Policy Recommendations for the 40th COMCEC Session on "Digital Transformation of Payment Systems in OIC Member Countries"

The 39th COMCEC Session agreed on "Digital Transformation of Payment Systems in OIC Member Countries" as the theme for the Exchange of Views Session of the 40th Session of the COMCEC and requested COMCEC Financial Cooperation Working Group to come up with concrete policy recommendations on this topic and report them to the 40th COMCEC Ministerial Session. In line with this request, the 22nd Meeting of the Financial Cooperation Working Group has come up with the following challenges and policy recommendations on digital transformation of payment systems in the OIC Member Countries:

CHALLENGES

1. Challenges Faced by Countries with Matured and Advanced Development Levels of Payment Systems

1. *Cybersecurity threats remain a key challenge for advanced level of development of payment systems.*
2. *Though the digital payment system is ubiquitous and transcends the national borders of a country, there is low cross-border collaboration among regulators and supervisory authorities.*
3. *Sharī'ah compliance with all aspects of the digital payment ecosystem for institutions offering Islamic financial services requires further consideration through the application of the Sharī'ah governance framework.*
4. *Cost of maintaining digital payment infrastructure may be high.*
5. *Protecting consumer privacy in digital payment systems in some mature and advanced jurisdictions remains a challenge.*

2. Challenges Faced by Countries with Intermediate and Low Development Levels of Payment Systems

1. *The limited internet penetration and mobile network infrastructure in some developing countries, particularly in rural areas, restricts the expansion and adoption of digital payment systems.*
2. *Low level of digital literacy hinders projected results in digital payment system utilization.*
3. *In some OIC Member Countries, the legal and regulatory framework is still evolving and does not yet fully address the growing digital financial services sector, including fintech innovations.*
4. *Cybersecurity risks remain heightened due to the level of development of digital financial services, which has led to identity and data theft or loss.*
5. *Adoption, operation, and maintenance of digital payment infrastructure pose high costs, especially for small businesses.*
6. *Lack of trust among many users, and this has led to the unacceptability of digital payment systems.*
7. *Digital inequality has led to situations where the elderly or uneducated population groups struggle to make payments that can be made only through digital platforms.*
8. *Although the informal economic sector, which is prevalent in rural areas, is one of the main targets of digital payment systems to promote financial inclusion, there is still a low level of acceptability in many jurisdictions.*
9. *Tax regulations related to digital payments have complicated businesses' use of these systems in some developing countries.*
10. *The lack of clarity and transparency and constant changes in legal and tax regulations related to digital payment systems can be confusing for investors and users.*
11. *Data privacy concerns still exist, and many users do not feel safe using digital payments.*
12. *Collaboration between public and private sector entities is limited, which hinders the development and expansion of digital payment systems and infrastructure.*
13. *Some countries still have a strong cash culture. Shifting this cultural preference from cash to digital payments requires sustained efforts in education and incentives, such as discounts for digital payments or awareness campaigns highlighting the benefits of digital payments.*

POLICY RECOMMENDATIONS

a. General Recommendations

1. *Developing an Interoperability framework for digital payment systems among the OIC Member Countries to clear and settle financial transactions and payments in real-time to help foster economic cooperation, facilitate smoother cross-border transactions and promote international trade.*

2. *Developing legal framework at the OIC level to oversee the implementation of regional multilateral cooperations on payment systems.*

3. *Setting-up dedicated task forces including digital payment experts to continue to harness the latest technology in payment systems.*

4. *Developing standards and protocols for joining Digital Payment System Platforms to facilitate international transactions.*

5. *Scaling up collaborative efforts towards strengthening cybersecurity among central banks of member countries.*

6. *Collectively investing in digital literacy and technical skills development to build a sustainable future workforce.*

7. *Promoting financial inclusion through expansion of digital payment platforms with simplified technology for unbanked and underbanked.*

8. *Enhancing consumer financial literacy and protection in the risks associated with the use of digital payments.*

9. *Fostering sustained innovation in the fintech sector and providing regulatory support to start-ups in the digital payment space to encourage healthy competition.*

b. Recommendations for Countries with Low Development Level of Payment Systems

1. *Developing public-private partnerships to expand internet infrastructure, particularly in underserved rural areas and providing subsidies and incentives for the private sector.*

2. *Launching nationwide digital literacy campaigns focusing on rural areas with more prevalent financial illiteracy.*

3. *Regularly updating and harmonizing legal and regulatory frameworks to reflect advancements in digital financial services.*

4. *Introducing/establishing the regulatory sandbox to include a broader range of fin-tech innovations and streamlining the licensing process to facilitate faster adoption of new technologies.*
5. *Implementing robust cybersecurity protocols, including establishing a national cybersecurity agency dedicated to monitoring and responding to digital threats.*
6. *Strengthening financial institutions' capabilities to monitor and report suspicious activities related to money laundering and terrorism financing.*
7. *Incentivizing public-private partnerships through subsidies, for developing shared infrastructure projects to promote and expand digital financial services.*
8. *Promoting digital inclusion through increasing broadband access and building the necessary digital infrastructure for nationwide transformation.*
9. *Implementing policies that promote a shift in consumer behaviour, such as offering incentives for digital transactions.*
10. *Mobilizing resources through collaboration and cooperation with development banks and other international institutions for research and innovation on digital payments.*
11. *Conducting scheduled risk assessments and documenting all findings for digital payments services and solutions to ensure risk management plans are up-to-date and reviewed in line with findings derived from regular risk assessments.*

c. Recommendations for countries with intermediate level of development of payment systems

1. *Running campaigns on digital literacy through social media, informative emails and text messages, bank apps, radio and television to reach a wider audience.*
2. *Utilizing corporate social responsibility (CSR) and providing incentives to businesses and users for participation in digital literacy programs with a view to promoting digital literacy.*
3. *Establishing smart partnerships with relevant stakeholders to focus on how to utilize digital payment solutions to enhance financial inclusion.*
4. *Investing in increasing the coverage of high-speed internet access, particularly fifth-generation cellular technology (5G), to support the expansion of mobile payments.*
5. *Upgrading data centres to support the increase in digital payments.*
6. *Encouraging training activities towards professionals to enhance their skills in the digital payment systems.*
7. *Exploring technical assistance from developed jurisdictions in conducting the exchange of expert programs for technical skills transfer.*
8. *Encouraging financial institutions and payment systems companies to invest in cost and energy-efficient technologies.*

9. *Enhancing interoperability between different digital platforms for a seamless consumer experience.*
10. *Ensuring the regulatory framework is adaptable to emerging technologies including future market developments, empowering cybersecurity measures and consumer protection.*
11. *Implementing an industry-wide framework to enhance regulatory policies so that continuous monitoring and evaluation of digital payment systems is ensured*
12. *Conducting scheduled risk assessments and documenting all findings for digital payments services and solutions to ensure risk management plans are up-to-date and reviewed in line with findings derived from regular risk assessments.*

d. Recommendations for Countries with Matured and Advanced Development Levels of Payment Systems

1. *Facilitating training programs for technical and regulatory teams in regulatory, supervisory and policy-maker authorities including central banks of other member countries*
2. *Organizing other capacity-building events such as workshops and seminars to share best practices with other member countries.*
3. *Introducing exchange programs for technical staff from central banks and other regulatory and policy-maker authorities of member countries with a view to raising awareness about the latest advances in Regulation Technology, cybersecurity measures, and other relevant aspects of the regulation of digital payment systems.*
4. *Assisting less developed OIC Member Countries in developing regulatory policies for digital payment systems and setting of digital payment infrastructure.*
5. *Conducting scheduled risk assessments and documenting all findings for digital payments services and solutions to ensure risk management plans are up-to-date and reviewed in line with findings derived from regular risk assessments.*
6. *Encouraging regulated entities to implement and regularly update cybersecurity standards such as ISO//IEC 27001.*
7. *Enabling regulated entities to stay ahead of security threats through regular investments in the latest cybersecurity solutions.*
8. *Ensuring all regulated entities to implement multifactor authentication and prioritizing full encryption of data in all digital payments to combat breaches associated with digital payment systems.*
9. *Extending Sharī'ah governance to digital payment systems for Islamic financial institutions.*
10. *Ensuring the Sharī'ah compliance of payment systems such as e-wallet and its parameters utilized by Islamic financial institutions.*
11. *Conducting annual trainings and capacity-building activities on Sharī'ah governance and issues in digital payment systems.*