have been developed to common standards should be used by as many and as diverse financial institutions as possible so customers may find the best and most suitable product or service for themselves. However, bank and non-bank actors have different reservations about participating. Established players have a larger customer base while newcomers may have more up-to-date technology and experience with it. Balancing these interests and ensuring fairness alongside safety is thus critical.
3. **Pricing and cost:** Financial institutions have to set up systems and reconfigure this so they can comply with new API standards. This involves costs that could be fixed or variable, or an opportunity cost given the risk of losing customers since their data can be easily migrated.
4. **Role of the central bank:** Currently playing a facilitating role, the BoT will need to consider other roles including as a catalyst, champion or judge if it is to advocate for common API standards to ensure their widest adoption.

The BoT follows four principles in designing business rules. These correspond to the guiding principles highlighted earlier. One, customers are data owners (customer centricity); two, consent must be given to share customer data, and compliance with data privacy laws is a must (customer protection); three, a prerequisite for participation of market players is reciprocity including mutual access to customer data (fair competition, level playing field); and four, security standards cannot be compromised (stability of the financial system).

## OPEN Q&A SESSION

**Question 1: Did the Bank of Thailand create the API standard and mandate it, or was it industry-driven?**

A: When the BoT asked stakeholders about the state of APIs, they said that if the BoT did not step in, the market for APIs would be very fragmented. At this point, the BoT decided to intervene but not to mandate

or force the adoption of a particular API standard.

The stakeholders themselves, however, saw it more beneficial for the BoT to coordinate the adoption of a common API. The BoT takes a stick and carrot approach towards this and is still considering how to incentivize greater participation in a common API standard.

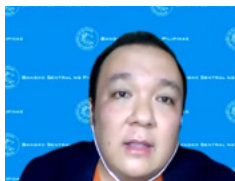
**Question 2: What are the current results of Open API and Open Banking in Thailand?**

A: Coming up with technical standards has not been difficult but pricing, deciding on the business rules to accompany these, is more challenging. For example, the national digital ID provides leverage for data to be used since that is where people perform e-KYC and provide consent. However, since this is an add-on service on the digital ID platform, how much to charge for the data shared is an additional consideration.

## STATE OF OPEN BANKING IN THE PHILIPPINES

### MHEL T PLABASAN

Officer-in-Charge, Technology  
Risk and Innovation Supervision  
Department [TRISD], Bangko Sentral  
ng Pilipinas



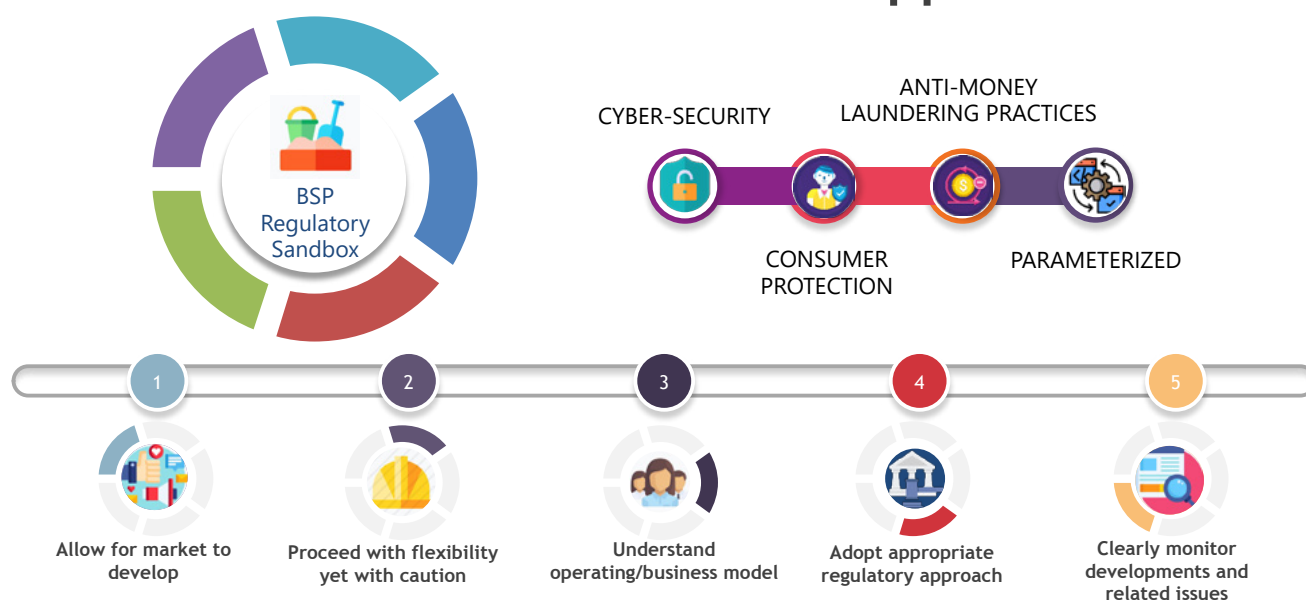
This presentation highlighted how the Bangko Sentral ng Pilipinas (BSP), the central bank of the Philippines, has promoted greater inclusivity using Open Banking. Similar to Thailand, the BSP has been cognizant of the benefits of moving to Open Banking, which it refers to as an Open Finance Framework. This espouses consent-driven data portability, interoperability, and collaborative partnerships among existing financial institutions and third-party players. The game-changing impact of Open Banking is in the permission access to customers' financial information, which is needed to develop innovative applications and services to provide customers and account holders with greater financial transparency options.

Underlying Open Banking is the concept that customers own their financial and transaction data. Thus, this data should be shared only if customers agree. This is why the BSP is embarking on policy initiatives to promote sharing of information among incumbent and third-party players.

As with other countries, BSP has conducted an Open Banking survey to gauge the level of stakeholder preparedness and interest in data sharing. It has also consulted subject matter experts and conducted comparative studies of different regulatory landscapes to determine the principles underlying their regulations as well as what measures have been adopted thus far.

The Regulatory Sandbox, BSP's 'test and learn' approach, is a critical component of the forthcoming regulations under its Open Finance Framework. This has five levels of action: (1) allowing the market to develop; (2) proceeding with flexibility, yet with caution; (3) understanding the operating/business model; (4) adopting an adequate regulatory approach; and (5) clearly monitoring developments and related issues.

## BSP's "Test and Learn" Approach



Given the inevitability of new concepts, products and services entering the market, the BSP will soon deploy this regulation and upload details onto its website. Earlier, it had already pilot-tested non-transactional payments (account statements) of 10 financial institutions within its 'test and learn' environment, while 11 others have indicated their interest in joining in as well. These entities have been allowed to operate in a live environment but the premise behind the 'test and learn' approach is that there are some non-negotiables, such as cybersecurity, consumer protection, and anti-money laundering.

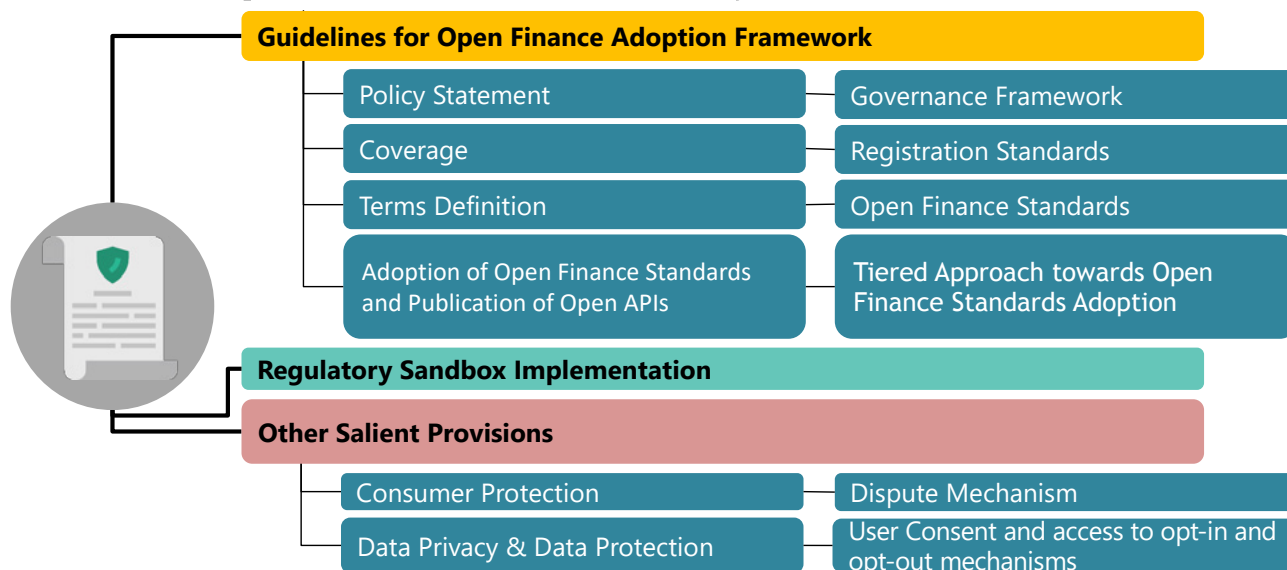
Of the related BSP initiatives, the most crucial has been formulating the Open Finance policy. While the approach is still to encourage competition and co-opetition, financial inclusion, and product innovation, this new regulation also has in-depth guidelines for its adoption.

It comprises a policy statement, governance framework, coverage, registration standards, definition of terms, Open Finance standards, adoption of Open Finance Standards and publication of Open APIs, and a tiered

approach towards Open Finance Standards adoption. It also includes Regulatory Sandbox implementation and other salient provisions such as consumer protection, dispute resolution mechanisms, data privacy and protection, and user consent and access to opt-in and opt-out mechanisms. Collectively, these form a firm backbone for an Open Banking ecosystem.

As the BSP moves towards an Open Banking system, there are some concerns around the adoption of the Open Banking framework, industry buy-in, and the determination of the industry-led, self-governing body that is expected to promulgate the detailed guideline standards and membership rules. Once this journey is complete, Open Banking is expected to be an industry game-changer resulting in overall benefits for both players and customers. This will be a testament to the BSP's long-standing innovation and digital transformation agenda to achieve financial inclusion.

## Open Finance Policy Formulation



## OPEN DISCUSSION AND Q&A

**Question 1: Open Banking is all about competition and collaboration. What are your ongoing or future initiatives that promote healthy competition in the market?**

A: The BSP faces similar challenges as Thailand. It is in the process of determining the governance framework for Open Banking, whether this should be industry-led as initially decided, or otherwise. The latest decision is that the BSP will oversee this but the industry will drive the details, including its standards, so that there will be buy-in from the private sector. At the end of the day, the framework will be owned by the industry so there will be both competition and co-opetition.

**Question 2: Could you elaborate more on the tiered approach to the Open Finance standard.**

A: There is a tiering of products and services in the draft circular. Tier One has product and service information only, such as account statements; Tier Two pertains to subscription and new account applications; Tier Three is on account information; and Tier Four on transactions and payments. This is the tiering that was initially identified. It will also serve as a guide for the adoption of the standards that the BSP will issue, as well as detailed rules introduced by the governance framework, the industry-led team.

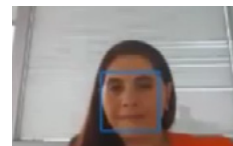
**Question 3: Is the Philippines' approach to API standard or mandated?**

A: After initially setting high-level expectations for standards, BSP had to strike a balance between being too broad (and confusing), and guiding the industry. Based on its survey, it discovered that the industry wanted guidelines on architecture standards, data standards and security standards. However, the details of implementation are expected to come from the industry-led governing body.

## STATE OF OPEN BANKING AND OPEN API IN MEXICO

**MARY PILY LOO**

Directorate-General for  
Operational and Technological  
Risk CNBV, Mexico

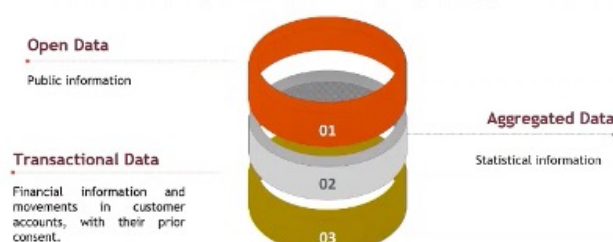


In 2018, Mexico passed the Law to Regulate Financial Technology Institutions (FinTech law). This covers financial services providers such as crowdfunding platforms and electronic funds payment (e-wallet) providers. It establishes the obligations of financial institutions with regards to Application Programming Interfaces (APIs) for interoperability and the sharing of customer data with prior customer consent. The law also covers the use of a regulatory sandbox for the regulation of different innovation models. It spells out the six principles of FinTech: financial inclusion and innovation; promotion of competition; consumer protection; preservation of financial stability; and AML-CFT (anti-money laundering and countering the financing of terrorism).

With the adoption of this FinTech law, Mexico recognizes Open Banking as a model of financial services where data is shared between banks or financial institutions and third parties. The inclusion of third parties is why this model is called Open Finance; APIs allow connectivity to interfaces developed by third parties so that customer data and information can be shared among different market players.

The financial sector in Mexico has evolved due to the incursion of technological innovation through disruptive business models with new access channels, scalable models and lower transaction costs. The number of FinTechs in Mexico increased in 2020, and greater growth is expected.

In Mexico, legal basis is stated in article 76 of the FinTech Law, empowering to Central Bank and the National Banking and Securities Commission to issue regulations in this regard, on 3 types of data:



Currently, the country has 50 banks, and 283 popular savings and credit institutions. Also, there are 94 FinTechs, including crowdfunding platforms and e-wallets, undergoing the authorization process.

Under Article 76 of the FinTech law, the Central Bank and the National Banking and Securities Commission are empowered to issue guidelines for the exchange of three types of data among financial institutions and third parties: open data (information available in the public domain); aggregated data (statistical information from customer activity); and transactional data (financial information and movements in customer accounts, with their prior consent).

There are particular risks involved in implementing an Open Banking model. The main ones are: (1) security of transactional data (for both sharing and consuming parties); (2) use of authentication methods considered unsafe (e.g. screen scraping); and (3) technical capacity of the regulatory authorities to stay abreast of new API standards and bring supervisory criteria up to date. These risks need to be mitigated.

In the first phase of its Open Banking/Finance project in Mexico, CNBV issued a set of regulations to help users of financial services enjoy the benefits of Open Finance. These regulations will take effect on 5 June 2021 and cover three areas:

1. **Information security.** These enable data providers and requesters to identify, exchange and process data securely. It considers usage of the OAuth 2.0 authorization structure, secure communication protocols, digital certificates, and encryption of information.
2. **Information architecture.** This enables data providers to develop standardized API query points (API endpoints) so that they can be queried by data requesters. (The protocol is based on the API Swagger version 2.0 specification format, which uses REST services and JSON format for data exchange.)
3. **Standard data dictionary.** This is a set of fields used on each API, for example, the ATM Locator includes data of a bank's location and services. Through this, vendors and requesters can exchange ATM data.

## APIS



### Accounts

Access to accounts (XSDA) and cards. Provide first-granted access to guests (auditor, accountant or public). Explore...



### Branches, ATMs and Products

Access open data related to banks including branches and ATMs including geolocation and opening hours. Explore...



### Transactions

Access the transaction history and transaction metadata. Explore...



### Metadata

Enrich transactions and counterparties with metadata including geolocation, comments, pictures and tags (e.g. category of spendings). Explore...



### Counterparties

Access the payees & payers of an account including metadata such as their aliases, labels, logos and home pages. Explore...



### Webhooks

Call external web services based on account events. Explore...



### Customer onboarding and KYC

Perform user, customer and account creation. Manage Know Your Customer (KYC) documents, media and status. Create customer meetings and messages. Explore...



### API Roles, Metrics and Documentation

Control access to endpoints, get API metrics and documentation. Explore...



### Payments & Transfers

Initiate Transaction Requests (transfers and payments). View and confirm charges (as per PSD2). Answer strong customer authentication (SCA) challenges. Explore...



### Search warehouse

Perform advanced searches and statistics queries on the data warehouse. Explore...



BANK NEGARA MALAYSIA  
DEBTA BANK OF MALAYSIA



The second phase of the Open Banking/Finance project included a piloting exercise with APIs for the exchange of transactional data. This focused on the customer experience, security of customer data, and an evaluation of possible adjustments to the technical data guidelines for transactional data. The pilot took place in a sandbox environment with data provided by participants from September to October 2020.

The standards defined in the APIs have been tested on four principal endpoints – accounts, balance, transactions and client consent. This generated a series of learnings related to definitions and implementation, and these have gone towards a draft document scheduled to be published at the end of 2020.

Details on the CNBV API Sandbox and endpoints were made available online<sup>4</sup> as was additional documentation on the APIs in this project. This included information on accounts, transactions, counterparties, customer on-boarding and e-KYC, payments and transfers, branches, ATMs and products, metadata, webhooks, API roles, metrics and documentation, and search warehouse.

For CNBV, the Open Banking/Finance project enables financial inclusion. FinTech APIs foster the creation of an ecosystem in which third-parties can offer more financial services, thus reaching the population that does not yet have access to traditional financial instruments. Banks and other entities offering different digital services that have API components (such as the CoDI digital payment platform or remote on-boarding) can reach more customers without them needing to be physically present at a branch. The collaboration between traditional financial entities and FinTechs beyond the information-sharing model is expected to create new business opportunities for the benefit of users.

In terms of regulation and supervision, CNBV has since 2018 been working to promote more intensive usage of supervisory technology (SupTech) to strengthen surveillance at two levels: (1) information gathering, and (2) the use of advanced analytics. In particular, a SupTech platform is being developed to allow the reception of information through APIs from FinTech institutions.<sup>5</sup>

---

<sup>4</sup> <https://apisandbox.ofpilot.com>

<sup>5</sup> There was no Q&A as the presentation pre-recorded to accommodate the different time zones involved.



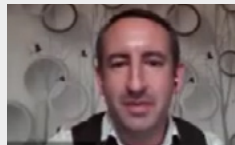
TUESDAY, 1 DECEMBER 2020  
DAY 1 - OPEN BANKING AND OPEN API

## SESSION 2: OPEN BANKING AND OPEN-API: OVERCOMING IMPLEMENTATION CHALLENGES

### MODERATOR

**ROBIN NEWNHAM**

Head Policy Analysis, AFI



Session two focused on how to leverage Open Banking initiatives to achieve the goals of financial inclusion. It showcased the experience of the UK, one of the first countries to have an Open Banking regime, for others to learn from its successes and challenges.

### OPEN BANKING: AN UPDATE ON UK'S LANDSCAPE

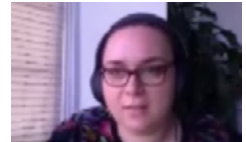
**RACHITA SYAL**

Senior Analyst, Fintech Hub,  
Bank of England



**IRINA MNOHOGHITNEI**

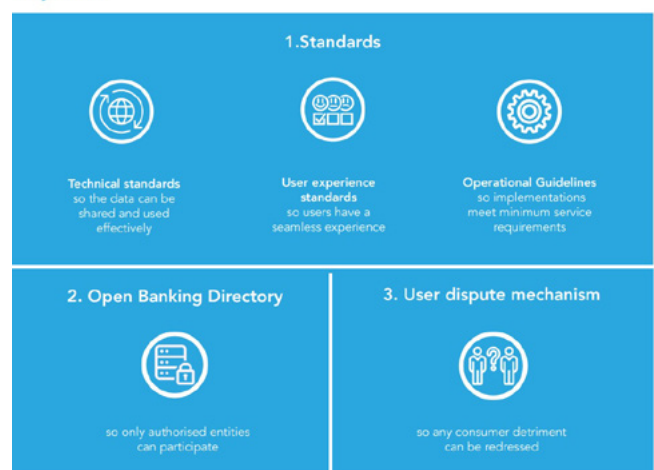
Senior Fintech Specialist, Fintech  
Hub, Bank of England



The United Kingdom adopted Open Banking in 2017 after nine of its largest banks – which account for 80 percent of the local market – agreed to give authorized third-party providers access to the personal financial data of customers who had consented to it. The delivery of Open Banking is mainly under the purview of the Open Banking Implementation Entity (OBIE), which among other roles, creates and maintains the Open Banking Standard and the Open Banking Directory, and monitors the nine banks (CMA9) involved.

- > The Competition and Markets Authority (CMA) initiated Open Banking in February 2017 as part of its Retail Banking Market Investigation to increase competition in the UK banking industry.
- > The Open Banking Implementation Entity (OBIE) creates and maintains a number of assets and delivers services in its role as the central implementation entity.

#### Key assets



#### Key services



- > While other PSD2 (The European Union's Revised Payments Services Directive) standards bodies (such as STET - France, Berlin Group - Germany) focus exclusively on technical standards, OBIE includes user experience standards and operational guidelines.
- > There are also functions providing implementation support for banks and TPPs seeking to implement Open Banking standards.
- > And a monitoring function that ensures CMA9 banks are meeting the requirements of the CMA order.

### HOW AN OPEN BANKING SYSTEM WORKS

The Open Banking system requires consumers and businesses to first consent to sharing their data with financial services and third-party providers that have met privacy standards. Drawing on data obtained across accounts, these providers then study, analyze and develop innovative tailor-made financial products and services. Bank customers can opt-out of this arrangement at any time.

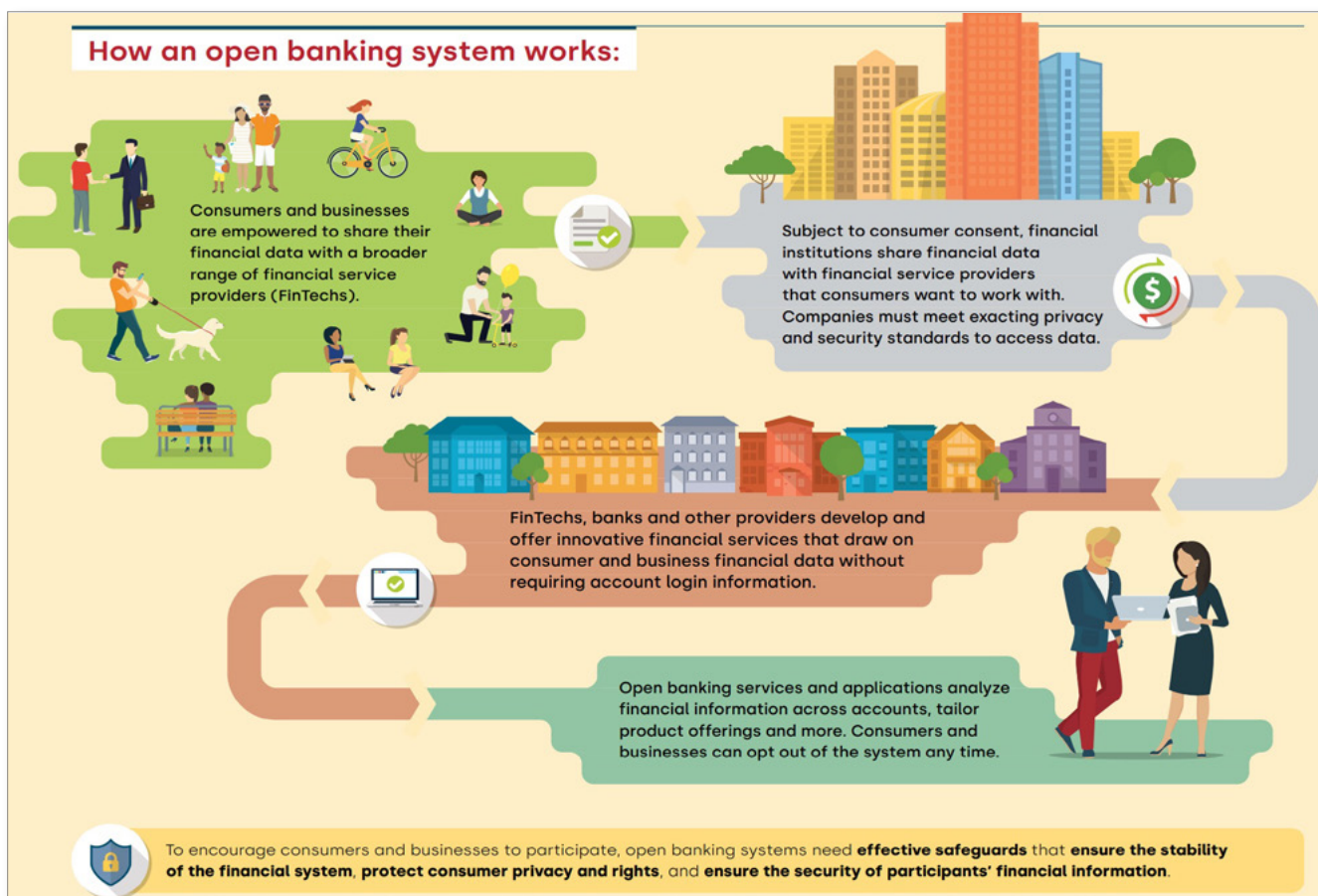
### THE GLOBAL PICTURE

A number of countries around the world have adopted Open Banking, each at various stages of maturity. Among the earliest in the field were the UK and European Union with its PSD2 (Revised Payments Services Directive). There exists a wide range of approaches. For instance, while the system in the UK, Brazil and Nigeria is directed and regulator-driven, some in Asia have taken a more market-oriented approach driven by the private sector.

### OPEN BANKING BUSINESS MODELS

There are three types of Open Banking business models:

- > Consumer products (e.g. bank account aggregators; personal finance tools; charitable giving; debt advice; credit file enhancement; identity verification).
- > Business products (accountancy and tax; debt management; loans and alternative lending; SME finance management; cash flow management).
- > Technical services (provision of software to help firms implement Open Banking Application Programming Interfaces [APIs]; premium APIs).



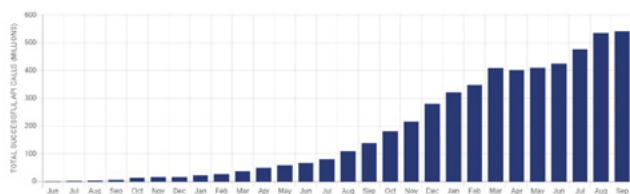
## PROGRESS TO DATE

By the end of 2020, the UK had two million customers signed up for Open Banking and over 94 such apps and products available. API usage had also grown significantly. However, there remain some gaps that prevent Open Banking from having greater traction.

A Crealogix survey in June 2020 revealed that two-thirds of UK consumers had not heard of Open Banking; and less than eight percent viewed it as a good idea. The majority were also concerned about privacy, data loss or fraud. There thus needs to be greater industry clarity and action on security, privacy, accountability (in cases of data breach), and liability for loss. In the UK, the OBIE and Financial Conduct Authority (FCA) are primarily responsible for driving this.

Successful API calls

This chart shows the number of successful API calls made by third party providers using account providers' (ASPs) Open Banking APIs.



## IMPACT OF COVID-19

In the UK, the Covid-19 pandemic saw a decline in cash usage (down to 10 percent in Q2 from 30 percent in Q1, while ATM withdrawals fell by 60 percent) and a rise in online sales (30 percent of all transactions in April 2020 versus 18 percent in 2019). Open Banking APIs also started to be used in innovative ways by consumers (e.g. to help the self-employed claim government support; gig workers to submit tax returns) and businesses (help firms to have more accurate revenue, cost and cash forecasts).

## MONITORING POTENTIAL RISKS AND REWARDS

For Open Banking to deliver on its potential benefits, its regulatory framework must incorporate appropriate consumer protection and privacy safeguards to win consumers' trust, as well as support the soundness of the financial sector. Potential risks need to be monitored, too: Open Banking may provide consumers and MSMEs with opportunities to optimize their savings and borrowing decisions but this could alter the financial market's structure. While it is too early to tell the impact of Open Banking in the UK, the situation is being monitored. For example, will the stability of the financial system be impacted if a TPP grows to become systemic, or will the business model and profitability

of banks be affected with heightened competition and greater transparency?

## OPEN FINANCE

Currently, Open Banking in the UK only covers personal and business current accounts and payment accounts. It has, however, shown the potential for sharing data securely throughout the financial system. Open Finance can apply the principles of Open Banking to allow businesses to link their data held at banks and utility companies to build a richer credit file, and also to make use of search, ratings and alternative data (e.g. social media). This is relevant for businesses since the UK has no credit history for businesses. Consumers and businesses can also have more control over a wider range of their financial data (e.g. savings, insurance, mortgages, investments, pensions and consumer credit).

## CONCLUSION

Open Banking has grown over the last two years but UK consumer awareness of it remains low. Nevertheless, it is likely that the landscape will continue to evolve as Open Banking API functionality improves and the impact from COVID-19 becomes clearer. Ultimately its success and the possibility of it leading to Open Finance opportunities will depend on customers giving consent, depending on whether customers using Open Banking have a seamless customer experience.

## OPEN DISCUSSION AND Q&A

**Question 1:** Did the BOE set up a dedicated Open Banking unit? Were there supervisory challenges that arose because of so many newcomers entering the market for financial services? What was the experience with inter-regulatory coordination between BOE and competition regulators?

A: Open Banking in the UK stems from the Competition and Marketing Authority's review of the competitiveness of the banking sector. The Open Banking Implementation Entity (OBIE) is responsible for developing the standards and the APIs that the top nine banks were required to implement to meet Open Banking requirements. The OBIE also maintains a directory of all third-party providers authorized by the FCA or national authorities in Europe. TPPs first need to meet certain requirements in terms of compliance and data security. Those in the OBIE directory can access OBIE-created APIs. The BOE monitors the market alongside other regulators in the UK. The FCA is responsible for the third-party providers authorized for Open Banking, including smaller FinTechs coming into the market to access customer data.

**Question 2:** How do you ensure that customer data privacy is not violated by the service provider or the FinTech firm? Could you provide some Insights into consumer protection risks, such as the process for handling complaints from consumers using these services?

A: Banks do not easily grant access to their customers' data; they only do so for customers who want their data shared with third-party providers that customers choose. Customer consent is key, and they can opt-in and opt-out at any time. Compared with previously when they surrendered much more personal information (e.g. via screen scraping or having third-party providers log into their bank accounts), under Open Banking, customers can give away just what is absolutely required. This was the idea in designing Open Banking principles in the UK: to put customers in control of their personal data and enable the data to be used in a safer way. There may be a greater risk of data leaks or cyberattacks, but in general, there are a lot of data rules and privacy laws such as the GDPR (General Data Protection Regulation) that all third-party providers and many of the banking applications have to first comply with. Complaints are handled by the FCA.

**Question 3:** Have you experienced any challenges to Open Banking from incumbent banks? Do they play a role in raising public awareness of Open Banking initiatives, or is this problematic given the concept could threaten their business by giving rise to the competition?

A: There was initial resistance as with any regulatory initiative. However, the incumbents were also the first movers in a lot of Open Banking initiatives; they recognized change was happening as their customers demanded it, and they had to share their personal data. Within the first year, more than half of the nine banks had implemented the Open Banking APIs. They understood that if data was to be shared, they too could see data that the customer had with other firms. By ensuring they had everything they needed within their own banking apps, they did not need to use that belonging to others. While the core functionality of Open Banking remains – that customers should be able to continue making payments for free from any account – a lot of thought has been given to how to monetize Open Banking given its potential as the market gets used to it. For example, if someone wishes to buy alcohol and needs to prove they are above 18, instead of sharing a copy of their ID which has a lot of personal information, one can use an Open Banking API to verify their age.

**Question 4:** Given that the majority of consumers do not have a positive view of Open Banking or understand the specific benefits, is there a strategy by the public sector to increase public awareness and education?

A: Initially, there was a conscious decision to not overly publicize Open Banking as the APIs had not been adequately tested. Efforts were made to improve their functionality and user experience only after it became clear that customer data could be safely shared. Ultimately the end consumer cares only about what is made possible by the technology and has now seen that Open Banking works. As the functionalities of Open Banking apps are improved, there will be a bigger drive to increase consumer awareness of the concept.



WEDNESDAY, 2 DECEMBER 2020  
DAY 2 - OPEN BANKING AND OPEN API

## SESSION 3: OPEN BANKING AND OPEN API: REGULATORY APPROACHES

### MODERATOR

**JAHEED PARVEZ**  
Technical Specialist, AFI



This session showed how the European Union makes for a very useful case study of the implementation of Open Payments due to the diversity of its Member States, and as an incremental step to Open Banking and Open Finance.

The European Banking Authority approaches the regulation of Open Payments through a particular lens based on the objectives of its creation. The EBA's inclusive Board of Supervisors is composed of the heads of the 27 supervisory authorities of EU Member States and makes the ultimate decision on what counts as a regulatory product and what does not.

## OPEN BANKING: AN UPDATE ON UK'S LANDSCAPE

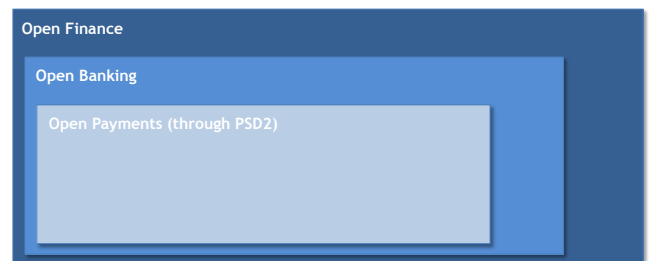
### DR DIRK HAUBRICH

Head of Conduct, Payments and  
Consumers, European Banking  
Authority



At the outset, Dr Haubrich observed that any discussion of Open Banking in the EU is more accurately and usefully referred to as Open Payments and would go on to elaborate on this important distinction later in his presentation.

What focuses on 'open payments' to start with.



He then introduced the EBA, sketching out why it was created, its main (or high-level) objectives and the tasks by which it goes about achieving them, and the effective legal instruments it has at its disposal to fulfill its mandates as a regional regulator and respond to market developments.

The EBA was established by EU law in the aftermath of the 2008 global financial crisis and came into being on 1 January 2011. It is an independent authority and is accountable to the EU Parliament and EU Council.

Haubrich then quoted and elaborated on the EBA's objective, from which its tasks flow: "To protect the public interest by contributing to the short, medium and long-term stability and effectiveness of the financial system, for the Union economy, its citizens and businesses." (Art.1(5)).

(In short, the EBA serves the public interest ("the Union economy, its citizens and businesses") by ensuring the short, medium and long-term stability of the financial system.)

This stability is meant to be achieved by "a sound, effective and consistent level of regulation and supervision" that prevents "regulatory arbitrage and

promot[es] equal conditions of competition”; and by “monitor[ing] new and existing financial activities and adopt[ing] guidelines and recommendations with a view to promoting the safety and soundness of markets and convergence of regulatory practice.”

This is the prism through which the EBA looks at Open Banking: It was created to further the goal of a single market of the EU.

A single market entails a level playing field, and equal levels of competition for all entities. Stated in practical terms, a business in one jurisdiction can offer its products in the other 26 member states without additional supervisory requirements.

The EBA has at its disposal different types of legal instruments. They differ in terms of their purpose and can be used to impose requirements on national authorities and financial institutions across Member States.

Of the eight types, two are most germane to open payments:

- > Technical standards are laws that the EBA has been mandated by the EU Council and Parliament to develop which, once adopted, become directly applicable in all EU member states. This means they are applied as written, without national implementation or transposition. So far, of the 120 to 130 technical standards developed by the EBA in the last 10 years, six are on open payments.
- > Guidelines and recommendations are not directly applicable in member states and do require national implementation by the national financial supervisory authority to come into legal effect. They are developed in collaboration with the relevant authorities of member states and are optional. However, of the 100 or so guidelines issued by the EBA to date, only a handful were not implemented due to specific reasons related to national legal frameworks.

Haubrich prefaced his discussion of the EBA’s regulatory approach to open payments by clarifying the important distinctions between Open Finance, Open Banking and

## Legal instruments available to the EBA

The EBA has different types of legal instruments at its disposal that differ in terms of purpose, legal status, and possible addressees.

- Technical standards
- Guidelines and recommendations
- Opinions
- Warnings
- Temporary prohibitions
- Joint Positions
- Breach of Union law investigations
- Binding and non-binding mediation





### Open Payments:

- > Open Finance goes beyond the banking sector into the insurance and investment sectors.
- > Open Banking is a subset of open finance; it offers typical banking products such as mortgage and consumer credit, in addition to payments accounts.
- > Open Payments is a subset of Open Banking; it refers to banks granting third-party service providers open access to their customers' payments accounts.

Open Payments is the only sector covered by the EU's revised payments law known as Payments Services Directive (PSD2), by which the EBA prescribes regulatory requirements for digital financial services related to open payments.

This legal approach was chosen over market self-regulation because there were some 6,000 banks in the EU at the time PSD2 came into effect in 2018. This diversity of banks, plus the diversity of TPPs that would access the payments accounts information of the banks' customers, made it necessary to legally require the banks to open their customers' payments accounts to TPPs systematically.

TPPs are allowed to access only information related to payments accounts in respect of payment initiations (i.e. to fulfill a request by the customer to buy something) or payment account information. Any data not required for these two regulated activities cannot be accessed by the TPP.

This narrow, incremental regulatory approach allows for learnings to occur before a broader foray into Open Banking takes place, and then into Open Finance. This possibility will be assessed in 2021 by the European Commission.

Haubrich then introduced the objectives of PSD2:



- > **Enhance competition** (among banks by opening their customers payments accounts to TPPs without charging the TPP); this is the key objective of PSD2.
- > **Facilitate innovation** by increasing competition in the payments services market via more types of product and services, and not only payment initiation. For example, account aggregation, where an app that aggregates information on the customers' accounts in various EU countries to display an overview of the customers' finances.
- > **Ensure technology and business model neutrality.**
- > **Promote customer convenience.**
- > **Contribute to a single EU payments market:** so a payments service provider based in any part of the EU can have customers in any part of the EU; the entire market is available to it without any added regulatory or supervisory burden across national borders.
- > **Protect consumers:** clarify legal liability in regards to a fraudulent transaction; the onus is on the bank to ensure authenticity.
- > **Strengthen security** to meet significant increases in payments fraud.

Some of the objectives necessarily compete with one another, and there is a need to strike a balance between them. For instance, the objective of single EU payments market, which is ideally based on a common API standard, competes with the objective of tech neutrality.

However, the need for innovation is also the need to encourage market competition in order to arrive at the best solution for the consumer. The assumption is that the best, most cost-efficient and user-friendly solution would eventually survive competitive pressures.

Notably, financial inclusion was left out as an objective of PSD2 because the overall rate of financial inclusion is very high among EU member states and increases yearly because most people have access to a payments account.

Asylum seekers and the homeless and temporary workers (who work outside their home state) are covered under a separate law that makes it mandatory for banks to allow these constituencies to open payments accounts so they may participate in the economy.

Haubrich then elaborated on the EBA's mandates, specifically those relevant to open payments.

**PSD2 mandates conferred on the EBA to implement Open Payments by Banks.**

RTS: regulatory technical standards;

ITS: Implementing Technical Standards;

SCA: strong customer authentication;

CSC: common and secure communication

**Mandate 1: Passporting Notifications.** A regulator in one jurisdiction keeps its counterpart in another jurisdiction apprised of entities from its own jurisdiction that intends to set up a business in the latter's. This aids transparency for regulators on business developments across the region.

**Mandate 2: Guideline on Authorization of Payment Institutions** stipulates uniform modes of payments for all national jurisdictions to ensure a seamless end-to-end payments process.

**Mandates 5,6,7: Guideline on Incident Reporting under PSD2, Regulatory Technical Standards on Strong Authentication and Secure Communications, and Guideline on Operational and Security**

**Measures, respectively.** Banks, TPPs and other payments institutions are required to report security incidents and operational issues arising from security incidents that affect consumers or other financial institutions to the national authority and thereon to the EBA. This must be done within 24 hours, with periodic updates and a final report within three days. (The more integrated the system, the more urgent such requirements become for the regulator to take action as soon as possible.)

**Mandate 6: Regulatory Technical Standards on Strong Authentication and Secure Communications.** This is key because it sets out requirements for permissions to access accounts. It avoids a situation where banks set up obstacles to access for TPPs thus undermining the spirit and objective of PSD2. This also protects banks from fraudulent manipulation of customers' data (from unauthorized access) and ensures payments accounts data are thoroughly protected.

**Mandate 9: Regulatory Technical Standards and Implementing Technical Standards on EBA Register** Maintenance of a register of all EU-based payment and money institutions (but not banks, which have a separate register, because banks are regulated entities

## PSD2 mandates conferred on the EBA

Mandates	Milestone reached			
	Milestone 1: EBA has started work	Milestone 2: EBA has published CP with draft GL/TS	Milestone 3: EBA has published Final draft TS or Final	Milestone 4: EBA has published GL Compliance table or Final GL or Commission has published TS in OJ
1 RTS on Passporting Notifications under PSD2	✓	✓	✓	✓
2 GL on Authorisation of payment Institutions under PSD2	✓	✓	✓	✓
3 GL on Professional Indemnity Insurance under PSD2	✓	✓	✓	✓
4 GL on Complaints Procedures by CAs under PSD2	✓	✓	✓	✓
5 GL on Incident Reporting under PSD2	✓	✓	✓	✓
6 RTS on Strong Authentication & Secure Comms. under PSD2	✓	✓	✓	✓
7 GL on Operational & Security Measures under PSD2	✓	✓	✓	✓
8 GL on fraud reporting under PSD2	✓	✓	✓	✓
9 RTS & ITS on EBA Register under PSD2	✓	✓	✓	✓
10 RTS on Central Contact Points under PSD2	✓	✓	✓	✓
11 RTS on home-host coordination under PSD2	✓	✓	✓	

that are by default allowed to offer Open Payments services). These currently number 3,000 to 4,000, plus 160,000 agents. The register is fed by data from national authorities but is available for free on the EBA website. It serves as a one-stop shop of information on all entities in the EU. No registration is required. The entire register is downloadable, and has been downloaded at a rate 100,000 times a month from more than 100 jurisdictions across the world. It is stable, fast, secure and reliable and provides transparency on all market players, even those of competing types such as TPPs and incumbent banks, thus allowing for useful market assessment.

The EBA has been working on open banking since 2016 and, in the process, has achieved several successes but also experienced a number of challenges. Some of these are: Some of the successes, challenges and mitigations so far in the EBA's implementation of its PSD2 mandates are as follows:

### SUCCESSSES

Successes include some 450 payment/e-money institutions now providing AIS (account information services) and PIS (payment initiation services) in the EU, leading to significant innovations in the market with new services being offered to consumers. Haubrich attributed this to the main objective of PSD2 of encouraging market competition. Related to this is the 100,000 downloads per month statistic of the EBA register, from over 100 countries worldwide; this shows that interest in data on open payments in the EU, and by extension, in the EU market, is high.

### CHALLENGES

- > Divergent API models across the 27 EU Member States.
- > Some incumbent banks establishing obstacles against AIS/PIS providers accessing accounts.
- > Some AIS/PIS providers making baseless claims about their rights to open banking/finance.

Challenges include divergent API models across the 27 EU Member States (as expected), and some incumbent banks establishing obstacles against AIS/PIS providers accessing accounts. On the other hand, some AIS/PIS providers have made baseless claims about their rights to open banking/finance. EBA has addressed this by issuing its opinion on the legality of their actions for national regulators to act upon.

### MITIGATIONS

- > Establishment of EBA Industry Working Group on APIs.
- > Constant monitoring and issuance of requirements to react to undesirable market behavior.
- > Technological neutrality.
- > Q&A tool.

To mitigate the challenges of opening the market to greater competition, EBA has set up an Industry Working Group on APIs comprising nine banks, nine TPPs, and nine API scheme providers to present their viewpoints and seek clarifications, which are published. The EBA also constantly monitors and issues requirements in response to undesirable market behavior by banks and TPPs. These requirements are both written and supervised in a technologically neutral way to avoid inadvertently signaling to the market which solutions the EBA prefers.

There is also a Q&A tool for market players, so helpful clarifications of regulatory requirements can be provided in a relatively short time of three to five months. These clarifications are publicly accessible, and are made in consultation with all regulators of the 237 EU Member States, but are not legally binding,

### OPEN DISCUSSION AND Q & A

**Question 1: How do the European Central Bank and European Banking Authority coordinate with each other when it comes to Open Banking and what are their different roles and responsibilities?**

A: The European Central Bank is not an EU institution; it doesn't have an EU remit. The remit for all 27 member states of the EU rests with the EBA which has been mandated to develop the 12 technical standards and guidelines referred to earlier, and how to supervise these requirements as well.

However, in the area of security requirements among the 12 standards, there are three, we have the mandate to develop these mandates in close cooperation with the ECB since the ECB has experience in the area of security. The ECB also has a mandate for the oversight of payments systems, and crucially the oversight of card schemes [such as] American Express, Visa, and Mastercard, but also many national card schemes. So the ECB also has an interest in [open payments] to ensure it can carry out its oversight function in that respect. Therefore we have both jointly developed these requirements. But the supervision of the Open Banking requirements is primarily the responsibility of

the EBA, which we are still carrying out.

**Question 2: What is the approach to API in the EU given that it cuts across several countries, for example. Is it a standard one, and is it mandated or industry-driven? Is there a governing body for this in the EU?**

A: [T]here were two opposing EU objectives: one is to create a single EU payments market and the other one to facilitate innovation. The objective of the former would suggest that the EBA establishes and imposes one single API across the EU, possibly to include even the programming code of that API. We have decided not to do that for a number of reasons.

One, there was another objective, facilitating innovation: we need to allow the industry to develop its API in a competitive way so that the best APIs survive eventually, and the most cost-efficient and most effective and most user-friendly API survives eventually. [Second], this was also because we only had 12 months to develop these technical standards, and to also add the API programming code within 12 months would not have been possible. Third, we thought that a public authority like EBA is not the best entity to impose a single technological standard across 27 jurisdictions. For those reasons, we didn't impose it and acknowledged that our decision might lead to market fragmentation.

At the moment, there are eight or nine different API schemes across the EU that we are aware of. Some of these cut across borders, but these are industry-driven. The Berlin Group is the most well-known; it cuts across several jurisdictions. More than 1000 banks and also third-party providers and other entities are included in that group, and it has its own governance. Some other API schemes exist with a more national focus but these are not governed by the EBA; they have their own governance, industry-driven. But we do bring them to the table in the API Working Group that I referred to earlier.

**Question 3: Could you share more details on how EBA set up the Industry Working Group. What are your major takeaways in terms of enabling factors and challenges in setting up one?**

A: That is a very good and also political question. We asked ourselves this question around two years ago when we set up the group. What we did is publish on our website, a call for expressions of interest, for everyone to know that we would be setting up

this group, that we want to receive applications. We explained there would be a limited number of seats. We also explained that there would be equal representation of these groups, so nine banks, nine third-party providers, and nine API schemes. We didn't want to get into a discussion of favoritism, but perception is sometimes quite striking. For example, the fact that we are called the European Banking Authority is perceived by many third-party providers that we are there to protect the banks. Therefore, we are not giving the third-party providers sufficient consideration, which is not true. This is a perception we frequently face which we want to avoid. So we made equal representation for the three groups.

Then we set out in the call of interest: who we want to have in terms of expertise and skills. We didn't want lobbyists, regulatory affairs directors, and so on. We needed those with technological skills about APIs and open bank access so they can tell us what issues they see, either as a TPP or a bank, and we can impose requirements to address those. We set this out in our call, so that the applications we received were judged against these criteria, like a vacancy notice. We also expected to get many more applications than the 30 seats we have. We received 160 applications and turned down 130.

We had five full-day meetings, now interrupted by Covid-19 but we will resume some point in the future. Each of these five meetings were prepared with particular agenda items. We requested information ahead of the meeting to make sure that at the meeting we had a substantive discussion on the issues. This was an industry group of 30 people. The national authorities of the 27 EU member states are in the room as well but EBA chairs it so that they hear what the issues are. After the one-day meeting is over, we have a second day only with the national authorities where we discuss what we heard the previous day and how we are going to respond to that.

Many of these responses are public on our website, dedicated page for this Working Group. We also publish the agendas and clarifications that we have provided in response to the issues that we have seen. We have Q&As to respond to the issues that we have been told about and that we found credible. Or we issue our opinion on issues raised by stakeholders.

**Question 4: Consumers may not understand how Open Banking works which might result in a fear of sharing data. Is there a role that regulators can play and have you seen any European**



### countries where they have played a role in raising consumer awareness?

A: EBA has not taken any measure to increase consumer awareness primarily because that role has been allocated to another body. In the PSD2 there is a mandate for the European Commission itself to publish an electronic leaflet that explains to consumers across the EU the rights and new opportunities they have through PSD2. The take up of new services is primarily the responsibility of those providing a service. It is not the responsibility of a regulatory authority like the EBA to generate revenue for a private sector institution. That is their responsibility, and they are usually much better at that.

**Question 5: Most of the publications indicate the difficult task financial regulators have in achieving a balance of supporting innovation, competition and consumer protection. What has been the EU's approach to maintain that balance?**

A: We had to develop these requirements as the EBA with our national authorities two or three years ago. This relates to different objectives. One is to protect consumers; the other one is to make payments more convenient and secure for consumers. That inbuilt tension pushes us as a regulator into opposite directions. As a regulatory body you just have to be open and transparent and explain your rationale. We go into a consultation for all our standards and guidelines. You get feedback from the respondents, and that gives you additional indication whether where you land on the spectrum is in the right place or needs adjusting. There is no magic bullet.

It is also a matter of history within your jurisdiction, how strong or sensitive you are to fraud, for example. In the EU, we are significantly sensitive to operational resilience generally but also payments fraud. Therefore, there is no one sentence answer; it is about being transparent about how and why you made a trade-off between competing objectives and soliciting public responses. Analyze these responses and if they are convincing, be prepared to change your position to the left or to the right of the spectrum. Be prepared also to reject responses.

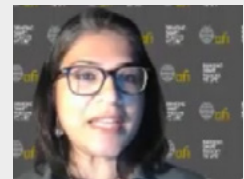
WEDNESDAY, 2 DECEMBER 2020  
DAY 2 - OPEN BANKING AND OPEN API

## SESSION 4: THE ROLE OF DFS IN ADDRESSING THE IMPACT OF COVID-19

### MODERATOR

ABAN HAQ

Project Lead, Digital Financial  
Champions, Alliance for  
Financial Inclusion



This session considered a broader view of Digital Financial Services (DFS), particularly in the context of COVID-19.

It weighed what a “better normal” means in practice for financial inclusion and looked towards the future from three perspectives that could help inform recovery policy and frameworks – digital finance, gender-inclusive finance, and inclusive green finance.

## THE ROLE OF DIGITAL FINANCIAL SERVICES IN ADDRESSING THE IMPACT OF COVID-19

### MELCHOR T PLABASAN

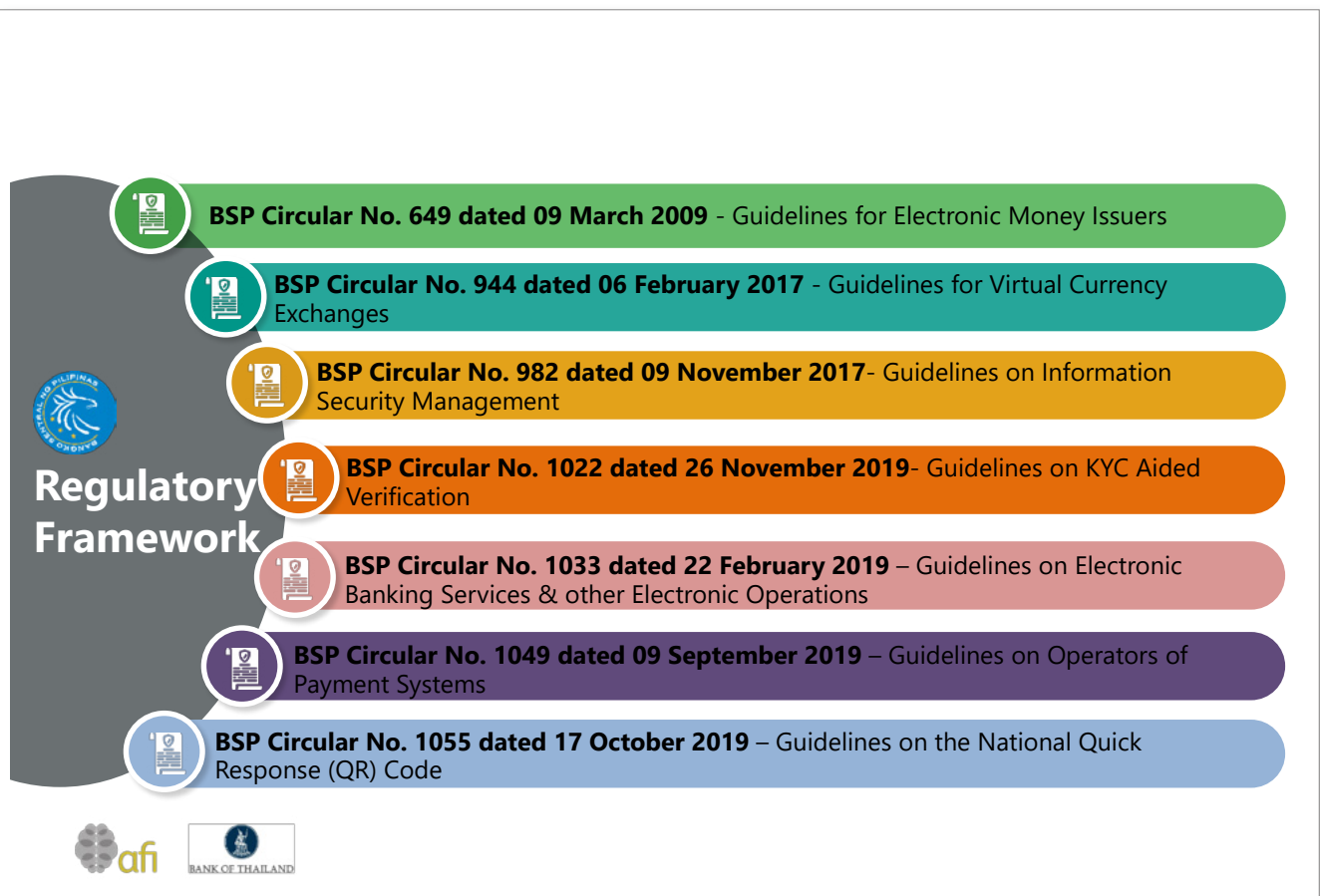
Officer-in-Charge, Technology  
Risk and Innovation Supervision  
Department [TRISD], Bangko  
Sentral ng Pilipinas



Prior to the Covid-19 pandemic, the rapid expansion of the digital economy in the Philippines was already transforming its financial landscape. In response, the Bangko Sentral ng Pilipinas (BSP, Central Bank of the Philippines) began to lay the groundwork to expand the country's digital finance ecosystem. From 2009-2019, it introduced a regulatory framework that included guidelines on electronic money issuers, virtual currency exchange, information security management, KYC-aided verification, etc. While the major theme of these regulations was innovation, they also sought to ensure that the associated risks were effectively managed. Underlying these reforms was a digital imperative: building a robust digital infrastructure, digital skills, digital ID, and an enabling regulatory framework.

The pandemic provided an unexpected catalyst for everyone to go digital. In the first two months of the local lockdown, there was a rapid rise in the number of Filipinos opening accounts using technology-aided or digital on-boarding processes (4.1 million). Domestic transfer facilities also saw increases in transaction count and value. For example, from July 2019 to July 2020, the PESONet transaction count rose by 122 percent, while its transaction value grew by 119 percent; the InstaPay transaction count increased by 739 percent, and transaction value by 442 percent. Even government payments experienced exponential growth. EGov Pay, which was devised to curb government revenue leaks through efficient collection means and enhance transparency, had a 688 percent volume growth, and a 799 percent value growth as of June 2020.

The BSP's Digital Banking Exposure Draft that was approved in 2020 strengthens guidelines on deposit and cash servicing outside of bank premises. It creates a distinct 'digital bank' category and provides guidelines on capitalization and how existing banks that would like to be digital banks will be transitioned within three





years. The BSP also reserves the right to determine the maximum number of digital banks allowed to operate. These banks are expected to primarily conduct their business using a digital platform or electronic channels and cannot establish branch or “branch-lite” units. All this is part of its digital transformation roadmap which recognizes the ability of digital banks to expand access to broader financial services in the country.

Additionally, the BSP is supporting the government’s efforts to come up with a national ID. It has begun gathering biometrics and soon a QR code will be adopted nationwide. However, since some still need cash agents, there will not be a seamless transition from cash to digital platforms. This is why digital banks have been given the authority to engage cash agents. The national ID system (PhilSys) is expected to enable Filipinos to access and utilize innovative digital financial products and services while the QR code will facilitate interoperability and allow merchants and clients to minimize the number of accounts they have to use.

If channeled the right way, these technological innovations are expected to curtail financial inclusion barriers. In fact, technological innovation in financial services can be a tool for survival in times of challenges like the current pandemic. For central bank regulators and policymakers, however, it is about striking the right balance between innovation and regulation.

## National Government’s Digital Initiatives

### National ID System (PhilSys)

Enable Filipinos to access and utilize innovative digital financial products & services

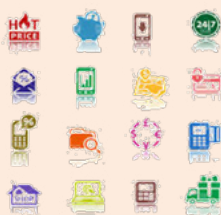


### QR Code Adoption

Facilitate interoperability and allow merchants and clients to minimize the number of accounts they have to use

### Strengthening of Guidelines on Deposit and Cash Servicing Outside of Bank Premises

(Circular 940, 20 January 2017)



### Expansion of cash agents



### Wider network



### Reaching the last-mile

**AFI POLICY FRAMEWORK FOR LEVERAGING  
DIGITAL FINANCIAL SERVICES TO RESPOND TO  
GLOBAL EMERGENCIES: CASE OF COVID-19****GHIYAZUDDIN ALI MOHAMMAD**Senior Policy Manager, Digital  
Financial Services, Alliance for  
Financial Inclusion

When the Covid-19 lockdowns began and many grappled with how to respond to the health crisis that rapidly became an economic and financial services crisis, AFI formed a subgroup under the Digital Financial Services (DFS) Working Group and produced a policy framework to respond to the pandemic, but that is applicable also for any emergency or disaster situations. The framework has seven key pillars as follows.

The first and most immediate response to the crisis was **promoting and incentivizing digital payments**. For example, AFI member countries introduced awareness and sensitization initiatives for making payments in a

safe manner. Key in this is engaging with stakeholders and taking the lead from them, making evidence-based decisions, and doing all this in a timely manner to maintain the sustainability and viability of industry.

The next pillar is around **secure and resilient digital payments and technology infrastructure**. This is about keeping one's house in order, and ensuring that there is a business continuity plan in place. Resilience in digital payments infrastructure is also important as seen in the number of phishing attacks and vulnerabilities that have grown manifold during the crisis. There needs to be an emergency and crisis communication plan to ensure that there is no misinformation, and to bring calm and reassurance to market and stakeholders.

The third pillar is having **enabling regulations**. Here the roles of financial regulators and central banks are crucial. Such regulations can ensure that solutions offered adhere to existing standards. For example, consumer protection and data privacy initiatives that ensure fair treatment of clients, and digital financial literacy-related initiatives for those with increased

## Key Contours of the Policy Framework

Promoting and Incentivizing Digital Payments

Secure and Resilient Digital Payments & Technology Infrastructure

Enabling Regulations

Agent & Merchant Operations

Facilitation of Additional Use Cases

Coordination Among Stakeholders

Cross Cutting Issues

<https://www.afi-global.org/publications/3322/Policy-Framework-for-Leveraging-Digital-Financial-Services-to-Respond-to-Global-Emergencies-%E2%80%93-Case-of-COVID-19>



vulnerabilities (women, elderly, disabled, displaced, small businesses). There can also be regulations for innovations to respond to increasing digitization including monitoring suspicious transactions, money laundering and financing-related risks.

The fourth pillar is about **agent and merchant operations** covering the ‘last mile’ cash-in cash-out transactions and digital payment transactions via agents or merchants. In the initial phase of lockdowns, many countries identified such agents and merchants as essential service providers to ensure that access to cash remained. It is thus important that they, as well as vulnerable customers, are made aware of and trained about hygiene and social distancing norms.

**Facilitation of additional use cases.** The pandemic saw an increase in the number of use cases (e-money, mobile money, online and offline payments). Some have estimated that the growth of e-commerce in the last 10 years happened in the first three months of the lockdown – that needed to be facilitated. Some facilitating of digital payments for emergency cash transfers and support programmes for smaller businesses and affected and vulnerable populations has already taken place.

There is also a need for **coordination among stakeholders**. The crisis was a big learning for AFI in terms of being prepared and ready for any eventualities. It learnt that central banks need to be part of the national task force - internal and institutional task forces and working groups comprising stakeholders from financial services providers need to be set up, and FinTechs and startups have to co-create solutions to meet customers’ needs in the midst of the crisis. At the global level, there must be a cooperation and collaboration platform for mutual learning, beyond the role AFI plays. There should be a platform to mobilize funds and deploy this in an effective and efficient manner, something international agencies such as the IMF and World Bank can do; specifically, to identify countries that are more vulnerable from a fiscal and monetary standpoint and provide timely assistance to them.

The final pillar is about addressing **cross-cutting issues**. Besides greening recovery efforts, there is a need for environmental impact assessments and to explore opportunities related to renewable energy and energy-efficient systems for small businesses and individuals. Given that women have been disproportionately affected, it is also important to have assistance programs and products focused on them along with other vulnerable groups.

## OPEN Q&A SESSION

**Question 1:** In the Philippines experience, were there any areas more work needed to be done after COVID-19 and the sudden uptake of DFS? What are the areas regulators need to focus on to ensure that our systems and regulatory frameworks are robust?

A: One of the areas needing attention now is consumer education, particularly digital literacy, given the massive growth in e-payments and the existence of online fraud, a lot of which involve consumers giving away their information. Strengthening digital literacy involves teaching consumers how to protect their digital identity and how to conduct online transactions safely. This will help further harness the digital ecosystem.

**Question 2:** In light of the COVID-19 experience, will there be more inclination towards risk mitigation in the short and medium-term, as opposed to innovation? Will there be a change in the trend in DFS regulatory approaches?

A: The immediate priorities are getting the ‘nuts and bolts’ of the financial services ecosystem in place to facilitate, for example, emergency cash transfers for supporting small businesses. Countries with existing digital infrastructure and enabling support policies have taken the lead. The US is one example where they have been able to use their digital identity system to improve the identification of beneficiaries and make payments in a timely manner. However, this was not the case in many advanced countries that did not have a nationwide digital identity framework in place. In the long run, from a digital standpoint, consumer education and capability is a paramount consideration while from a cyber-security standpoint, it is about securing financial services infrastructure and ensuring its resilience and security. Likewise, with data privacy frameworks and ensuring it translates to the financial sector.

## GENDER FINANCIAL INCLUSION AND COVID-19

## HELEN WALBEY

Head of Gender Inclusive Finance,  
Alliance for Financial Inclusion

Globally, nearly a billion women remain financially excluded. In the developing world, the **financial inclusion gender gap** of nine percent has stubbornly persisted since 2011. The widest gap is observed in the Middle East and North Africa, Sub-Saharan Africa, and South Asia. Advancing women's equality could add an estimated USD12 trillion to global GDP by 2025 but barriers that prevent this from happening include socio-cultural factors, lack of gender-sensitive policies, limited ownership or control of mobile technology, inadequate access to digital devices, and limits in financial literacy/financial capability.

During Covid-19, many of the policies and regulations developed have not been gender-sensitive. When regulators do not understand the difference between gender-sensitive and gender-neutral interventions – the latter frequently replicates existing structural barriers – this can impact on women's opportunity to access DFS. If unable to develop gender-sensitive policies, they need to be open to taking expert advice. This is where AFI can help. As well, its Denarau Action Plan identifies ten key areas where governments can take action to close the gender gap, including its third point that recognizes the key role that DFS and innovative technologies play in women's financial inclusion.

Two clear **gendered impacts of Covid-19** are in relation to the renewed reliance on technology and the internet, and the risk of women and other vulnerable groups being further marginalized.

## Gendered Impacts of COVID-19

**Lack of sex-disaggregated data** is limiting policy makers' understanding of the true socio-economic impacts of COVID-19 on women and ability to assess the potential or actual impact of government policies and programmes during this crisis

Opportunity to take concrete action to better understand the female market segment and implement gender-inclusive policy initiatives so that we can **build a more inclusive, stronger and sustainable future** where the gains made towards closing the financial inclusion gender gap are not lost, but sustained



The former is important to maintain economic activities and includes access to banking and government social assistance programs where the majority of beneficiaries are women or women-headed households, as seen in the Philippines, Pakistan, Peru, Morocco and Togo. The latter is about how in response to the pandemic, the move towards an accelerated adoption of DFS may adversely impact on women or those with limited or poor literacy and digital capabilities, and their access to reliable and easy-to-understand information (e.g. in local languages, promoted over radio or in markets and health centers). Issues around DFS are a risk but also an opportunity. When regulators of financial service providers can develop gender-sensitive products and services, there is a real opportunity to support women's financial inclusion. Such is the case with the Central Bank of Egypt's role in digitizing a gender savings group and supporting women to continue saving and accessing loans throughout the pandemic, in a safe manner.

The **lack of sex-disaggregated data (SDD)** hampers policymakers from understanding the true socio-economic impact of COVID-19 on women, limits their ability to accurately assess the potential or actual impact of government policies and programs during this crisis, and to make evidence-based decisions. There is an opportunity to take concrete action to better understand the female market segment, including how

## In Country Examples: Pakistan

- An example of unconditional cash transfer payments for women can be seen in Pakistan with the launch of the Ehsaas, the federal government's new poverty alleviation program, which sees cash payments delivered to 12 million families, representing over 80 million people.
- The majority of these payments have gone to women and are being delivered using biometric identification.
- This method is more cost effective and dignified, than just vouchers or food aid, since it is linked to benefitting the local economy and providing stability to vulnerable families.

## In Country Examples: Jordan

- In Jordan, the Central Bank of Jordan amended regulation to enable e-KYC for mobile wallet opening for forcibly displaced persons in the country. All refugees can now use UNHCR identification cards to remotely open mobile wallets, which they can optimize to make remittances and P2P transactions.
- Within 24 hours, the Central Bank of Jordan communicated this to all payment service providers to instruct them to develop needed requirements for this purpose.



it is not homogenous, and implement gender-inclusive policy initiatives towards building a more inclusive, stronger and sustainable future; gains made towards closing the financial inclusion gender gap are not lost but sustained. Towards this end, AFI offers technical expertise and tools such as its new SDD reporting template, and publications like “Why the Economic Response to COVID-19 Needs to be Financially Inclusive and Gender-Sensitive”.

In this publication, AFI has identified **five key pillars for developing a fully inclusive and gender-sensitive financial system**.

1. **Women and Regulatory Institutions:** Gender-sensitive Covid-19 response plan; Gender-sensitive communications plan; Gender/Regulatory Impact Assessments (GIAs/RIAs).
2. **Women and MSMEs:** Women-focused SME guarantee schemes; Subsidize credit and support restructuring/refinancing; Decreased taxes and social security contributions; Movable collateral registries and alternative credit scoring; Incubation programs dedicated to women-led MSMEs.

3. **Women and Social Protection:** Unconditional cash transfers for women; Maternal and sexual healthcare services for women and girls; Remittance fee waivers; Insurance services.
4. **Women and DFS:** Digitization of village savings and loans associations; Gendered approach to responsible DFS; Women’s mobile phone ownership; Agent network cash-in and cash-out; Digital identity.
5. **Women and Regulatory Frameworks:** Gender-sensitive regulatory and legislative frameworks; Gender-sensitive National Financial Inclusion Strategies (NFIs); Women’s financial literacy strategy and national strategies for financial education (NSFE).

Underlying these pillars are the cross-cutting themes of SDD collection, tiered KYC, and an institutional Gender Focal Point, i.e. someone within your organization who will lead and coordinate all work in this area.

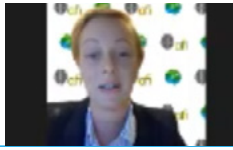
(Two country examples, Pakistan and Jordan, were identified as best practices. However, due to time constraints, no details were given but these cases are found in the publication mentioned earlier.)

## Key Pillars for Developing A Fully Inclusive & Gender-Sensitive Financial System

WOMEN & REGULATORY INSTITUTIONS	WOMEN & MSMEs	WOMEN & SOCIAL PROTECTION	WOMEN & DFS	WOMEN & REGULATORY FRAMEWORKS
<ul style="list-style-type: none"> <li>➢ Gender-Sensitive COVID-19 Response Plan</li> <li>➢ Gender-Sensitive Communications Plan</li> <li>➢ Gender/Regulatory Impact Assessments (GIAs/RIAs)</li> </ul>	<ul style="list-style-type: none"> <li>➢ Women-focused SME Guarantee Schemes</li> <li>➢ Subsidize credit and support restructuring/refinancing</li> <li>➢ Decreased taxes and social security contributions</li> <li>➢ Movable collateral registries and alternative credit scoring</li> <li>➢ Incubation programmes dedicated to women-led MSMEs.</li> </ul>	<ul style="list-style-type: none"> <li>➢ Unconditional Cash Transfers for women</li> <li>➢ Maternal and sexual healthcare services for women and girls</li> <li>➢ Remittance fee waivers</li> <li>➢ Insurance services</li> </ul>	<ul style="list-style-type: none"> <li>➢ Digitization of Village Savings and Loans Associations (VSLAs)</li> <li>➢ Gendered approach to responsible digital financial services</li> <li>➢ Women’s Mobile Phone Ownership</li> <li>➢ Agent Network cash-in and cash-out (CICO)</li> <li>➢ Digital Identity</li> </ul>	<ul style="list-style-type: none"> <li>➢ Gender-sensitive regulatory and legislative frameworks</li> <li>➢ Gender-sensitive National Financial Inclusion Strategies (NFIS)</li> <li>➢ Women’s Financial Literacy Strategy and National Strategies for Financial Education (NSFE)</li> </ul>

CROSS-CUTTING THEMES: SEX-DISAGGREGATED DATA COLLECTION, TIERED KYC AND INSTITUTIONAL GENDER FOCAL POINT



**INCLUSIVE GREEN FINANCE AND COVID-19  
RECOVERY****JOHANA NYMAN**Head of Inclusive Green Finance,  
Alliance for Financial Inclusion

When contemplating how nations can be rebuilt following the COVID-19 crisis, it is crucial to consider greening economic recovery. There may be limited scope for this in the short-term, but there is a lot of potential for medium and longer-term responses. There is a very clear business case for greening. For instance, taking bold climate action can yield direct financial gains of USD26 trillion through to 2030. There are also strong returns from investing into climate change adaptation, with benefit-cost ratios ranging from 2:1 to 10:1. Greening MSMEs (e.g. building their resilience to climate change, reducing energy costs and potentially giving a competitive repetitional advantage) can yield great benefits too. Those at the base of the economic

pyramid stand to gain as well from savings and benefits generated through a green transition. Likewise, the potential for increased demand and job creation, which can be especially beneficial to MSMEs.

Thus far, not many AFI members have incorporated green elements into their COVID-19 recovery response. There are, however, examples of general inclusive finance policies, ones that can be repurposed for greening COVID-19 recovery. Drawing from the experiences of its members, AFI developed the '4P' policy framework of inclusive green finance and shared this with the wider network.

The policies listed below can be used for COVID-19 recovery as well.

- 1. Provision:** Refinancing schemes for MSMEs; Lending quotas for green (or greening) MSMEs; Other financing schemes for green lending; Inclusion of gender elements in the provision policies for MSMEs.

**4Ps AND A POST COVID-19 RECOVERY****1. PROVISION**

1. Refinancing schemes for MSMEs
2. Lending quotas for green (or greening) MSMEs
3. Other financing schemes for green lending
4. Inclusion of gender elements in the provision policies for MSMEs

**2. PROTECTION**

1. Credit guarantees for climate smart agriculture / greening of MSMEs
2. Climate risk insurance

**3. PREVENTION**

1. ESRM guidelines to be kept also during the recovery
2. Expanded to climate mitigation and adaptation?



2. **Protection:** Credit guarantees for climate smart agriculture/greening of MSMEs; Climate risk insurance.
3. **Prevention:** ESRM (environment social risk management) guidelines – existing for these to be kept also during the recovery so that existing standards are not ignored; Expanded to climate mitigation and adaptation.
4. **Promotion:** Policies to allow government to offer incentives to the private sector to offer financial services to qualified beneficiaries.

Some AFI members have Disaster Risk Reduction policies (DRR) and emergency preparedness measures in place. These include disaster reconstruction facilities, refinancing recovery and reconstruction policies, and digital distribution of social payments. After the 2015 cyclone in Fiji, its Reserve Bank used DFS mobile money in its “Help for Homes” program, and currently there is a lot of discussion about using blockchain for disaster payments and humanitarian help responses following a national disaster.

While the impact of a global pandemic is vast, such measures can provide a relative safety net for financial institutions that can, for instance, enable them to help clients resume their economic activities. The pandemic and climate change have the biggest impact on those at the base of the pyramid and have similar economic shocks. The COVID-19 crisis can thus provide lessons for designing future DRR policies, and responses to national disasters linked to climate change.

Within the Inclusive Green Finance Working Group of AFI, there is a specific subgroup looking into the intersection of DFS and Inclusive Green Finance to see how DFS can accelerate and enable the roll out of Inclusive Green Finance policies, and ensure they reach more people and those who really need it, so they can build resilience and enable mitigation.

To date, there are only two examples from the AFI network where there has been a greening of the Covid-19 response. The first is the Green Transformation Fund of Bangladesh Bank, which was set up in 2016, later expanded to respond to COVID-19. This finances manufacturer-exporters against the import of capital machinery and accessories for implementing specific green/environment-friendly initiatives. The second is from Bangko Sentral ng Pilipinas, which has been involved in an Inter-Agency Working Group to outline ways to recover from COVID-19. There is also the Go Green Inclusive Financing Program of the Land Bank

of the Philippines, which while not COVID-related, is a concrete example of MSMEs linking together the inclusive, recovery and green elements.

In conclusion, it bears reiterating that the COVID-19 crisis has put the spotlight on the importance of building resilience for future crises and risks such as climate change. Green finance policies are needed not only for greening purposes but also to ensure recovery is inclusive since those at the base of the economic pyramid are hit hardest by the ongoing pandemic and will also bear the brunt of climate change. Greening the COVID-19 response is not an act of charity; there is a clear business case for it. There are already examples of climate change mitigation and adaptation policies that offer potential business opportunities and which support MSMEs to become green(er).

## Q&A SESSION

As there was no time left for a Q&A, the moderator wrapped up the session by highlighting two key learning points that had emerged. One, if anything COVID-19 has shown that the future is going to be digital, and regulators will need to continue balancing innovation with the risks that rapid digitization can pose; two, not only does this digitization journey have to be inclusive and not leave behind anyone by remaining aware of the needs of different groups, it also has to be backed by a commitment to ensuring that recovery is sustainable.

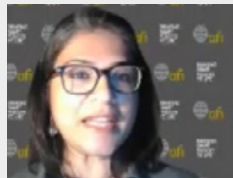
WEDNESDAY, 2 DECEMBER 2020  
DAY 2 - OPEN BANKING AND OPEN API

## SESSION 5: IMPACT OF COVID-19 ON SDGS AND KEY RISKS IN COVID-19 DIGITAL FINANCIAL TRANSFER

### MODERATOR

**ABAN HAQ**

Project Lead, Digital Financial  
Champions, Alliance for  
Financial Inclusion



Session Five explored how advances in DFS can enable governments to mitigate the adverse effects of COVID-19 and sustain progress towards the 2030 agenda.

It also sought to highlight risks that have emerged in the DFS sphere during the pandemic, specifically in the use of digital transfers for vulnerable segments.

## FINANCIAL INCLUSION AND THE SDGS: OPPORTUNITIES TO REPORT, AND INSIGHTS FROM THE SDG COMPENDIUM

**DAVID SYMINGTON**

Policy Advisor, Fintech  
and Digital Payments Office  
of the UNSGSA



In September 2015, the UN General Assembly adopted a plan of action for people, prosperity and the planet titled, “Transforming the World: the 2030 agenda for sustainable development”. Better known as the SDGs, this ambitious set of 17 goals do not specifically target financial inclusion but for many of them, greater access to financial services is a key enabler. Moreover, there are seven SDGs that reference financial inclusion as a target: SDG1 eradicating poverty; SDG2 ending hunger; SDG3 health and well-being; SDG5 gender equality; SDG8 promoting economic growth and jobs; SDG9 supporting industry and innovation; and SDG10 reducing inequality.

Financial inclusion is not a goal in itself; it is a means to creating better development outcomes. Advocacy around financial inclusion should thus not only be about making transfers or access to credit easier, but as an opportunity to improve overall human and social development. There is a growing base of evidence of how DFS are creating this means to an end of achieving better social and economic outcomes.

For example, in relation to SDG1, ending poverty for all, an MIT study found that the spread of mobile money in Kenya lifted roughly one million people out of extreme poverty from 2008-2014, equivalent to two percent of the population. On SDG2 eliminating hunger, the Indonesian experience of digital finance inclusion saw 1.4 million recipients covered under the subsidized rice program move out of extreme hunger. Within this 1.4 million, 9 out of 10 moved from extreme hunger to outside of hunger, a result based on the incentive structures and voucher structures around the digital payments. In Bangladesh, SDG3’s goal of better health was achieved with mobile money when they managed to get enough community health agents to register a million new mothers for maternal and health programs.

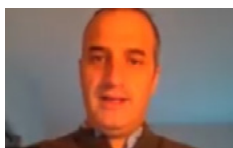
There is scope to document the progress in relation to financial inclusion targets like these, including through the SDG reporting process for every country. While the contents of these reports are determined by the respective countries, AFI members can encourage national bodies to report on financial inclusion indicators. The Fintech and Digital Payments Office of

the UNSGSA has collaborated with Better than Cash Alliance and the World Bank to publish a compendium of how DFS supports the progress of 13 of the 17 SDGs. This is currently being updated to take into account the impact of Covid-19.

Finally, while there are many challenges with utilizing DFS at this time, there are also new opportunities for this to play key roles in supporting social and development outcomes. For example, through the onboarding of millions of new customers for social security payments, or the utilization of digital platforms for SMEs to sell products and explore markets, or the utilization of digital online payments for consumers to shop for services and goods. Similarly, with needs related to education, health and work – digital platforms have offered many opportunities in this regard.

## RESPONSIBLE PRACTICES TO ADDRESS SEVEN MAJOR RISKS IN COVID-19 DIGITAL FINANCIAL TRANSFERS

**RAFE MAZER**  
Innovation for Poverty Action



This presentation shared the findings of a Working Group comprising a diverse set of stakeholders (governments, humanitarian representatives, researchers, market facilitators), which set out to discuss experiences with Digital Financial Transfers (DFTs) during COVID-19, including the most significant risks faced by such programs during this period. The pandemic created a situation where making social welfare payments via digital means was not only good for inclusivity but also essential given the challenges of limited mobility due to lockdowns in many markets. There were a lot of quick responses and innovations during this time, many of which have been quite successful. The Working Group, however, also identified seven major risks and solutions that have been or could be implemented to address these. Further details can be found in the Working Group's report that is available online.

### 1. Inadequacy of complaints feedback mechanisms:

When rolling out programs quickly for new populations, it may be difficult for them to access customer care or perhaps customer care will be overwhelmed. Complaints data from markets like Uganda showed a significant drop in mobile network customer care volumes during the pandemic not

because people had less problems but because the customer care was short-staffed. The Krishna system in India is a good example of where a single integrated complaints handling mechanism was built to address the challenges of adequately managing complaints during a crisis. Alternatively, if communities are inaccessible, having local community leaders form teams to monitor the situation and provide feedback is a good way to ensure a program is being rolled out effectively. It is also possible to be creative and have randomized SMS or integrated voice-response based surveys of beneficiaries to help ensure that everyone gets better services.

**2. Risk of financial and digital illiteracy:** There are a lot of risks for new populations with new technology. Some people receiving payments via digital channels may have limited prior experience with these devices or never opened an account like this before. They are susceptible to falling victim to fraud and fake government transfer schemes. The World Bank's 'Integrating Financial Capability into Government Cash Transfers' Report (2018) is one resource that can help address this situation. Another is the financial literacy training toolkits for refugees developed by UNCDF. In fact, there is a lot of literature on effective training for hard to reach populations that can be leveraged, whether this is to do with literacy or onboarding of people or account registration.

### 3. Exclusion of either current beneficiaries under a cash program, or potential beneficiaries:

Many welfare transfer programs under COVID-19 are reaching a much wider range of people than previously targeted. The challenge is ensuring that no one is left out, including seeing that those receiving cash payments before agreeing with the digital switch. In some cases, like in Colombia, both cash and digital options are given because it is not feasible for everyone to switch to the latter. Similarly, there are situations where women have limited mobility due to cultural reasons; how does one ensure that they get access? This is a risk that is less about mitigating a risk and more about doing the work to ensure inclusivity in the roll-out of programs.

**4. High transaction failure rates:** With the increase in transaction loads, the risk of failure becomes even more important. The solutions to this lie at two levels. On the regulatory side, one can set a maximum permissible number of failed transactions or monitor failure data to pinpoint where this is

occurring: Is it certain locations? With accounts just registered? This data can then be used to work with the providers on improvements. From the provider's side, having specialized customer care desks and processes can effectively resolve failed or incorrect transactions. In mobile money, there are special customer care desks that only handle payment reversals, and transaction errors. This can be replicated to resolve high transaction failure rates.

**5. Lack of knowledge or information about the nearest cash help-point:** Another significant challenge is how at the same time more people wanted to use an agent to cash out, there were fewer mobile money or bank agents available during COVID-19, or they had less liquidity since they lacked super agent networks or agent network managers giving them extra cash. To resolve this, it is the role of regulators to actively engage more providers, and to do more than just hold them to certain standards. For consumers, there are examples of cash-in cash-out network mapping whereby tools can be created for individuals to find agent locations. Such an approach has been implemented in India, Kenya and Rwanda.

**6. Overcharging fees for cash-out and transactions:** DFS surveys show that in some markets, the incidence of overcharging fees can be as high as 30 percent of users. There is also evidence of agents in the social payments sector preying on those with less knowledge about their rights or do not know how to check their receipts. This is a supervision challenge. One of the best ways to check overcharging is through mystery shopping. Have consumers go on a particular transaction before asking them in a questionnaire, questions related to this experience, such as were there informal fees? A check of the cashbook against the debit receipt on phones may surface discrepancies and evidence of overcharging. Another approach is to work with provider networks to raise consumer awareness that this is not permissible or put up signages at agent locations regarding not paying extra fees.

**7. Overcrowding and health and safety risks at cash-out points:** COVID-19 protocols specify social distancing but at the same time, there is a greater push for money to reach a wider range of population that needs this urgently. This can result in overcrowding and health and safety risks at cash-out points. One way to resolve this is by increasing wallet transaction limits so people do not have to cash out, another is to remove or reduce transaction

fees. When the digital transaction is free, people might be more likely to see the funds digital. The rollout of payments can also be staggered to reduce the possibility of long queues at agent locations. Where agent operation hours have been reduced, there can be agreements with providers regarding provision of protective equipment such as masks, hand sanitation, and training for agents and bank staff on COVID-19 protocols. This is one way of keeping beneficiaries and frontline workers safe.

## OPEN DISCUSSION AND Q&A

**Question 1: Are all risks created equal? Do some matter more than others? Do you find policymakers more prepared for some risks than others?**

A: Not all risks created equal. The way to think about this is to ask what risks are particularly unique or more significantly exacerbated by COVID-19 and start with those. One that jumps to mind is the risk of exclusion. As countries across the globe try to expand social payments to a broader population, they continue to face the challenge of reaching people who cannot be reached. Surveys show people still having to sacrifice food and other basic essentials during this period. At the core, what matters most is "do these people get the funds?" because we are talking about saving lives. There are also user-side challenges where the complaints mechanisms and financial and literacy aspects come in. There is a need to monitor overcharging, but this is perhaps a second-level priority since it will not stop the deployment of payments.

The critical role of trust in DFS was highlighted in relation to vulnerable people receiving digital payments for the first time. How does one ensure that new customers who are not familiar with formal financial services or DFS have good user experiences? Or that there is trust so that opportunities to access government emergency payments as a gateway to broader usage of DFS and for DFS to have good social and economic outcomes, can be maximized. If there is fraud or overcharging, the lack of complaints or advice mechanism can undermine potential achievements that can be made.

**Question 2: In terms of consumer awareness especially in rural areas, how effective is disclosure as a means to achieve trust, decrease fraud, etc.?**

A: Disclosure is essential but insufficient. You have to disclose the terms of a product for consumers to understand it and trust you, not feel tricked or cheated



in the long run. Compared with digitization, disclosure is for your laziest customer. It provides the minimum of what everyone has to know. Digitization, on the other hand, is exciting because it is easy to quickly test the different formats of conveying information and seeing which one is the best. So one needs to see how to build on disclosure standards so that consumers become more informed and engaged.

In Colombia, there was a program around welfare payments where they brought tablets containing information and a training video. These were passed around to ensure everyone was aware of how to use these accounts.

For rural populations like those in Bangladesh, limits imposed on many low-end handsets — these do not read the Bangla script and it is illegal to phonetically transcribe the Bangla language into Romanic letters — were overcome through integrative voice response mechanisms like audio recordings.

In Pakistan, the response to COVID-19 was to use radio in local languages and SMSes to ensure the information on social safety net programs reached those in rural areas. Besides innovation, understanding what the rural community looks like and recognizing that it is diverse and has many segments is a necessary first step.

THURSDAY, 3 DECEMBER 2020  
DAY 3 - E-KYC AND DIGITAL ID

## SESSION 6: STATE OF E-KYC AND DIGITAL ID

### MODERATOR

**RITESH THAKKAR**

Senior Manager, EECA &  
Asia Region, AFI



The moderator set the stage for Day Three of the program by noting the previous sessions had shown how digital disruption of the financial sector is a global trend that is driving increasing choices for consumers and changing their behavior.

Significant changes are expected as market players adjust to a digitally enabled economy and regulators need to provide better outcomes for customers and manage the risks of a new ecosystem appropriately. The following observations were made:

An increasingly **customer-centric** regulatory agenda is compelling institutions to leverage new technologies to give customers more control over their data and identity in the digital economy.

For a truly **integrated digital ecosystem** to work, businesses and individuals must be able to seamlessly navigate across ecosystems without having to endure repetitive authentication and onboarding processes.

Developing efficient and effective e-KYC systems remains a common industry objective and a formidable regulatory challenge. However, **harmonizing industry standards with risk appetites** for new technologies is a frequent stumbling block to industry-wide KYC initiatives.

Providing a cross-industry, cross-sector, verified and enriched digital ID would eventually provide the foundation of a **trust network** where customers participate and control their own data. Such access to simplified digital products and services will be the key enabler to digital transformation.

## STATE OF E-KYC AND DIGITAL ID

WIJITLEKA MAROME  
Bank of Thailand

The Bank of Thailand approaches the regulation of the country's digital financial services ecosystem collaboratively. Its objective is to enhance the overall competitiveness of Thailand's financial services sector to ensure the sustainability of the country's financial system. In short, BoT works with its stakeholders in both the public and private sectors for mutual benefit.

The Thai DFS ecosystem comprises two main parts: the e-KYC or digital ID platform that connects the relevant parties to a transaction (such as the financial institution, third-party service provider and customer); and the e-KYC process used for the identification, verification and authentication of a customer's digital ID.

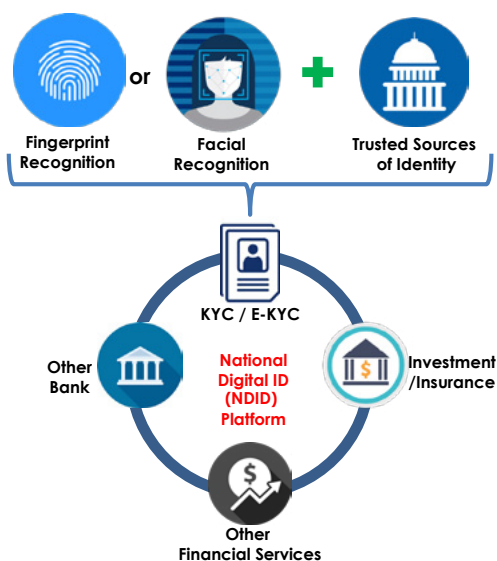
BoT takes the view that an effective e-KYC solution is one that can run a complete e-KYC process, thus increasing efficiency and savings on the cost of doing

business for financial services providers, which they can then pass on to their customers. To this end, an e-KYC solution is an important building block for developing digital financial services in order to increase the financial sector's competitiveness to the benefit of the overall economy.

BoT considers e-KYC as foundational for all digital financial services and as one of the most important tools to reach those without bank accounts in order to increase financial inclusion. This importance has been amplified by the COVID-19 pandemic.

For example, the conventional KYC process to open a bank account (or onboarding a new customer) involves customers presenting themselves in person at a branch of the financial institution. Thus, by default, it excludes those who do not have access to a branch whereas e-KYC obviates such a need. The customer is also expected to present the bank officer with credentials such as a physical citizen ID card which the bank officer relies on to verify the customer's identity. There is potential for human error from the imprecise subjective process of identification, and also from forgery of the physical ID.

## National Digital Identity as a Key Enabler for Digital Financial Services



- **Biometrics technology**, within **KYC/e-KYC** process, is adopted to provide **identification and verification** for bank account opening digitally.
- Combined with supportive regulations and effective business rules, e-KYC will enhance **financial inclusion and security** from frauds and misuses of individual's identity.
- **National Digital ID Platform** is the **open and interoperable infrastructure linking relevant parties together** in order to share information for identity verification and authentication.
- The e-KYC projects are being tested in the **BOT regulatory sandbox** and there are 7 financial services providers allowed to provide services in the general public in this year

Thailand's e-KYC process combines biometric technology such as fingerprint or facial recognition with data from trusted sources such as a citizen ID card or passport. This increases the effectiveness of customer identification, reduces the risk of forgery and promotes accessibility of digital financial services and facilitates the virtual onboarding of new customers. Combined with supportive regulations and effective business rules, e-KYC will enhance financial inclusion and security from fraud and misuse of customer identity.

National Digital ID (NDID) is the common, open and interoperable e-KYC platform that connects the parties to an e-KYC transaction in order to share information for identity verification and authentication. It is a key enabler of DFS in the country; NDID complies with international standards of security, thus supporting companies in doing business globally and promotes pervasive online transactions. Any exchange of data over the platform is subject solely to the owner's consent. Data is distributed over the platform but is not stored on it, but transaction logs (a sequential record of all changes made to a database while the actual data is contained in a separate file) are kept for future reference.

### Q&A SESSION

**Question:** What was BoT's role in the establishment of the National Digital ID platform?

BoT acts in the role of a facilitator and does no implementation. The parties most-ready to use the NDID and most-needed for its usage are the banks, which are under BoT's regulation. Hence as the bank regulator, BoT provides for their collaboration to use the NDID, such as the setting of common standards and business rules to conduct the e-KYC process. e-KYC is just the first use for the information-sharing NDID platform. Other information, such as bank statements and credit ratings can in theory also be shared over NDID.

### MODERATOR'S SUMMARY

BoT's approach has three main pillars: An ecosystem approach towards digital transformation of its financial sector; customer centricity; ensuring convenience for a high take-up rate and usage of the platform among the general public; and a common infrastructure for all stakeholders.

### How the Thai e-KYC process works on its NDID platform)

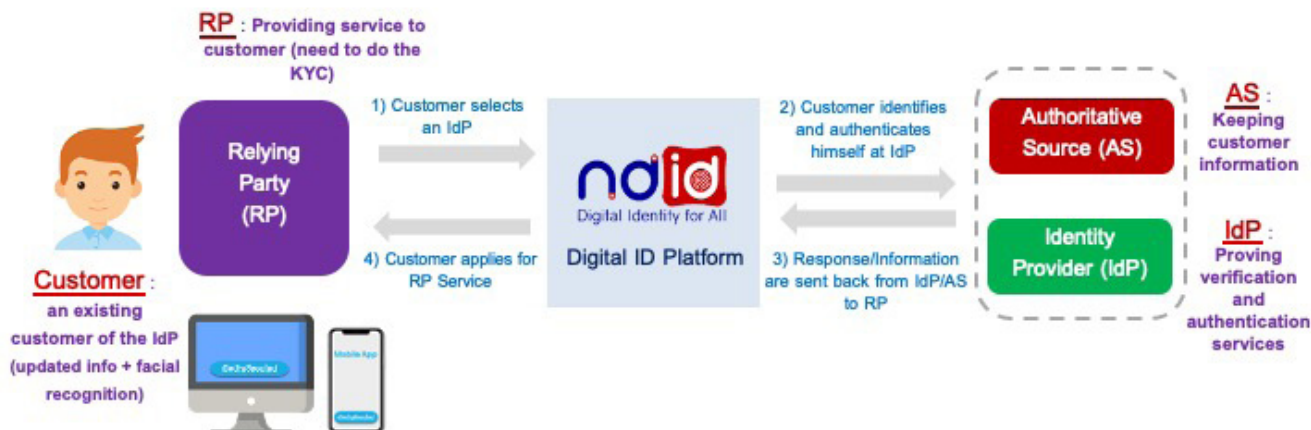
When a customer wants to open an account at Bank A, it is considered the Relying Party (of the e-KYC platform) and is obliged to conduct the e-KYC process.

From Bank A's website or other digital channels, the customer selects an Identity Provider, such as Bank B where he or she holds an existing account, that provides verification and authentication services via the NDID platform to verify and authenticate his or her identity.

In this case, Bank B is the Identity Provider that holds the customer's data and is also considered the Authoritative Source the customer's data has already been authenticated (when the customer opened an account with Bank B earlier).

The customer's data is then shared by Bank B with Bank A, where the customer wants to open an account.

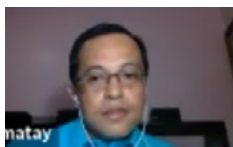
This example illustrates that the NDID platform is designed for banks (and third-party providers) to share already authenticated information among themselves.



## CURRENT STATUS OF E-KYC AND DIGITAL ID REGULATIONS: PHILIPPINES' E-KYC AND DIGITAL ID

### RUEL BUMATAY

Deputy Director, Bangko  
Sentral ng Pilipinas



Bangko Sentral ng Pilipinas (BSP) considers e-KYC an important regulatory tool to broaden financial inclusion because of its potential for innovation that makes financial services more widely accessible. With this in mind, the country's regulatory framework was designed from the outset to anticipate the implementation of a national digital ID system and platform.

The Philippines Identification System Act aims to establish a single identification system for all its citizens and resident aliens in the country to reduce fraud, simplify public and private transactions and facilitate onboarding efficiency. It sets out a "central identification" platform known as PhilSys, which relies on the national ID system known as PhilID for its e-KYC processes.

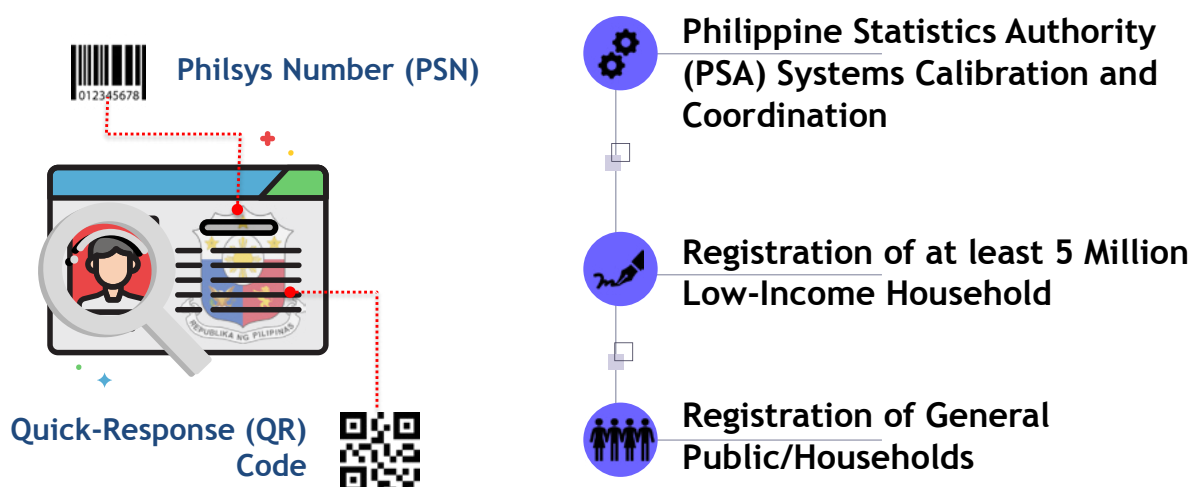
PhilID is recognized as an official document for financial transactions and the government is currently enrolling the population to its database. Each PhilID is assigned a unique PhilSys Number which is held by its owner for life and has a QR code for easy verification in physical use.

BSP has established a stakeholder collaboration and coordination mechanism between the private and public sectors on the implementation of PhilID, especially in regard to the activities of BSP-supervised institutions and their industry associations.

In the fourth quarter of 2020, the Philippine Statistics Authority conducted a systems calibration and coordinated with various agencies and stakeholders to register at least five million heads of low-income households with PhilID. Registration of the general population begins in 2021 and is expected to cover all citizens and resident aliens by 2022.

Some key outcomes of the introduction of PhilSys and PhilID so far include reduced time spent on due diligence for low-risk clients, such as reduced face-to-face, in-person contact. More efficient distribution of social cash transfer programs, such as during the quarantine

## Current Status of E-KYC and Digital ID Regulations



periods for COVID-19, where the number of beneficiaries rose to 11.6 million. Of this figure, 7.3 million were new digital transaction accounts. PhilSys and PhilID are also expected to increase the reach of the Pantawid Pamilyang Pilipino Program for the hardcore poor which aims to break the intergenerational cycle of poverty by encouraging recipients to invest in their children's and their own health, nutrition, education.

Bumatay reiterated the key opportunities of e-KYC and digital ID for financial inclusion by noting that transactions such as account opening, transaction authentication, and account validation are made highly efficient and cost-effective. He also noted that studies conducted by the Asian Development Bank corroborate the Philippines' national experience.

Particularly in the case of social transfer payments, in countries such as the Philippines, these can be informal community networks that channel payments based on trust. In such a case, digital ID and transaction accounts reduce the risk of misdirected payments.

Similarly, the accurate identification of social welfare beneficiaries and efficient delivery of public services facilitated by PhilSys and PhilID will also enable payments to reach those in remote areas faster and more cheaply by improving coverage and robustness of credit assessment systems of financial institutions and FinTechs with a unique identifier.

In terms of commercial benefit, e-KYC can reduce onboarding costs by as much 80 percent by providing a unique identifier across financial sectors, improving compliance with requirements such as for AML/CFT regulations. This makes customer acquisition a viable business proposition for new players in the market.

Moving forward, BSP's Digital Payments Transformation Road Map 2020-2023 identifies some broad challenges. The first relates to the behavioral change among users needed for networks to function efficiently, i.e. the more widely used they are, the better they will work, especially between the public and private sectors. In this regard, there will need to be awareness and promotion campaigns to shift mindsets towards utilizing digital payments.

The second challenge is systemic and arises from the need to use smartphones for users to make optimal use of digital payments. This can increase the digital divide because it favors those living in urban areas, and puts those residing outside Metro Manila at a disadvantage due to the quality of connectivity and because internet services are less widely available.

Bumatay noted that the building of internet infrastructure and its maintenance and upgrading can be likened to the need for roads and bridges, especially for rural communities.

Another challenge that affects the effectiveness of digital solutions are banking rules. While digital solutions such as e-KYC may make onboarding easier, those from lower-income backgrounds may struggle to meet owner-identification requirements for the opening and holding of bank accounts in regard to minimum balances, and in keeping their accounts active over a minimum period of time.

#### Q&A SESSION

**Question 1:** The challenges of shifting mindsets towards digital, the digital divide and access to a quality internet connection are shared by many countries. What has BSP's response been to these three challenges and what are its specific initiatives now, with the collaboration of stakeholders, to ensure the digital transformation happens?

A: First, we create public awareness and promote the use of the digital platform among people to avail themselves of financial services and to open accounts. Second, the regulations are dynamic. We adopt regulations that promote financial inclusion.

**Question 2:** What are some of the safeguards to mitigate the risks of money laundering?

We require financial institutions to conduct a risk assessment of the e-KYC technology to be used for the products they will offer customers. Their assessment should indicate they have the systems in place to mitigate money laundering and terrorism financing risk. Although BSP's prior approval is not needed for them to offer e-KYC, BSP validates their chosen platform during inspections of these institutions. Most financial institutions that offer e-KYC voluntarily provide some presentations to BSP to ensure they are within the parameters set by the regulations.



## ENABLING E-KYC FOR THE FINANCIAL SECTOR

IAN LEE

Bank Negara Malaysia



Bank Negara Malaysia BNM considers e-KYC as foundational for the innovation that will lead to the digitalization of Malaysia's financial sector. It issued its Policy Document on e-KYC on 30 June 2020 to streamline and catalyze industry-wide adoption of e-KYC technology. The Policy Document sets out best practices for the security and integrity of the customer onboarding process and the parameters of their implementation. It identifies and clarifies what BNM considers as desirable outcomes arising from the use of e-KYC. Broadly, these are:

- > The safe and secure application of e-KYC technology in the financial sector.
- > A conducive environment for the secure digital onboarding of customers.

- > Lower onboarding costs for both users and providers.
- > Greater innovation by the private sector in its digital financial services for customers.
- > An inclusive transition to a digital economy.

Lee provided insight into how the Policy Document came to be informed. BNM's "outcomes-based approach" to e-KYC began with the question of how the technology could be optimally implemented in Malaysia. This required a review of BNM's existing regulatory requirements and their effectiveness for the current and future financial landscape.

With the participation of the private sector, BNM used a regulatory sandbox to trial alternative e-KYC solutions, and used the learnings to identify areas in need of regulatory clarity and how to effectively facilitate implementation models for the private sector. The Policy Document is neutral on the choice of technology solutions in order to promote market competition and innovation that leads to greater choice and better solutions for the customer.

## Enabling e-KYC for the financial sector- Bank Negara Malaysia

### Key requirements of the e-KYC Policy Document

#### 1 Role of Board

"The Board is responsible to approve e-KYC implementation and set effective implementation of risk management procedures.."

#### 2 Risk based measures

"FIs shall ensure that e-KYC measures undertaken are commensurate to the risk of inaccurate identification.."

#### 3 Desired outcomes

"FIs shall ensure that the e-KYC solution is robust and capable of distinguishing between genuine and non-genuine identities.."

#### 4 Reporting obligations

"FIs shall record and report the performance of e-KYC solutions, including FAR every 6 months.."

#### 5 Additional safeguards

"A credit transfer check must be in place for an FI offering higher risk products e.g. CASA through e-KYC.."

#### 6 Regulatory process

"Banks and insurers may proceed to implement e-KYC upon 14 days of notifying the Bank.."



BNM also considered the following factors for its Policy Document for their effects at a national level:

- > The presence or absence of a national digital ID, which will affect the requirements of e-KYC policies.
- > The maturity of the technology used for different e-KYC solutions in the country and internationally, given that different authentication methods rely on different technologies.
- > The level of financial inclusion in the country.
- > The ongoing changes to lifestyles wrought by COVID-19 that preclude in-person transactions and necessitate lower-touch or virtual ones.

Lee highlighted key requirements of the Policy Document: First, it makes a financial institution's board of directors responsible for ensuring that an effective risk assessment process is conducted for an e-KYC solution before it can be considered for approval.

The onus is thus on the board to be cognizant of how e-KYC changes existing risk assessment processes, i.e. how to identify their potential risks for the business and then effectively manage these risks upon e-KYC implementation.

Second, "Financial institutions shall ensure that e-KYC measures undertaken are commensurate to the risk of inaccurate identification." In other words, the more complex a financial product, the greater the consequences of misidentification and the stronger the risk mitigation measures and additional safeguards would need to be. For example, full-fledged current accounts and savings accounts would require a more precise e-KYC solution and risk mitigation measures than a basic credit card account.

Third, in order to ensure the adopted e-KYC solutions are fit for purpose when used for a product or service, financial institutions are required "to record and report the performance of e-KYC solutions, including FAR (false acceptance rate) every six months." FAR is a measure of the accuracy of predictive algorithms used in AI-based machines, such as for facial recognition of customers, who are then assigned a score for a likeness match. In brief, FAR is a measure of how well AI decides to on-board a customer based on e-KYC criteria. Because this decision is made by a machine or AI, there is a real need for policy clarity on AI decision-making. The desired policy outcome here is for the adoption of e-KYC solutions that are "robust and capable of distinguishing between genuine and non-genuine identities."


Fourth, additional safeguards, such as a credit transfer check, are required to be conducted by a financial institution offering high-risk products through e-KYC.

Fifth, the regulatory process is meant to ensure the desired outcomes can be achieved. In this case, they are the safe and secure application of e-KYC solutions as well as greater market innovation. These seemingly opposite outcomes are reconciled to an extent by there being no requirement for financial institutions to obtain BNM's prior approval to implement e-KYC solutions, but may proceed to implement e-KYC upon 14 days of notifying BNM.

Looking towards the immediate and already rapidly evolving future, Lee then identified some continuing challenges for regulators in the landscape of e-KYC and digital ID in the following questions:

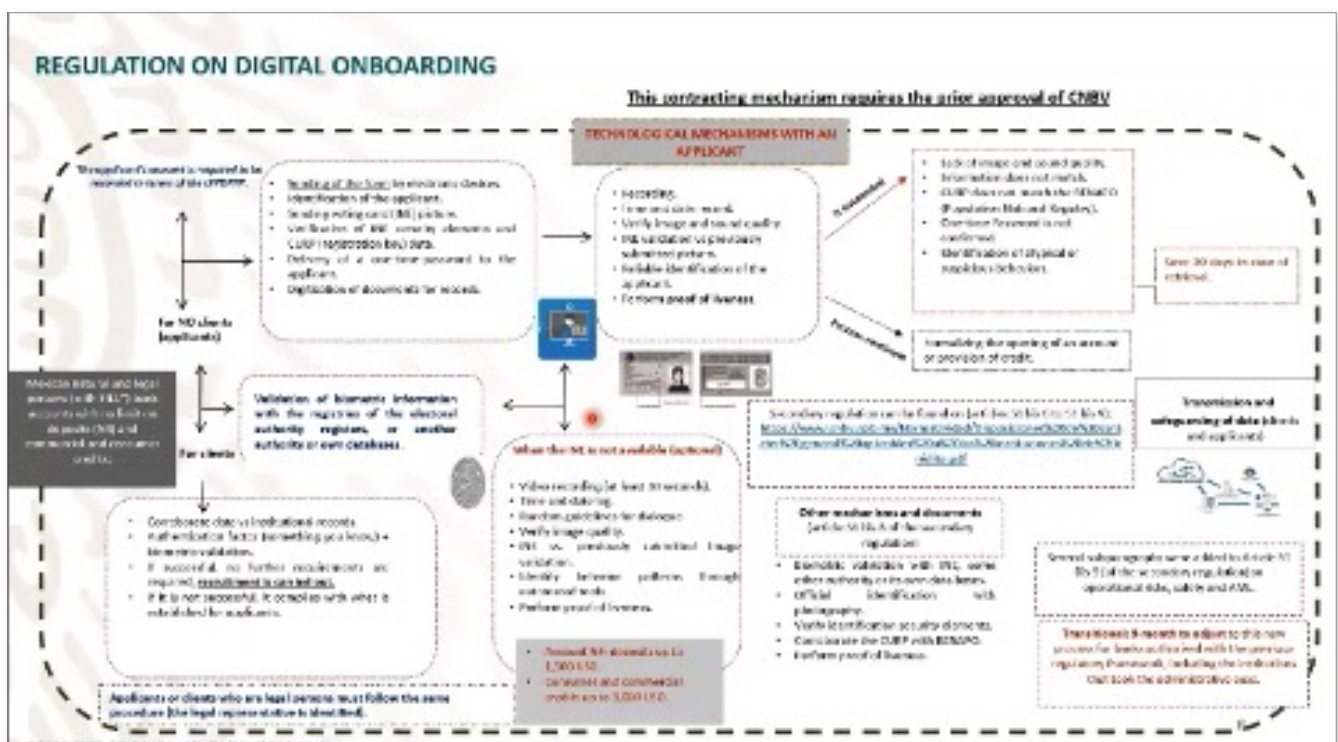
- > For countries with a national digital ID scheme, how have existing customer due diligence requirements been calibrated to support digital onboarding? BNM has decided to supplement existing requirements with additional policy principles and safeguards.
- > To drive e-KYC adoption in the financial sector, should regulators adopt an approval regime for solutions providers or allow the market to make its own assessment and choose from the available solutions providers that are left standing?
- > Given the ongoing and rapid technological disruption of the financial sector, how can policy be made adaptable to harness the better effects of disruption while maintaining policy clarity? In seeking a balance between providing guiding principles and prescribing rules for the market, where is the sweet spot? How should requirements be calibrated accordingly? By nature, regulators are not-so-agile in shifting or changing existing regulation regimes wholesale.
- > What would be the role of e-KYC and identity solutions providers or vendors in a country where digital ID is prevalent and available? Conversely, what is the envisaged role of these entities in a landscape where national digital ID is not yet available? In the quest for both open standards and interoperability, how would all e-KYC processes converge towards a national digital ID, or is there still space of solutions providers to complement the services already provided by the national digital ID?

**GILBERTO ARTURO PEREZ  
HERNANDEZ**



Financial entities must have data for low-risk accounts (full name, personal address, date and country of

Banks have been allowed to remotely open accounts (of up to certain qualifying levels) for customers, i.e. without the customer needing to apply in person at a physical branch, since 2017. This regulation on the remote identification of customers included those applying for consumer and commercial credit. It was



issued to help prevent, inhibit, mitigate and detect any unlawful conduct aimed at impersonation of identity.

CNBV issued updated regulations applicable to banks in October 2020 for the remote identification of customers. These strengthen the identity verification process by requiring image captures of clients' identification documents; proof of "aliveness" using video selfies; and biometric validation referenced against the official database of the electoral authority - the biggest biometric database in Mexico covering 95 percent of the adult population.

The updated regulations now also allow legal persons to open bank accounts remotely via legal representatives, using the firm's electronic signature. It also provides for separate application tracks for existing bank clients and new clients in an effort to make the regulations more flexible. The allowance for video selfies to be used by customers to identify themselves also lowers onboarding costs, as only online video conferences could be used previously, which was very expensive to implement for banks.

#### OPEN DISCUSSION AND Q&A

The moderator took the question from the Bank of Cambodia and invited the Bank of Thailand to share its experience on this point.

**Question:** Since e-KYC development can involve various stakeholders such as the national security office or interior ministry in some countries, what is the role of the Central Bank in coordination with these stakeholders?

**A:** For the (Thai) digital identity card, its development does not only involve the Central Bank of Thailand and is much broader than that because it covers all electronic transactions and digital channels. So it also involves the Electronic Transactions Development Agency, the lead regulator for the digital ID. So what is the role of the central banker? Basically (BoT) regulates based on activity, that is, whatever activities under its regulatory framework should be enabled by e-KYC. One of the most important things about this is the secured channels (for transmission) and also the security of the person's information under the Personal Data Protection Act. So in order to transport or process the data of the customer, the e-KYC requirements are meant to ensure (the mode of transmission is secure) and ensure the protection of the customer's data privacy.

**Moderator:** As the entire (DFS) ecosystem evolves, there are many options regulators will have, depending on their risk appetite.

THURSDAY, 3 DECEMBER 2020  
DAY 3 - E-KYC AND DIGITAL ID

## SESSION 7: E-KYC AND DIGITAL ID: REGULATORY APPROACHES AND INNOVATION

#### MODERATOR

**ELIKI BOLETAWA**

Head of Policy Programs and  
Regional Initiatives, AFI



Noting that the day's first session had provided an excellent overview of e-KYC and digital ID in Thailand, Philippines, Malaysia and Mexico, the moderator proceeded to introduce the presenters from the developed countries who would take participants on a deep dive of the regulatory approaches in their respective jurisdictions.



**ESTONIAN EXPERIENCE: E-KYC AND DIGITAL ID  
REGULATORY APPROACHES AND INNOVATION****RAINER OSANIK**

Accelerate Estonia

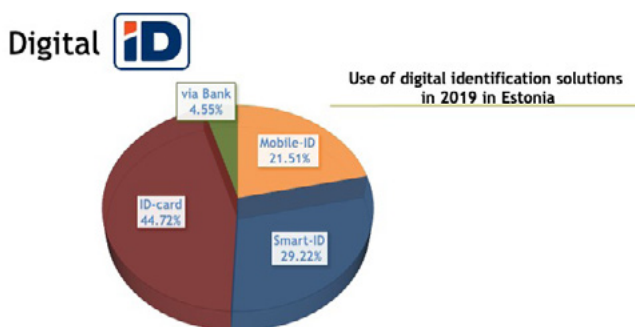


The Republic of Estonia is one of the smaller EU Member States with a small population that has historically been widely dispersed throughout the country. Realizing it could not sustain a large and costly physical state apparatus, Estonia began to digitalize its public services to make them available to everyone, anywhere, even in isolated areas. The government declared access to the Internet as a human right and, coupled with a nationwide digital literacy program from the mid-90s, the Internet became the enabler of effective public services.

Accelerate Estonia is a government innovation lab under the Ministry of Economic Affairs and Communication that was launched in 2019. Its aim is to solve wicked problems (socio-economic issues with confounding factors) and turn them into new ideas that serve citizens and create economic value. It does this by bringing together government ministries, the public and private sector, experts and leaders to build new innovation.

The next e-breakthrough for Estonia is envisioned as something that will allow hundreds, if not thousands, of private sector companies based in the country to achieve viable new business models to solve public services issues currently handled by the state.

Usage statistics (2019) for Estonia's three digital ID solutions are as follows: ID card, 44.72 percent; via Bank: 4.55 percent; Mobile-ID, 21.51 percent; Smart-ID: 29.22 percent.



Accelerate Estonia has so far hosted four “missions,” among which is the e-KYC service solution concept which was an outcome of the first Hack the Crisis online hackathon during the first COVID-19 lockdown in March 2020. (Hack the Crisis has grown into a global movement comprising 68 countries that seeks solutions to ease life during public crises.)

A brief history of the evolution of digital ID in Estonia. There are three types of identity cards in Estonia. In chronological order, the Estonian ID-card is a mandatory identity document for citizens who can use it to communicate directly with government agencies via an assigned email address. It can be used to access health care services, e-banking, and for signing contracts, public transit (since 2004), travel across the EU and European Economic Area, voting (since 2005) and by businesses as customer loyalty cards. Estonia offers 900 e-services to citizens and over 2,600 services to businesses.

To facilitate the above, Estonia adopted the Digital Signature Act in 2000. A microchip was incorporated into the card in 2002; it stores the authorized user's digitized data (full name, gender, national identification number, and cryptographic keys and public key certificates). Ninety-nine percent of Estonians hold the Digital ID card and use it to access 99 percent of government public services. In its first use for e-voting in the 2005 general election, e-votes comprised just 2 percent of total votes cast. In 2019, this figure was 46.7 percent. Some usage figures: 1,403,313 cards have been issued, which have been used more 1,063,459,199 times for digital identity verification, and 1,128,434,390 times for digital signatures.

Mobile-ID (MO BILL ID) is a digital ID card for mobile phones; it is incorporated into a SIM card that can also be used in older mobile phones because it does not require an internet connection to be functional. Introduced in 2007, Mobile-ID has the same functionality as the Digital ID card and can be used to digitally sign documents and vote in elections (via encrypted SMS).

Smart-ID is an app that was introduced in 2017 as an alternative to Mobile ID for use in any smart device as a secure alternative means to access e-services. It requires an internet connection and is downloadable from Google Play and AppStore. It has some three million users throughout the Baltic states who use it to make 65 million transactions a month. It can facilitate biometric authentication such as facial recognition, which Mobile ID cannot.



KYcer is the working name of an e-KYC solution that emerged as the winner in a hackathon organized by Accelerate Estonia in Sept 2019. It is designed to be a fast, reliable and secure platform for the sharing of personal data from government databases to the institutions or parties that request for them. The owners of the personal data to be shared must first consent to their use in this way.

KYcer automatically collates KYC profiles and common KYC data from various databases, including government ones. These KYC profiles are interoperable and reflect any updates to them in real-time.

KYcer mediates between the government and external or private databases, and between private companies. The requesting party (e.g. bank that wants to onboard a new customer) that uses KYcer does not have access to the customer data shared with it nor does it store any of it. For customer data to be accessed by the requesting party, its owner must already have consented to it.

The data owner can choose with whom to share his or her profile data and can view from the app with whom or what parties his or her data has been shared, and other relevant details.

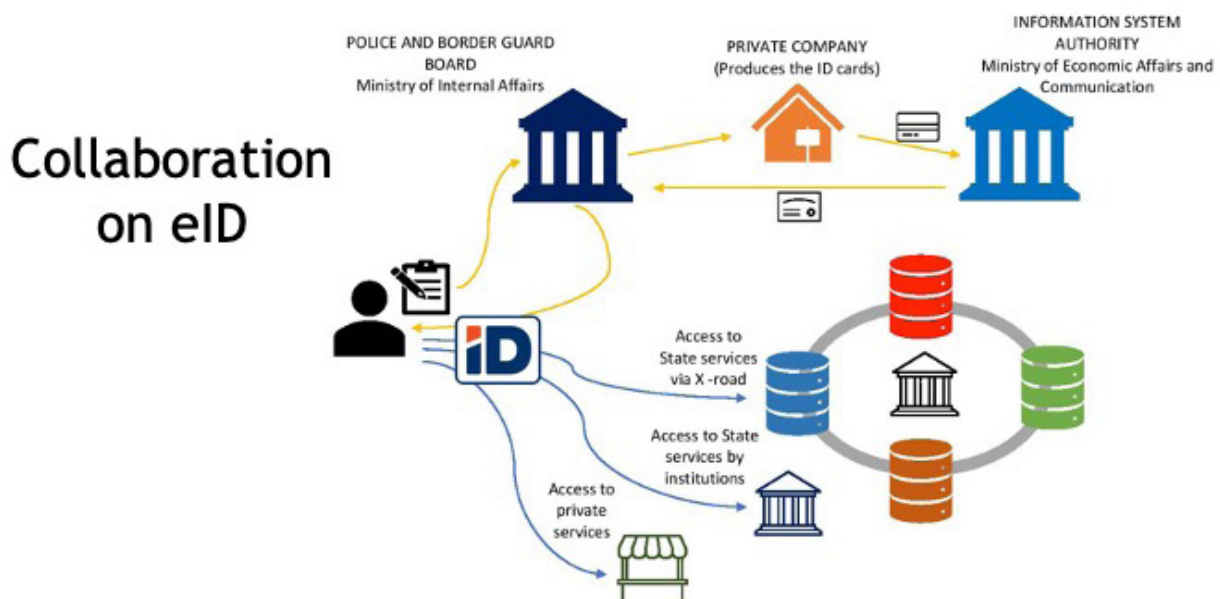
Such user control and transparency alleviate public fears of the misuse of personal data, and are an example of customer-centricity demanded by e-KYC solutions.

KYcer was made in eight, systematic steps:

1. Mapping of all government databases and verifying that they contain all the required data for the types of transactions they will be used for, in machine-readable format (this last part is crucial for an automated workflow).
2. Creation of KYC profiles (private person, legal person, and so on).
3. Mapping the KYC profiles to primary and secondary databases.
4. Designing the platform architecture and workflow.
5. Prototyping using mock data.
6. Thorough legal analysis of the platform, including a compliance check with the General Protection Data Regulation (GDPR).
7. Drafting of laws and amendments to existing laws to enable e-KYC data exchange services.
8. Production of KYcer platform and user interface.

### Digital IDs multiple party production team

The production of a digital ID card involves coordination between the public and private sector. In the public sector, it involves various ministries and agencies. The card is produced by a private company (selected under a state procurement process) and issued by the Police and Border Guard Board under the Ministry of Internal Affairs. Its encryption keys are provided by the Information System Authority under the Ministry of Economic Affairs and Communication.



---

Extending digital ID with e-Residency

- Estonia is creating a borderless digital society for global citizens as the first country to offer e-Residency since 2014
- E-Residency is a transnational digital identity that anyone in the world can apply for to obtain access to a platform built on inclusion, legitimacy and transparency. E-residents then have access to the EU business environment and can use public e-services through their digital identity
- The primary reason e-residents are joining this community is to run a trusted location-independent EU business online with all the tools needed to conduct business globally
- By have now over 73 000 e-resident with over 14 000 companies established by them. Tax revenue created over 50 million Euros

---

Digital cross-border solution

## e-KYC solution visioning

- In 2018, after thorough analyses of common cross-border problems within countries around Baltic Sea, was discovered that one the biggest issues was data exchange and access to the data for the purpose of fighting with money laundering (AML)
  - Under EU funded DIGINNO (Digital Innovation Network) project were established country workgroups and international workgroup to find ideal to-be module for future cross-border KYC solution [www.diginno.eu](http://www.diginno.eu)
  - In spring 2019 to-be vision was presented by the international workgroup and in the autumn feasibility study and policy recommendations were submitted
  - Already in spring 2019 Latvia and in autumn Estonia started to develop their e-KYC solution based on DIGINNO principles
-

Importantly, with regard to step (7) above, the Anti-Money Laundering Act was amended to add:

- > The definition of KYC data exchange.
- > Principles of collection, transfer and usage of such data.
- > Data security requirements.
- > Service provider requirements.
- > Rule allowing the Minister of Finance to adapt data for KYC profiles.
- > Amendments to statutes of different registers to make it legal for personal data to be shared with a Third Party via an e-KYC service provider, assuming the owner of the data has consented to it.

The planned launch date for KYcer is 1 July, 2021, when the new legal framework takes effect. Its biggest likely challenges can be stated as follows, starting with the hardest, which is the change of mindset required in the public and private sector, more so in the former as government machinery can be slow to change gears. Because of its wide-ranging effects, KYcer's progress may also be slowed by a deficit in political will needed to implement it, depending on the political trends of the season.

When it comes to the general public, surveys show there is a reluctance to share personal data because of a fear it will be disseminated; it should be pointed out that this is the same data required by banks for the application of the same products and services, but in digital form. The fear that one's personal data will be misused is also persistent, given cybercrime, data leaks and cyber attacks of security systems. As KYcer will be linked with the voter database and used to cast votes, it will require constant, vigilant monitoring and management of security threats.

The challenge posed to KYcer from fake news, "alternative facts", and conspiracy theories about big brother is the most well-known one that it faces.

However, the important but less well-publicized challenge faced by KYcer is the partial knowledge on e-ID security and KYC principles in the commercial sector as well as the public sector. A little knowledge without the full picture and understanding can be misleading for the general public and even dangerous. All these challenges are being dealt with to move KYcer ahead.

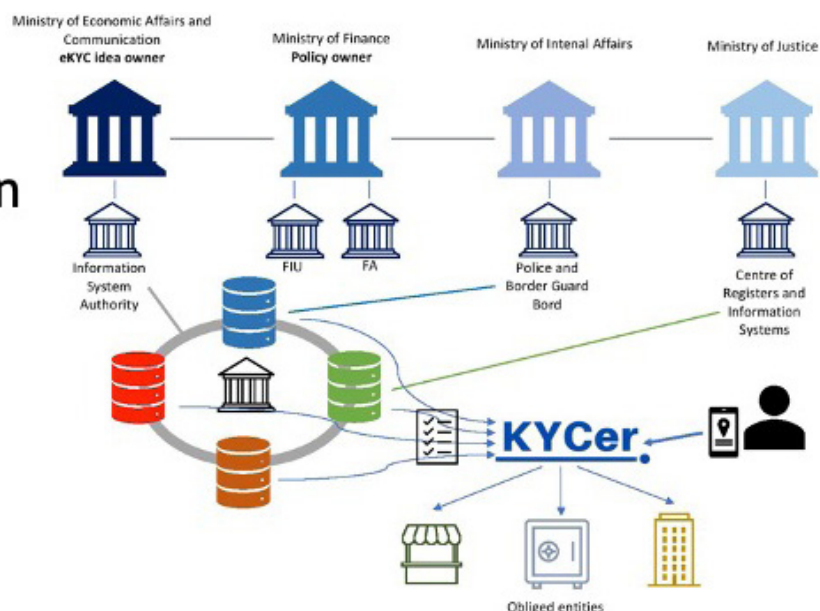
### KYcer coordination

As with digital ID, KYcer is made possible by the coordination of even more ministries and agencies:

- > The Ministry of Economic Affairs and Communication is responsible for e-KYC as the Information System Authority comes under it

- > The Ministry of Finance sets policy and has supervisory roles via the Financial Authority and Financial Investigation Unit
- > The Ministry of Internal Affairs is responsible for security via the Police and Border Guard Board
- > The Ministry of Justice houses the Centre of Registers and Information Systems

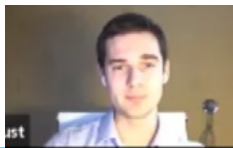
## Collaboration on eKYC



## E-KYC IMPLEMENTATION: PRIVATE SECTOR PERSPECTIVES

### PAVEL SHOUST

Russian Electronic Money and  
Remittance Association



The pivotal roles that e-KYC and digital ID can play in improving financial inclusion and boosting market competition become more apparent by the day. However, there are cases where the existence of e-KYC regulation does not always lead to financial institutions implementing e-KYC solutions. To identify and understand the barriers, e-KYC regulation was considered from the perspective of the private sector.

New regulations are usually viewed with caution by the private sector because they would still be uncertain about how much they would cost to implement, and how much of this added cost can be passed on to the customer, if at all.

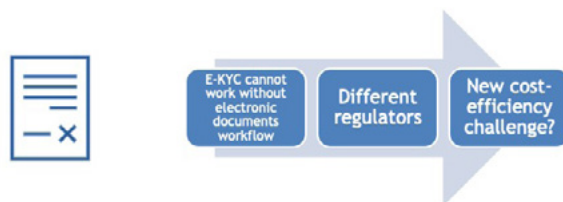
This cautious view can be better understood from a financial institution's organizational capacity to meet, or not meet, the requirements of the regulator. In brief, the relevant department of the financial institution could be understaffed to take on the extra work, or it completely lacks the in-house expertise needed to implement the regulation.

Also, in addition to financial institutions needing to implement the e-KYC requirements of the regulation, they would also be required to conduct an internal risk assessment of such new technology according to Financial Action Task Force (FATF) Recommendations. In Shoust's professional experience, financial institutions are usually wary of being sanctioned for inadvertent non-compliance with regulation.

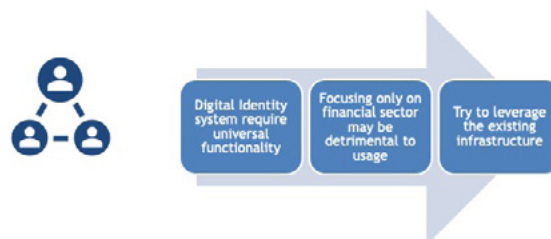
He explained that while regulators deal with the known, i.e. a breach of a regulation is established after the fact, financial institutions must deal with the unknown in seeking to comply with regulation, such as mitigating the risk of a customer doing something illegal in the future.

An appreciation by regulators for how financial institutions see regulation affecting their operations (and, one assumes, vice versa) would help to ensure wider implementation of e-KYC regulations. As to internal risk assessment, a consistent regulatory approach to AML / CFT regulation in different jurisdictions would make it less complicated for a financial institution to determine the potential risks

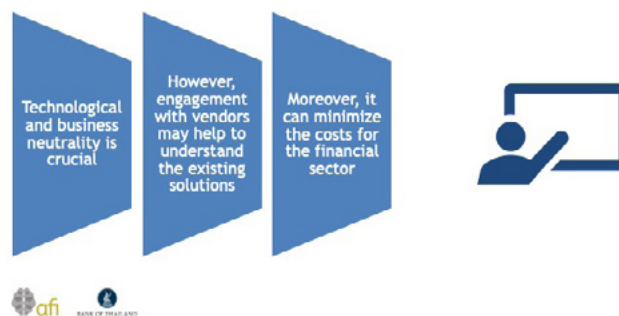
## Electronic documents and signatures



## Make Digital Identity Universal



## Work with vendors



and costs of adopting new e-KYC technology. Shoust then highlighted the following areas and suggested some solutions.

### COORDINATION OF RELATED REGULATIONS

e-KYC cannot work without a certified e-document workflow. However, financial institutions might choose not to use e-KYC because of uncertainty over regulations on trust requirements for e-signatures and e-documents. The issue here arises because e-KYC and e-documents and e-signature usually have different regulators. For e-KYC, this is usually the central bank (among others) while e-documents and e-signatures are usually regulated by a ministry of communication, technology or finance. Requirements under the two different sets of regulations on the same subject in the same jurisdiction have been known to differ; handwritten signatures can still be required when e-signatures can be used.



### ONE SIZE FITS ALL (UNIVERSAL) FRAMEWORKS

Implementing e-KYC in compliance with a universal regulatory framework such as the European Union's eIDAS (electronic identification and trust services) legal framework can prove complicated and thus costly. To reduce the overall cost of compliance, Shoust recommends the implementation of e-signatures in a tiered approach. He noted that the comprehensive national implementation of e-KYC planned by Estonia may be because it was an early adopter of the digitalization of public and private services.

### BROADER USAGE FOR DIGITAL ID

The success of a platform depends on its popularity with users and a high rate of engagement. Shoust recommends that a national digital ID platform should be usable across multiple sectors and not just the financial sector in order to encourage a high enrolment rate. Anecdotal evidence shows a low rate of usage in Russia, where the digital ID system for financial institutions is usable only for the financial sector. In this regard, it is recommended to leverage ID infrastructures that already exists, such as for passports and driving licenses.

### HOW TO CONTINUOUSLY UPGRADE REGULATOR CAPACITY AND LOWER IMPLEMENTATION COSTS:

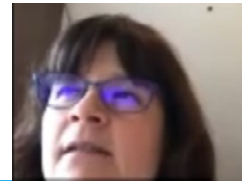
Working with vendors or third-party providers allows regulators to stay abreast of technological solutions that have already been implemented in the market, which can be surprisingly advanced. Solutions for liveness detection and deep fakes, for example, are readily available.

e-KYC regulation is perceived as presenting many uncertainties by the private sector whose concerns are implementation costs, costs to the customer, organizational capacity and possible restructuring costs. To minimize such concerns, regulators could organize vendor presentations of e-KYC solutions for financial institutions that can be integrated into their systems cost efficiently. These solutions may even lower the cost of drafting the regulation. In short, it is strongly encouraged for regulators to work with vendors, while retaining their neutrality and not endorsing any particular technology or vendor.

### E-KYC AND DIGITAL ID: REGULATORY APPROACHES AND INNOVATION IN LUXEMBOURG

#### CECILE GELLENONCOURT

Head of Department, Supervision of Information Systems and Support PFS, Commission de Surveillance du Secteur Financier (CSSF))



In Luxembourg, e-KYC and e-ID or digital ID solutions are part of a response by banks to increased competition from neo-banks, which are fully digital, virtual banks with no physical presence that attract younger customers.

The benefits of these solutions are clearly experienced by banks and their customers in a more user-friendly and faster onboarding process, for example, besides encouraging collaboration or a mutualization of costs and effort by financial sector entities. They have also allowed for business continuity in a time of pandemic, when physical branches are closed, and for safe distancing to be observed.

The context for Luxembourg's regulatory approach toward e-KYC and digital ID is the European Union eIDAS Regulation. The Electronic Identification, Authentication and Trust Services Regulation is a common legal framework for trust services and means of electronic identification in the EU. It specifies the nature of identification checks to be performed but is silent on the mode of performing them.

Because trust services include e-signature, e-seals, time stamping, otherwise physical processes involved in contracting for financial services, electronic identification is essential for remote client onboarding solutions, among others.

The Fifth AML EU Directive (Luxembourg Law of 12 November 2004 (amended) on money laundering and terrorist financing refers to the use of trust services for identification as defined in the eIDAS Regulation as an option for secure remote or electronic customer identification. While it sets out the requirements, it leaves it open for national regulators to define the methods to be used for this purpose.

Because of eIDAS' open-ended specifications on the methods that can be used for authenticating a customer's identity, there is a high level of fragmentation in the APIs used for e-KYC among EU jurisdictions. A new EU strategy on digital finance aims to enable EU-wide interoperable digital ID by 2024. It will be based on harmonized AML/CTF rules and revised



eIDAS regulations that will, inter alia, specify which technologies are used for checking a customer's identity remotely. They will also cover the reuse of customer data, subject to the customer's consent, and facilitate compliance with other onboarding requirements, such as assessing the risks of approving a customer for certain investment products.

The authentication of a customer's identity is possible via live video chat in real time, which is considered equivalent to an in-person, face-to-face identification. However, its requirements must be read in the context of the overall ALF-CFT rules. For example, if there are suspicions of money laundering or terrorist financing activity, or about the authenticity or previously obtained data, live video chat should not be used.

Where a bank engages a third party or external service provider for remote onboarding, it must conduct complete due diligence on the provider according to AML/CFT rules, and to ensure the provider has the technical capacity for the job, including for ensuring the security of the customer's data. The bank must obtain the customer's consent for the sharing of the recording and data with the service provider. The quality of the data used for identification must also be of high integrity, such as an official ID with security features. Banks are also required to retain the video of the authentication process, and both banks and their third-party service must comply with all other requirements for security and data privacy.

Other solutions, without the intervention of a natural person, are not considered equivalent to face-to-face, and require supplementary safeguards to be used. In this regard, CSSF verifies the fitness-for-purpose of the security tools and systems and whether they are effectively integrated with the requirements of the overall AML/CFT framework.

Third-party/external providers that provide so-called Support PFS such as back office services or IT operating services to the financial sector in Luxembourg are regulated. TPPs do not have to be licensed to perform customer identification unless their services go beyond this activity, such as the storage of KYC documents; or if they are required by the bank to keep documents updated and contact customers on their behalf; or if they provide an e-KYC platform for the bank.

TPPs offering Support PFS to banks are licensed and subject to the same requirements as banks because they share the same operational risks that must be mitigated. They are supervised via reporting requirements,

meetings, on-site inspections or by their presenting of specific IT or business solutions they offer the financial sector for analysis by the supervisory authority. TPPs offering Support PFS to banks may be sanctioned for lack of compliance.

Luxtrust has initiated interoperability for Luxembourg's national e-ID (digital ID) scheme (also called Luxtrust) in the private sector with other jurisdictions, beginning with Belgium's national digital ID scheme called "itsme". With this, Belgians may open accounts with Luxembourg banks and vice-versa for example.

Banks in Luxembourg may capitalize on Luxtrust's own e-KYC processes for customer identification and secure communication by delegating it the task of prospective customer identification. Luxtrust then performs its own KYC checks to create an e-ID for the prospect, and first makes the prospect one of its own customers. It then sends the prospect's e-ID data to the bank (first obtaining the consent of the prospect), which assesses the prospect's suitability and risks as one of its customers according to AML/CFT requirements. It may request for further e-KYC documents before electronically signing a service contract with the prospect.

Luxembourg also has centralized KYC repositories. In brief, these are providers of bespoke business-to-business KYC management services that, while not being an e-KYC platform, collect, index and verify data required for KYC for their clients, besides also doing due diligence, risk scoring and offering secure digital storage for all their data from separate sources in one place. Natural persons or individual customers also avail themselves of these services, mainly to reduce the burden of repeatedly presenting the same set of documents for financial purposes.

Another type of related service connects the different parties in a transaction to one another, such as databases with TPPs, e-signature providers and so on. Such providers are not a platform but provide a mediation service.

The financial sector's growing usage of digital/e-ID and e-KYC solutions has efficiency and cost benefits for banks and other financial entities, and their potential to make tedious processes more user friendly will benefit financial inclusion. Not least, COVID-19 will accelerate the sector's digitalization and make demands on regulators to meet novel situations.

While a clear EU-wide strategy is needed to improve the regulatory toolkit, standardization and mutualization of processes would need to fit into the AML/CFT regulatory framework and its specific requirements for different entities. More evidence of the need to meet the digital disruption of the financial sector now is the growing constellation of third-party service providers to the financial sector in Luxembourg, and almost all are being supervised as providers of PSF support services.

#### OPEN DISCUSSION AND Q&A

**Question 1: How do we ensure that digital ID systems are as inclusive as possible, and reach all groups disproportionately affected by financial exclusion, which include women, the rural population and, possibly, displaced persons?**

A: (Pavel Shoust) Digital ID systems are two-fold: enrollment and authentication. What we are referring to here is the enrollment process. What regulators try to do is to make the enrollment process as robust as possible - bulletproof. Unfortunately, this makes it difficult to access. Some jurisdictions have regions that take seven hours by car to reach, like Tajikistan which is a very mountainous area. Regulators need to leverage the identification systems they already have, such as passports, national IDs; post offices can be leveraged to get people on board a digital ID system. On the contrary, we have seen that when regulators limit the points of service (for enrollment) such as only to financial institutions, the digital ID system is very slow to pick up. In brief, use the identification technologies you already have in your country, whether it is paper-based IDs or something similar; secondly, use the physical infrastructure you already have. Make (the enrollment) as broad as possible.

**Question 2: Have there been efforts to ensure providers take the route towards regional or global interoperability of e-KYC?**

A: (Rainer Osanik) To be honest, there is no good solution, and no such regulatory practice yet. Every country is going its own way because they think what they are doing is the correct and right way. The biggest problem is no standardization, so there is no possibility of a solution going cross-border or to be interoperable. The second problem is that the data is so fragmented between states. For example, the KYcer tool can only be used in Estonia if it cannot access databases outside of the country. Technically, the dream is to one day have a global e-KYC standard or an understanding of how it is going to work. But in real life, seeing how slowly things are going, in 20 years, we will still be struggling (to find commonality). There may be bilateral interoperability

that could lead to regional interoperability, but our experience is that it does not look positive at the moment, unfortunately.

#### MODERATOR'S SUMMARY

The moderator thanked Rainer Osanik for bringing home the diversity of experiences and approaches that each individual country has, and some of the challenges that all countries have to face. He noted that the Knowledge Exchange Program is an official platform to share such experiences from which each jurisdiction can draw its own lessons to make headway in their own contexts. The importance of e-KYC and digital ID was also made clear, and they can be seen as critical for addressing financial exclusion risks.

The moderator then encapsulated the key learnings from each of the three presentations:

- > The importance of shifting mindsets and achieving buy-in to embark on, and roll out, a sophisticated, national-level project with regional potential.
- > Why matching organizational capacity with regulatory requirements is essential for engaging with private sector stakeholders.
- > In addition to AML/CFT standards, consumer protection, data privacy and security must be considered for e-KYC and digital ID.

With that, the moderator thanked the presenters for sharing their insights and the participants for their engagement with them. The session was then brought to a close.

THURSDAY, 3 DECEMBER 2020  
DAY 3 - E-KYC AND DIGITAL ID

## WAY FORWARD: KEY POLICIES AND REGULATORY LESSONS, KEY ACTIONS AND SUPPORT

### MODERATOR

**KENNEDY KOMBA**  
DIRECTOR, STRATEGY &  
FINANCIAL INCLUSION POLICY,  
AFI



This was set out as an interactive session for AFI members to seek clarification or deliberate further on two main topics: key policies and regulatory lessons, and key actions for AFI support.

With regard to key policies and regulatory lessons, the following points emerged in the three days of exchanges among participants:

- 1 **Leadership** (governance and monitoring) is critical in digital transformation as evidenced by AFI members leapfrogging onto Open Banking and its peripherals (digital ID and e-KYC) which already have real traction in the markets of member countries.
- 2 **Collaboration and coordination** between the public and private sector as well as cross-agency collaboration are imperative for the development of Open Banking, e-KYC and digital ID because their effective implementation relies on a multidisciplinary perspective. Thus far there have been interlinkages between government agencies, ministries, central banks, and regulatory authorities.
- 3 **A robust legal and regulatory regime** is key for creating and reinforcing certainty in the Open Banking sphere and to encourage adoption of its enabling technologies such as e-KYC and digital IDs.
- 4 **Consumer protection and data privacy protection** rules which stem from legal and regulatory regimes play an integral part in sustaining consumer trust in the integrity and security of Open Banking.
- 5 **Systemic and strategic implementation of Open Banking programs** is important since it offers promising value for the deepening of financial inclusion services.
- 6 **Regulatory and supervisory technology capacity** is critical for the execution of an authority's public policy mandate. More than ever, it is important for regulators and supervisory authorities to acquire and enhance their technical capacity to effectively regulate and supervise the use of these new technologies.
- 7 **The readiness and maturity of the DFS infrastructure** is critical for mitigating and cushioning the impact of national or global emergencies such as the COVID-19 pandemic and promoting key SDGs for financial inclusion.

[Note: There were no questions or comments]

# APPENDIX: AGENDA

Knowledge Exchange Program-2 - Harnessing the potential of Fintech in deepening Financial Inclusion: Practical Regulators Expositions Bank Negara Malaysia (BNM), Bank of Thailand (BOT), Bangko Sentral Ng Pilipinas (BSP) and Comisión Nacional Bancaria y de Valores (CNBV) Mexico. 01-03 December 2020

**TUESDAY, 1 DECEMBER 2020**

## **DAY 1 - OPEN BANKING AND OPEN API**

10:00-10:15	<b>OPENING AND WELCOMING REMARKS</b> <ul style="list-style-type: none"> <li>&gt; Ronadol Numnonda, Deputy Governor, Bank of Thailand</li> <li>&gt; Dr. Alfred Hannig, Executive Director - Alliance for Financial Inclusion (AFI)</li> </ul>
10:15-10:25	<b>AGENDA AND CONTEXT SETTING</b> <p>This session will set the context for the three-day Knowledge Exchange Program by highlighting the objectives and the key thematic areas for discussion. The lead facilitator will also lay out the logical flow of the agenda and expected outcome of the event. This will be followed by a round of introductions from the participating member institutions.</p> <p><b>Moderator:</b> Kennedy Komba, Director, Strategy &amp; Financial Inclusion Policy, AFI</p>
10:25 - 11:00	<b>STATE OF OPEN BANKING AND OPEN API</b> <p>The session will provide an overview of the regulatory landscape and current state of Open Banking and Open API in participating member countries. Member institutions will share their experiences, challenges and opportunities on the topic and linkages to Financial inclusion. The contents of the presentations will be along the following lines:</p> <ul style="list-style-type: none"> <li>&gt; Current state including regulatory approaches to Open Banking and Open API</li> <li>&gt; Key outcomes thus far and implications of Open Banking/Open API on the financial services industry as experienced by the member institutions.</li> <li>&gt; Key opportunities and challenges in Open Banking/Open API from the perspectives of regulation and supervision.</li> <li>&gt; Gaps and areas for improvement</li> </ul> <p><b>Presenters:</b></p> <ul style="list-style-type: none"> <li>&gt; Thammarak Moenjak, Bank of Thailand</li> <li>&gt; Melchor Plabasan, Bangko Sentral Ng Pilipinas</li> <li>&gt; Mary Pily Loo, Comisión Nacional Bancaria y de Valores (CNBV) México</li> </ul> <p><b>Moderator:</b> Jaheed Parvez, Technical Specialist, PPRI, AFI</p>
11:00 - 11:15	Q&A, Open Discussion
11:15 - 11:30	Coffee Break
11:30 - 12:00	<b>OPEN BANKING AND OPEN API - OVERCOMING THE IMPLEMENTATION CHALLENGES</b> <p>The session will provide better understanding of the trends and innovations in Open Banking &amp; Open API and will assess implications of various regulatory approaches. The session will also present various potential open banking enabled products that are useful for financial inclusion. The key discussion points will include:</p> <ul style="list-style-type: none"> <li>&gt; Trends in Open Banking and Open API</li> <li>&gt; Key factors affecting interagency collaboration for Open Banking and Open API</li> <li>&gt; Consumer protection, Privacy and Security considerations for Open Banking and Open API</li> <li>&gt; Open Banking and API Implementation challenges</li> <li>&gt; Trends and innovations in cross-border payments</li> <li>&gt; Opportunities for cross-sectoral and cross-border collaboration/cooperation among the authorities to minimize risks associated with Open Banking and Open API</li> <li>&gt; Opportunities for leveraging RegTech and SupTech solutions</li> <li>&gt; Implications for Open Banking regulatory framework</li> <li>&gt; Potential opportunities and Innovations under the COVID-19 recovery phase and its linkages to financial inclusion</li> </ul> <p><b>Presenters:</b></p> <ul style="list-style-type: none"> <li>&gt; Rachita Syal, Bank of England</li> <li>&gt; Irina Mnogohitnei, Bank of England</li> </ul> <p><b>Moderator:</b> &gt; Robin Newnham, Head, Policy Analysis, AFI</p>
12:00 - 12:15	Q&A, Open Discussion and Closing

WEDNESDAY, 2 DECEMBER 2020

## DAY 2 - OPEN BANKING AND OPEN API - *Continued*

10:00 - 10:40	<p><b>OPEN BANKING AND OPEN API - REGULATORY APPROACHES</b></p> <p>The session will provide an overview of different models as implemented in developed countries. In addition, the speaker(s) in this session will dive deep into discussions around opportunities, challenges, framework and regulations for innovation. The key topics of the discussions will include:</p> <ul style="list-style-type: none"> <li>&gt; Diverse regulatory approaches to Open Banking and Open API</li> <li>&gt; Standardization of API</li> <li>&gt; Roles of banks, third parties and regulatory authorities</li> <li>&gt; Consumer protection, privacy and security considerations for Open Banking and Open API</li> <li>&gt; Key stakeholders and interagency collaboration</li> </ul> <p><b>Presenter:</b></p> <ul style="list-style-type: none"> <li>&gt; Dr. Dirk Haubrich, Head of Conduct, Payments and Consumers - European Banking Authority</li> </ul> <p><b>Moderator:</b></p> <ul style="list-style-type: none"> <li>&gt; Jaheed Parvez, Technical Specialist, PPRI, AFI</li> </ul>
10:40 - 11:00	Q&A and open discussion
11:00 - 11:45	<p><b>THE ROLE OF DFS IN ADDRESSING THE IMPACT OF COVID-19</b></p> <p>The discussions will focus on the ways which DFS promotes financial inclusion in general and more particularly how it can be leveraged to mitigate the challenges presented by the pandemic including various policy measures that financial regulators have put in place. The considerations for Inclusive Green Finance (IGF) and Gender Inclusive Finance (GIF) for Covid-19 recovery face will also be discussed in this session.</p> <p><b>Presenters:</b></p> <ul style="list-style-type: none"> <li>&gt; Melchor Plabasan, Bangko Sentral Ng Pilipinas</li> <li>&gt; Ali Ghiyazuddin Mohammad, Senior Policy Manager, AFI</li> <li>&gt; Bank Negara Malaysia (TBC)</li> <li>&gt; Helen Walbey, Alliance for Financial Inclusion</li> <li>&gt; Johanna Nyman, Alliance for Financial Inclusion</li> </ul> <p><b>Moderator:</b></p> <ul style="list-style-type: none"> <li>&gt; Aban Haq, Project lead Digital Financial Champions, AFI</li> </ul>
11:45 - 12:00	Q&A and open discussion
12:00 - 12:20	Coffee Break
12:20 - 12:50	<p><b>IMPACT OF COVID-19 ON SDGS AND KEY RISKS IN COVID-19 DIGITAL FINANCIAL TRANSFER PROGRAMS</b></p> <p>The session will look into the role of digital Financial Services in achieving SDGs and the impact of Covid-19 on SDGs. The session will present the key risk areas in Covid-19 Digital Financial Services programs.</p> <p><b>Presenters:</b></p> <ul style="list-style-type: none"> <li>&gt; Rafe Mazer, Innovations for Poverty Action (IPA)</li> <li>&gt; David Symington, UN Secretary General's Special Advocate for Inclusive Finance for Development (UNSGSA)</li> </ul> <p><b>Moderator:</b></p> <ul style="list-style-type: none"> <li>&gt; Aban Haq, Project Lead, Digital Financial Champions, AFI</li> </ul>
12:50 - 13:00	Q&A and open discussion, evaluation and closing



**THURSDAY, 3 DECEMBER 2020**

**DAY 3 - e-KYC AND DIGITAL ID**

10:00 - 10:50	<p><b>STATE OF E-KYC AND DIGITAL ID</b></p> <p>The session will provide the current state of e-KYC and Digital ID policy implementation and challenges facing the member countries - What has worked and what has not worked. Member institutions will share their experiences, challenges and opportunities on the topic and linkages to Financial inclusion. The contents of the presentations can be along the following lines:</p> <ul style="list-style-type: none"> <li>&gt; Current status of e-KYC and Digital ID regulations</li> <li>&gt; Key outcomes of e-KYC and Digital ID regulations in expanding Financial Inclusion as experienced by the member institutions</li> <li>&gt; Stakeholder collaboration and coordination mechanism</li> <li>&gt; Key opportunities and challenges in e-KYC and Digital ID from the perspectives of regulation and supervision - as facing the member institutions.</li> <li>&gt; Impact on both domestic and international remittances</li> </ul> <p><b>Presenter:</b></p> <ul style="list-style-type: none"> <li>&gt; Wijitleka Marome, Bank of Thailand</li> <li>&gt; Ruel Bumatay, Bangko Sentral Ng Pilipinas</li> <li>&gt; Ian Lee, Bank Negara Malaysia</li> <li>&gt; Gilberto Pérez, Comisión Nacional Bancaria y de Valores (CNBV) México</li> </ul> <p><b>Moderator:</b></p> <ul style="list-style-type: none"> <li>&gt; Ritesh Thakkar, Senior Regional Manager, EECA &amp; Asia, AFI</li> </ul>
10:50 - 11:05	Q&A and open discussion
11:05 - 11:15	Coffee Break
11:15 - 12:15	<p><b>E-KYC AND DIGITAL ID - REGULATORY APPROACHES &amp; INNOVATION</b></p> <p>The overall objective of this session is to deep-dive into effective regulatory frameworks for E-KYC and Digital-ID with a developed country perspective on how financial regulators should balance between financial integrity and financial innovation. The session will also discuss some of the prominent innovations in the private sector and cross-cutting considerations such as youth, gender, and other disadvantaged groups, in a bid to further draw value from e-KYC/e-ID innovations as an enabler for financial inclusion. The session will touch upon the following topics:</p> <ul style="list-style-type: none"> <li>&gt; Infrastructure and Framework for e-KYC and Digital ID - A developed country perspective</li> <li>&gt; Emerging role of Digital ID verification in KYC, AML &amp; onboarding</li> <li>&gt; Implications of KYC Standardization</li> <li>&gt; Interagency collaboration</li> <li>&gt; e-KYC for remittance</li> <li>&gt; e-KYC regulation for FinTech firms</li> <li>&gt; Consumer protection, Data Privacy and Security considerations for e-KYC and Digital ID</li> <li>&gt; Private sector Innovation</li> <li>&gt; Potential role of e-KYC and Digital ID in promoting financial inclusion of refugee and Forcibly Displaced Populations (FDPs)</li> <li>&gt; Potential opportunities and Innovations under the COVID-19 recovery phase</li> </ul> <p><b>e-KYC and Digital ID - Regulatory Approaches &amp; Innovation Presenters:</b></p> <ul style="list-style-type: none"> <li>&gt; Rainer Osanik, Accelerate Estonia</li> <li>&gt; Pavel Shoust, Russian Electronic Money and Remittance Association</li> <li>&gt; Cécile Gellenoncourt, The Commission de Surveillance du Secteur Financier (CSSF), Luxembourg</li> </ul> <p><b>Moderator:</b></p> <ul style="list-style-type: none"> <li>&gt; Eliko Boletawa, Head PPRI, AFI</li> </ul>
12:15 - 12:45	Q&A, Open Discussion
12:45 - 12:50	Coffee Break
12:50 - 13:20	<p><b>WAY FORWARD</b></p> <ul style="list-style-type: none"> <li>&gt; Key Policy and Regulatory Lessons</li> <li>&gt; Key Actions for Support</li> </ul> <p><b>Moderator:</b></p> <ul style="list-style-type: none"> <li>&gt; Kennedy Komba, Director, Strategy &amp; Financial Inclusion Policy, AFI</li> </ul>
13:20 - 13:30	Evaluation and Closing

**Alliance for Financial Inclusion**

AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia

t +60 3 2776 9000 e [info@afi-global.org](mailto:info@afi-global.org) [www.afi-global.org](http://www.afi-global.org)

 Alliance for Financial Inclusion  AFI.History  @NewsAFI  @afinetwork