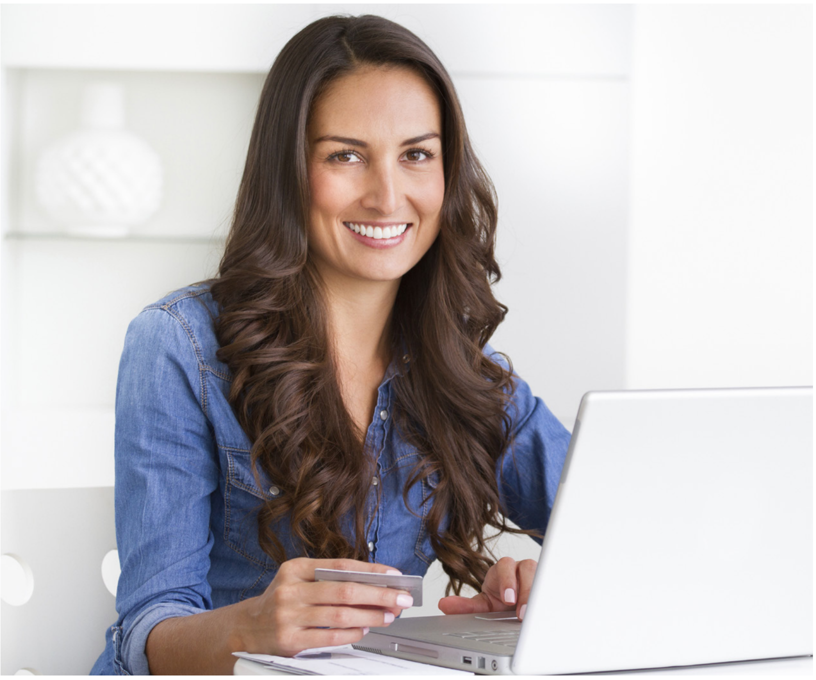
U.S. CHAMBER OF COMMERCE

USINDIA BusinessCouncil

Contents

Recommendations for policy interventions

Accelerating digital payments and deepening financial inclusion



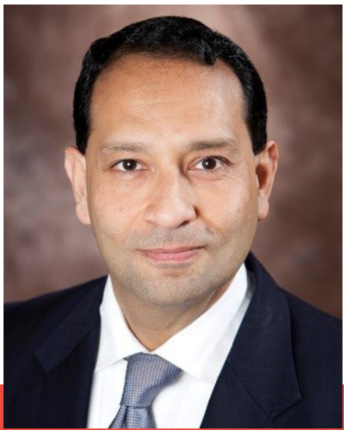
The Ministry of Finance, Government of India, and the U.S.-India Business Council conclave held on March 29, 2017

September 2017

pwc

www.pwc.in

Message from the U.S.-India Business Council



Khush Choksy

Acting President, USIBC, and Senior Vice President,
US Chamber of Commerce

The U.S.-India Business Council (USIBC), in partnership with the Ministry of Finance, Government of India, hosted its first symposium on 'Accelerating Digital Payments and Deepening Financial Inclusion' on March 29, 2017 in New Delhi. The symposium brought together a large number of stakeholders, including senior government officials, industry leaders and financial experts, to discuss challenges that exist in accelerating digital payments and advancing financial inclusion. The symposium included discussions on developing a vibrant digital payments ecosystem; enabling a robust and secure digital payments framework; ensuring last mile connectivity to maximize consumer access; and charting an innovative path for financial inclusion and the financial health of Indian consumers.

The United States has been a leader in digital payments, with a number of American companies at the forefront of innovation. Companies such as PayPal, Mastercard and American Express have disrupted markets globally and can add tremendous value to India with their rich experience. Further, American companies in India have been contributing to India's digital economy. India and the U.S. have increased their bilateral engagements on the sharing of technology, digital transformation and financial inclusion to support "Digital India".

Further, there are opportunities for increased collaboration and policy intervention to create a more conducive environment for innovation, digitization and financial inclusion. The 'catalyst' initiative between the Government of India and the United States Agency for International Development (USAID) aims to expand digital payments and financial inclusion in India, especially for small merchants and low-income consumers. Every economy is built on trust, and a digital economy more so. The security of digital financial transactions against fraud, data theft, phishing and cyberattacks remains a key concern.

This USIBC-PwC report focuses on the challenges in the digital payments ecosystem and outlines a few areas for policy intervention that are necessary to ensure that all Indian citizens participate in the digital drive.

We hope you find the report insightful.

Foreword

Jamuna Rao Verghese

Senior Advisor, Financial Services,
PwC India

PwC India was the knowledge partner for the symposium on 'accelerating digital payments and deepening financial inclusion', which was jointly hosted by the USIBC and Ministry of Finance on 29 March 2017.

Financial inclusion is essential for human development. India is deeply committed to financial inclusion, which is evident from the single-point focus of the present government. The unprecedented 1.13 billion bank accounts opened through PMJDY and the introduction of new kinds of banks, i.e. payments banks and small finance banks, are global firsts. One of the basic building blocks for financial services is payments, with digital payments serving as the catalyst for financial inclusion. Towards the digitisation of cash and payments, an ambitious demonetisation effort was conducted in India in November 2016. Additionally, UPI, BHIM, Aadhaar Pay and BharatQR are innovative initiatives undertaken by the government to promote a 'less-cash' India. Further, the Indian Budget 2017 introduced a number of measures to accelerate digital payments, such as mandating non-cash payments beyond a certain threshold and providing incentives for merchants to use BHIM and Aadhaar Pay.

While the policy for digital payments in India has been forward-looking, there is still a long way to go. At the USIBC and the Ministry of Finance symposium, which was attended by various stakeholders from the government and private sector, some digital payments recommendations were debated. We have attempted to distil some of these recommendations and have outlined some areas for policy interventions.

We hope you find this USIBC-PwC report useful and relevant. We welcome your thoughts and views.

Summary of key recommendations

1. Regulatory dialogue to be consultative and not reactive

While there have been stakeholder consultations, we recommend that this process be proactive rather than reactive and that it involve a larger number of industry players instead of a few representatives. An official forum, comprising a number of industry players and policymakers, will foster continuous dialogue and achieve the objectives of transparency and buy-in from the stakeholders for policy changes.

2. Regulations not to be ownership-driven and to provide currency for all instruments

The ownership of a wallet instrument need not be a limiting factor for operational flexibility. Presently, banks have greater manoeuvrability with their wallets compared to non-banks on aspects of cash-outs and interoperability. Allowing the ubiquitous usage of wallets through interoperability and allowing cash-outs for semi-closed wallets (currency) will help boost the industry.

3. Regulations to be activity-dependent and not value-dependent

To ensure high frequency of digital payments, small-value digital payments must have negligible charges. The present and proposed regulations put MDR charges as a percentage of the value of transactions. This does not provide adequate motivation for small-value transactions to migrate to digital. Charges need to be negligible for low-value payments to increase the volumes of digital payments. The proposed regulations on separate logins for online retail and PPIs will increase friction and impede the adoption of digital payments for large customer segments.

4. Regulations to be based on CBA

For digital wallets to be successful, it is essential for the current business model, which is presently being challenged, to be robust. The revenue opportunity for wallets is impaired due to low interest paid by banks on escrow accounts and costs related to KYC. With the proposed new PPI guidelines, the operational costs and challenges of converting from minimum KYC to full KYC are tremendous. Additionally, two-factor authentication will add to the inconvenience faced by customers. Allowing a substantial amount of core portion[1] to be invested in government securities and easing KYC requirements will improve the viability of digital wallets.

5. Regulator and industry to collaborate on skill development in cyber security

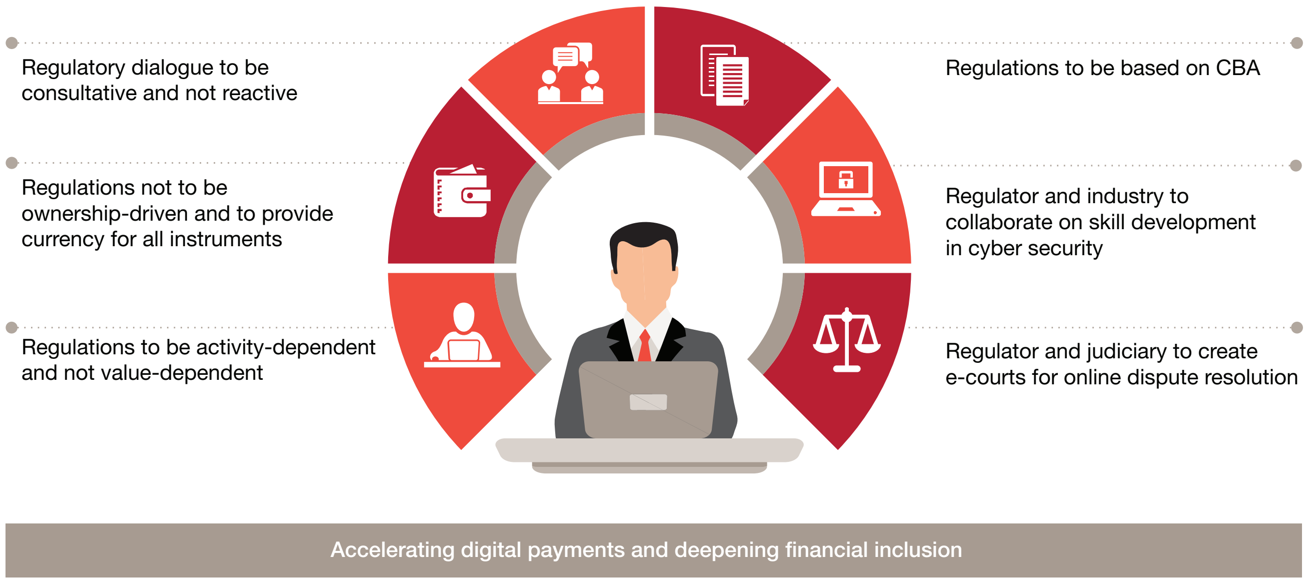
Training 500,000 to 1 million personnel on enforceable cyber security practices is essential for India to tackle the risks of cyber security and compliance. In this regard, the government and the industry can come together through PPPs to create IT standards, policies, security frameworks, training and certifications.

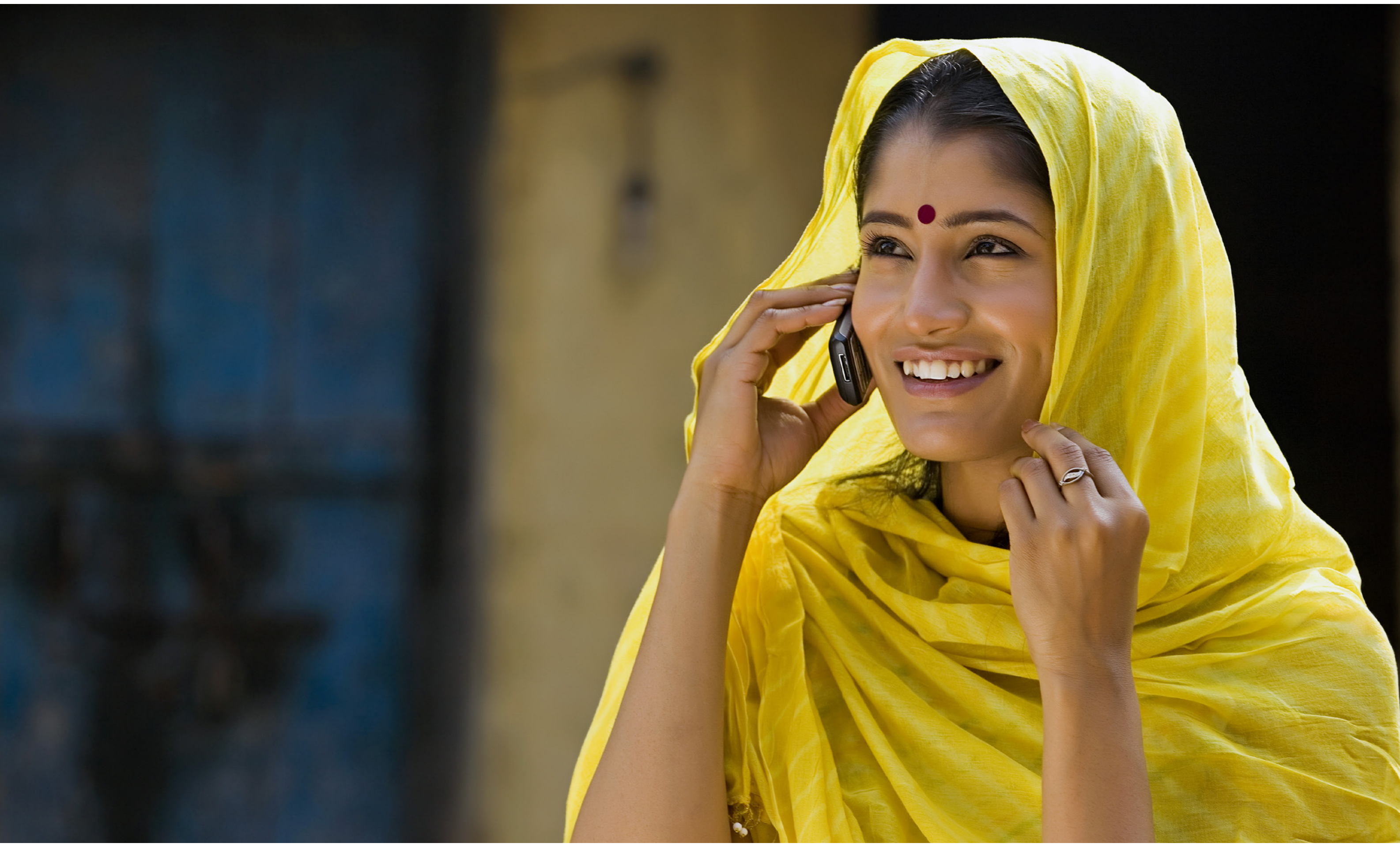
6. Regulator and judiciary to create e-courts for online dispute resolution

Financial cybercrimes need to be resolved in a timely manner to prevent them from recurring. Creating a special cyber security court with judges who are well trained in the aspects of cybercrime will be effective in addressing financial cyber complaints and investigations. These courts will work closely with the Cyber Security Cell of the Government of India and private players.

1 *Core portion is computed by finding the lowest daily outstanding balance on a fortnightly basis for one year (26 fortnights) from the preceding month and averaging these lowest fortnightly outstanding balances.*

Policy recommendations to drive digital payments





1. Regulatory dialogue to be consultative and not reactive

Challenge

Industry participation in formal regulatory dialogue in India has historically been reactive rather than consultative. However, in recent years, regulators and policymakers in India, such as the Committee on Digital Payments (headed by Ratan Watal) and the Chief Minister's Committee on Digital payments have been soliciting feedback. Additionally, many more industry participants would like to play consultative roles in the formation of regulations on digital payments.

Recommendation

Create an official forum with a larger number of industry players and policymakers to promote continuous dialogue. This will be more effective than one-off feedback and will help in introducing new measures quickly and in real time. It will also achieve the objectives of fostering transparency and ensuring stakeholder buy-in for policy changes. A consultative policymaking process is essential to minimise unintended impact on the digital payments ecosystem.

Example

The Payments Strategy Forum in the UK leads a process to identify, prioritise and help deliver initiatives. The forum has helped different stakeholders hold productive, open-minded discussions for the UK's 75-trillion GBP payments industry. This has been done through fair representation of diverse stakeholders in the forum. The forum consists of a chair who is independent of the industry and its membership includes service-user representatives and payment service providers. The BoE, PRA, FCA and PSR are all observers on the forum.

Action point

Create a body like the Digital Payments Forum for continuous dialogue and participation on payments policies. The body must consist of government representation from bodies such as NITI Aayog, Ministry of Finance, Ministry of Electronics and Information Technology, RBI, NPCI and a larger group of payments system providers.

Policy recommendations to drive digital payments

2. Regulations not to be ownership-driven and to provide currency for all instruments

Challenge

Mobile wallet companies are important and active contributors to the payments ecosystem in India. However, there are disparities in the regulations on PPIs/wallets for banks and non-banks. Banks can operate open wallets that allow cash-out facilities for customers to use interoperable payments systems. Non-banks, on the other hand, can operate only a semi-closed wallet which does not allow cash-outs. Presently, non-banks cannot access the interoperable payments network, which limits P2P and P2M operations and business. PPI/wallet regulations have impacted the ability of mobile wallet companies to harness their full potential and contribute towards mass financial inclusion through the use of digital platforms.

Recommendation

The owner of a wallet instrument need not determine its operational flexibility. Allowing ubiquitous usage of all payment instruments through interoperability will create multiple avenues for new and conventional players to disrupt the market and ensure interaction between different instruments and services, creating multiple use cases. Specifically, allowing cash-outs for semi-closed PPIs will enable PPI companies to make payment services accessible to their large customer base. Equitable treatment of banks and non-banks in payments will lead to exponential growth and expansion of the digital payments infrastructure and its usage.

Example

The Government of Colombia introduced a conditional cash transfer programme to move cash disbursements from bank branches to prepaid cards, allowing 4,50,000 beneficiaries across seven cities to withdraw their payments at the ATM network of a private bank. This reduced the inconvenience of visiting distant bank branches for cash. The initiative was possible because prepaid cards were allowed cash-outs, which also enabled the government to piggyback on the infrastructure created by non-banking entities.

Action point

The RBI and the government will review the present and proposed guidelines for PPIs to ensure that banks and non-banks get the same treatment. Specifically, implementing interoperability for PPI players at the earliest and allowing cash-outs will ensure parity.

3. Regulations to be activity-dependent and not value-dependent

Challenge

Low-value retail payments are largely driven by small merchants who serve the less affluent. These payments are driven by volume and ease of use. Since there is no explicit cost associated with the use of cash for low-value transactions and cash is 'convenient', it remains the dominant method of payment for such transactions. One of the key reasons hindering the growth of digital payments for low-value transactions is the explicit cost component, i.e. MDR, which trims merchant margins and disincentivises the uptake of digital payments. In the proposed draft guidelines on rationalisation of MDR for debit cards, a flat fee has been proposed to be levied on smaller value government transactions which need to be extended to all small-value transactions. However, similar regulations have not been prescribed for non-government transactions.

PPIs provide a low-friction payment experience which incentivises customers to adopt digital payments. The proposed PPI regulations require customers to go through additional factors of authentication. The regulations have also proposed that for online retail, PPIs have separate logins for the main PPI app through additional authentication steps. This will create friction in the payments experience and prevent customers from using digital means for making small-value payments.

Recommendation

To drive digital payments, the government has to bring low-value high-volume transactions into the ambit of 'digital'. The need of the hour is to drive payments based on activity. As retail payments comprise the largest chunk of payments, they have a higher chance of getting digitised if the explicit cost associated with small-value payments is removed or reduced. Friction for online retail transactions through PPIs can be reduced if the new regulations do not prescribe separate logins for the PPIs. Issuers can develop a mechanism that prompts login before the use of funds from the wallet. Minimal MDR for small-value digital transactions and convenience of PPI transactions can bring low-value high-volume transactions under the umbrella of digitisation.

Example

Measures supporting reduced cost to access digital services have borne fruit in India. In 2002, the TRAI abolished extra charges borne by customers when connecting calls across different mobile network operators, after which the Indian telecommunications industry began to experience tremendous growth. The more recent stand of the TRAI, which allows customers to be charged for mobile data only, has led to reduced costs for customers. It has increased the number of online users in India and has also spurred consolidation in the telecommunications space.

Action point

The government and RBI will review MDR charges on debit cards, especially for small-value transactions. Additionally, the RBI will review the proposed PPI guidelines regarding separate login requirements for online retailers.

Policy recommendations to drive digital payments

4. Regulations to be based on CBA

Challenge

For wallets to be successful in driving digital payments and financial inclusion, it is imperative that they are commercially viable. Presently, wallets do not earn equitable revenue from the money kept in escrow accounts of banks. Additionally, the proposed new PPI guidelines prescribe a number of operational processes which will stifle the functionality of wallets and add to their operational costs. For example, the new draft guidelines require minimum KYC accounts to be converted to full KYC accounts within 60 days of opening of the PPI account. Aadhaar-based full KYC will be a challenge given that a large number of Aadhaar accounts are not linked to a mobile number or are linked to an incorrect mobile number (some estimates suggest this to be 40%). PPI players will have to incur prohibitive costs to complete full KYC through other means, thus destabilising their business models. The proposed PPI guidelines of two-factor authentication will further add to the inconvenience faced by customers.

Recommendation

The introduction of present and new regulations needs CBA. Mandating parking of wallet funds in escrow accounts serves the purpose of protecting customer money. However, as wallet players do not get adequately compensated, regulators need to evaluate if there are any other options for providing a boost to wallet providers as well as protecting customers' money. One option is allowing a substantial amount of wallet core funds to be invested in government securities. This will provide a business impetus to wallet providers and also improve digital payments in the country. Review of two-factor authentication for small-value transactions through wallets is recommended as it will add to the friction without providing any benefits.

Example

The Australian government uses CBA for regulatory impact analysis. It encourages decision makers to take account of all the positive and negative effects of proposed regulations, and helps identify cost-effective solutions to problems by identifying and measuring all costs.

Action point

The government and RBI will review the present and proposed guidelines for PPIs with respect to the number of requirements which add to the cost and the effectiveness of PPIs, making the business unviable and the adoption of digital payments difficult. In particular, there is a need to review the requirement to retain minimum KYC, two-factor authentication and usage of funds to allow investment in government securities.

5. Regulator and industry to collaborate on skill development in cyber security

Challenge

Established security protocols, policies and certificates play a major role in setting cyber security standards. However, in the current IT ecosystem, essential standards and benchmarks are either unavailable or are not implementable to test the systems because they have not been standardised. IT policies are dependent on the proactivity of the player rather than on established standards in the industry. These infrastructure and process gaps are exacerbated by the dearth of professionals trained in skills of IT security and risk mitigation.

Recommendation

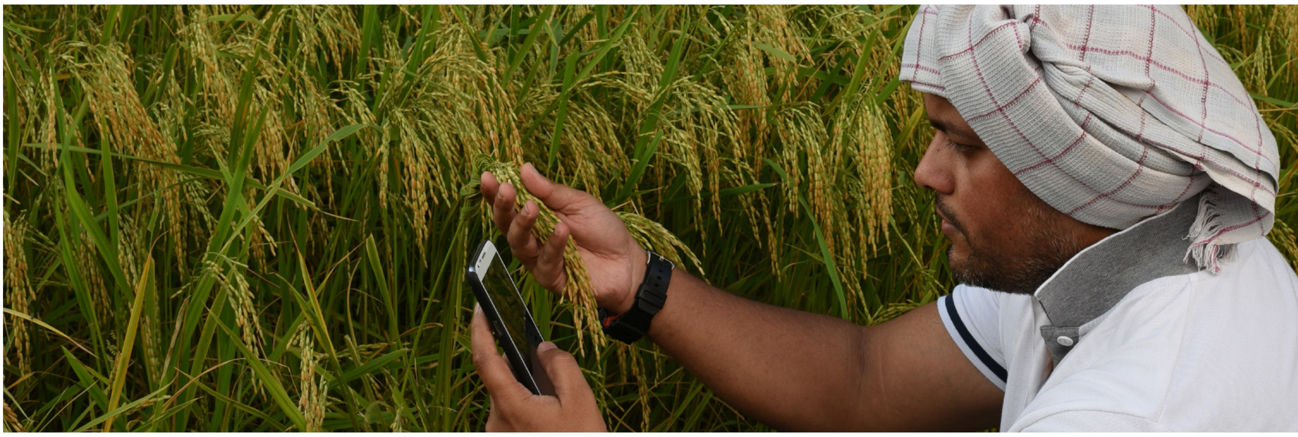
Standardisation of skills and certifications for 'man behind the machine' is critical for IT security and risk mitigation. PPPs will be of immense value in this area to provide curriculum and certifications for new-age, technology-led payments players. They should incorporate global best practices as well as global standards. This initiative will help the industry create safeguards and foster trust.

Example

The Government of the UK worked with leading industry partners to develop e-learning courses to understand online threats and how to protect business data, money and reputation. A course was developed with the Law Society and the ICAEW to increase the knowledge base of cyber security for legal and accountancy professionals.

Action point

Create a body to set standards, provide certification and create e-learning courses on IT security and risk mitigation. This body can comprise government and payment providers such as NITI Aayog, the Ministry of Finance, Ministry of Electronics and Information Technology, RBI, NPCI and other payment networks, payment gateways and payment technology players.



Policy recommendations to drive digital payments

6. Regulator and judiciary to create e-courts for online dispute resolution

Challenge

Innovation in technology is the key driver and disrupter for digital payments. The world of online transactions and virtual interfaces works at an astonishing pace and is complicated. Likewise, frauds and security breaches are perpetrated at a fast pace. The conventional judiciary systems are not adept at resolving such issues. A slow judiciary and law enforcement process implies a higher cost and increased time for investigation and dispute resolution. Swift adjudication is critical to maintain customer trust in digital payments and also reduce potential financial loss that can be incurred due to delays in processes. Real-time risk monitoring can help the judiciary and law enforcement institutions to work in the present rather than in retrospect.

Recommendation

Proactivity of the judiciary system is the most effective way to ward off the perpetrators of cybercrimes. One way is to set up specialised e-courts with judges who are well trained in the aspects of cybercrime. This court could work closely with the Cyber Security Cell of the Government of India. Private players can also collaborate to educate a new breed of judiciary for resolution of tech crimes. This way, the government, judiciary and private players can play an important role in addressing cyber security problems in India.

Example

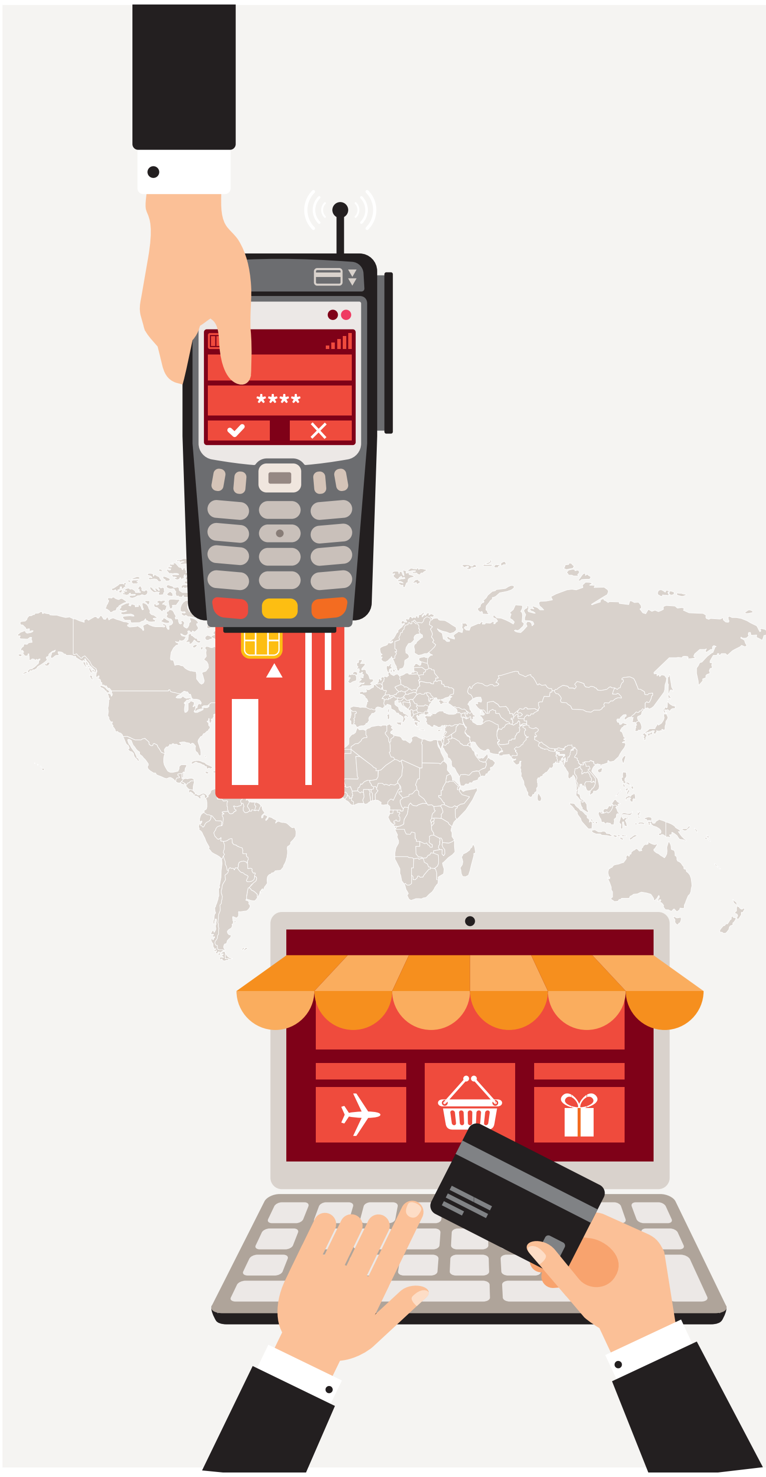
Malaysia has set up the first special court for cases involving cybercrimes to fast-track the prosecution of offenders. The court is dedicated to handling offences such as financial fraud, online gambling, spying, defamation, document falsification and pornography. This cyber court is equipped with facilities to function as an e-court and has technology-savvy judges and prosecutors. Twenty-seven judges have undergone a training programme to enhance their knowledge of cybercrimes.
This training was conducted by local and foreign experts at the Judicial and Legal Training Institute, in collaboration with the Communication and Multimedia Ministry (Malaysia).

Action point

Form a working group to evaluate the creation of specialised e-courts in India. This group should comprise representatives from the Ministry of Electronics and Information Technology, Ministry of Law, Ministry of Finance, NITI Aayog, RBI and other payment players.

Abbreviations

ATM	Automated teller machines
BHIM	Bharat Interface for Money
BoE	Bank of England
CBA	Cost-benefit analysis
FCA	Financial Conduct Authority
ICAEW	Institute for Chartered Accountants in England and Wales
IT	Information technology
KYC	Know your customer
MDR	Merchant discount rate
NITI	National Institution for Transforming India
NPCI	National Payments Council of India
P2M	Peer-to-merchant
P2P	Peer-to-peer
PMJDY	Pradhan Mantri Jan Dhan Yojana
PPIs	Prepaid payments instruments
PPPs	Public private partnerships
PRA	Prudential Regulatory Authority
PSR	Payment Systems Regulator
RBI	Reserve Bank of India
TRAI	Telecom Regulatory Authority of India
UK	United Kingdom
USA	United States of America
UPI	Unified Payments Interface
USAID	United States Agency for International Development
USIBC	U.S.-India Business Council



About the USIBC

Formed in 1975 at the request of the US and Indian governments, the US Chamber of Commerce's USIBC is the premier business advocacy organisation, comprising top tier US and Indian companies. The council was created to advance US-India commercial ties.

Mission

To promote bilateral trade relations between India and the US through pro-growth policies that will advance commercial partnerships from 100 billion USD to 500 billion USD in the near future.

Vision

To create an inclusive bilateral trade environment between India and the US by serving as the voice of industry, linking governments to businesses, and supporting long-term commercial partnerships that will nurture the spirit of entrepreneurship, create jobs, and successfully contribute to the global economy.

Contacts

Nileema Pargaonker

Senior Director, Policy Advocacy, Financial Services,
Capital Markets and Tax
USIBC
Email: npargaonker@usibc.com

Rohan Sirkar

Senior Director, Financial Services
USIBC
Email: rsirkar@usibc.com

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,23,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

Contacts

Akash Gupt

Partner and Leader, Regulatory Services
PwC India
Email: akash.gupt@in.pwc.com
Phone: +91 12 4616 9602

Jamuna Rao Verghese

Senior Advisor, Financial Services
PwC India
Email: jamuna.r.verghese@in.pwc.com
Phone: +91 12 4616 9606

Team members

Aishwarya Agarwal
Avnee Gupta
Youhan Noria

AK/September2017-10504