ed messaging/session between consumer's phone and third party service provider/telecom Company. Minimum encryption standards to be specified to make the transaction banking grade.

¬ All subsequent routing of messages to the bank's servers must be with the highest level of security with dedicated connectivity like leased lines.

¬ All transactions that affect an account (those that result in to an account being debited or credited, including scheduling of such activity) should be allowed only after authentication of the mobile number and the PIN associated with it.

6 PROPOSED SECURITY POLICY

In the course of research for this report, which included interviews with key informants such as bank sector, multilateral donor and INGO officials, it is evident that despite recent successes, the private and public sector have some ways to go to actualize the potential for financial inclusion in Bangladesh.

With regard to the private sector, if one considers agent banking, it is evident that not all participating banks have a coherent strategy and business model with which to target segments of the underbanked market. Banks can capitalize on investments already made, even if they have been made by non-banking entities, such as International NGOs (INGOs) and other potential development sector partners, which tend to be better at understanding this segment of the market. A few banks have already begun to partner with INGOs to better understand how to approach this market.

Banks with agent banking licenses must carefully consider the early-mover advantages to the business of financial inclusion and devise governance processes in line with coherent corporate strategies. These strategies should encourage short-term investments in view of long-term returns, both in terms of profitability and branding value propositions. Capacity building is another important area, as banks need to build capacity to recruit, train, and manage agent banking networks, respecting both the uniqueness of agent banking operations relative to existing banking products, while not rendering them too exceptional to be integrated into strategic priorities.

The government of Bangladesh, through various ministries, departments and initiatives, has taken cognizance of the importance of and potential for financial inclusion and DFS, respectively. Salient are the role of the Bangladesh Bank and the Access to Information (A2i) initiative. The latter has sought to create Union Digital Centers (UDCs) to serve as agent banking points. The MRA and Palli Karma-Sahayak Foundation (PKSF) have also worked closely with international partners and multilaterals to refresh their thinking on financial inclusion.

As next steps, it is important for the government to set specific, measurable targets related to accomplishments in financial inclusion in line with global standards followed by the Alliance for Financial Inclusion as part of their Maya Declaration targets. Consumer protection has recently been announced through the September 2017 Prudential Guidelines. However, this remains an area where coordination with financial services providers and civil society entities remain important, so that customers of agent banking and mobile financial services are aware of the redress mechanisms and protection facilities.

Financial technology, or Fintech, as it is widely known, will also be a clear driver and catalyst for DFS-led financial inclusion. There remain several opportunities for the public and private sector to maximize the benefits and mitigate risks associated with Fintech. Fintech will entail integration of legacy systems in banks with IT systems required for MFS and agent banking. This is likely to be time-consuming and fraught with near-term challenges that bank boards need to embrace. Fintech entities, start-ups or more established companies, should also welcome and if necessary, make the case for "regulatory sandboxes" in which to operate within prescribed timelines to showcase the utility of their innovation (Brookings, 2017). The central bank should also mandate that Fintech companies be subject to cyber-security assessments and risk management trainings.

Last but not least, a much-needed Fintech-related innovation that is hopefully forthcoming is electronic KYC, or e-KYC. The UNCDF's Shift Project identifies e-KYC and "tiered KYC" as one of the salient challenges to including the under-banked. Existing KYC procedures constitute a significant barrier to formal financial inclusion. The database of National Identity (NID) that the Bangladesh Election Commission (BEC) has been developing, can facilitate the introduction e-KYC by financial services providers, and drive DFS adoption and financial inclusion. The UNCDF in Bangladesh prescribes a set of steps (See the figure on Steps towards E-KYC and Tiered KYC) in order to actualise e-KYC and tiered KYC. As is evident, improved coordination between firstly regulators, subsequently private sector players in harmonizing KYC can lead to development of practical guidelines on e-KYC and tiered KYC, which can remove a significant barrier to adoption of DFS.

Bangladesh Bank is planning to add a tool in its payment system to monitor transactions through Bkash and other mobile financial services in real time to check money laundering and terror financing, a highly placed central bank official said.

A recent report published by the USAID said, Bangladesh is among the biggest mobile banking market in the world and accounted for almost 8% of total registered global mobile banking users. Since a large number of population don't have access to conventional banking, mobile banking has become an instant hit in the country.

But the report has identified safety as one of the major critical points for mobile banking in Bangladesh. Concern has always been expressed by various stakeholders of MFS market regarding money laundering and terror financing through mobile phone system.

With careful planning that includes all the stakeholders, pro-

International Journal of Scientific & Engineering Research, Volume 8, Issue 1, Jun-2019
ISSN 2229-5518

cesses and technologies involved, the opportunity exists to make security an intrinsic element of all mobile payment systems.

Main issue that should be taken care of for electronic payments system is Authentication which identifies buyer and also makes sure that person is who he/she claims to be. Used methods are i.e. digital signature, finger prints, two steps verification (like Gmail), password or smart cards etc. Data integrity which means, that there must be a way to verify that data is not changed during the transactions. Confidentially must also be preserved.

Security for Online Systems Security of a customer's financial information is very important, without which online system could not operate. There are set up various security processes to reduce the risk of unauthorized online access to a customer's records, but there is no consistency to the various approaches adopted. The use of a secure website has become almost universally adopted. Though single password authentication is still in use, it by itself is not considered secure enough for online system in some countries. Basically there are two main systems for transaction security, secure socket layer and secure electronic Transaction.

Secure Socket Layer (SSL) SSL is the widely used secure service system and is an important measure to establish trust between online seller and buyer [8]. Encryption and decryption allow secure transfer of information between an Internet browser and server. Data cannot be intercepted or changed during transmission. SSL also permits merchant identification through SSL server certificates. The SSL standard has been widely adopted because it is relatively simple and easy to use and does not place excessive demands on the average consumer's home PC. SSL has an over 90% share of security measures, about the same as credit cards among online payment systems. Until recently, SSL provided services exclusively for fixed networks. But as mobile networks are increasingly important e-commerce markets, SSL services for wireless devices have been developed.

Secure Electronic Transaction (SET) SET is an alternative, more complex security system based on digital certificates and signatures [9]. SET needs specific software and is more difficult for cardholders to obtain and use, and despite the high level of security offered it has not gained widespread use.

7 What the government can do to spur growth?

The government has been extremely supportive of the ICT industry with significant funds flowing into digitization. However, for payment gateway integration a few supports has become essential. At this stage given the mobile internet ecosystem of Bangladesh (~60 million internet users, 95% of whom are on mobile devices) DCB (Direct Carrier Billing) has become an important issue. DCB will allow consumers to directly use their mobile balances to purchase via their smart devices directly. This will make the user purchase experience extremely smooth and will add growth points for the local tech ecosystem who can have a direct monetization channel. The adaptive behavioral change will definitely add to the e-banking growth.

Centralization of citizens' database via social security numbers to ensure credit history and accountability will help account maintenance and tracking experience. While we understand that smart card is a good start adding more centralization algorithms will reward consumers with proper credit history and will make due-diligence by the financial institutions a lot more fluid and hassle free.

8 Into the Next Level?

Digital Banking is the future – the Telecom revolution is a testament that consumers here are adaptable and open to moving into the cyber age. We just need to figure out how we integrate more immersive FinTechs while sufficiently addressing their concerns on security and mobilize the right stakeholders.

4 Conclusion

Though banking customers grow increasingly with the digital lifestyle, most Bangladeshi customers are not aware about m-banking in the country. They are not fully aware of the power of technology and do not seek to leverage it to enjoy better control over their banking operations and reap the benefits of m-banking. Instance, creating new markets, and reducing operational costs, administrative costs and workforce are increasingly important aspects for the banks' competitiveness, and m-banking may improve these aspects as well.

As mobile banking is still relatively new in Bangladesh, an understanding of the prospects and challenges to use mobile banking may influence its implementation. The findings of this study offer insight to commercial banks in Bangladesh in promoting the use of mobile banking among bank customers. In order to achieve this it is important for commercial banks to take into account the factors that this study had found on the use of mobile banking. The study results indicate that consumers are interested in assessing a wide range of banking services via mobile phone. The ability to access account balance enquiries via a mobile phone is the most compelling consumer banking service, followed by mobile fund transfers.

A second-tier of mobile banking opportunities includes reports for potentially fraudulent behavior, which reflect some of the security concerns around mobile banking and stock market information. The customer's perception was found to be overwhelmingly positive. The most appreciated feature was ubiquity and the overview over bank account. Fast reaction to market developments often cited as one of the most attractive feature of mobile banking did not find high appreciation. Security concern was found to be widespread followed by the cost of using mobile banking services. This means that

International Journal of Scientific & Engineering Research, Volume 8, Issue 1, Jun-2019
ISSN 2229-5518

the technology used must be secure and cost effective and at the same time convenient to deploy.

The plea for lower cost was found to be the preferred factor that will make mobile banking more attractive. This is followed by high speed of data transmission. Several factors including technical and security standards, regulatory and supervisory issues, and business and legal issues were found to be the main factors that may hinder mobile banking implementation in Bangladesh. Connectivity and secure communication platform and encrypted messaging system were found to be the factors that will enhance mobile banking implementation in Bangladesh. So, Bangladeshi banks should take the advantages of m-banking in the country and also take care of the factors that can make the m-banking service more attractive and user friendly.

Adoption rates of mobile banking are very high in some countries and this includes Bangladesh, and this is evidence of the tangible benefits and potential opportunities associated with mobile banking. While the main service that is supported at present is cash transfers the scope for offering more bank services is there. There are risks and costs associated with mobile banking for vulnerable people and these are associated with the consumer's own limited resources, structural inequality, and the asymmetry of power and resources the consumer faces vis-a-vis mobile bank suppliers. Some of these have been well documented by field work undertaken by CGAP.

Development practitioners can play a critical role in managing these risks and costs so that vulnerable people benefit from mobile banking. This will improve the likelihood that poor people benefit, that adoption by others continues, and that mobile banking contributes to national level development. Practitioners will need to understand the complex process of social innovation that requires they communicate with and gain the trust of local people and simultaneously working with mobile bank providers

ACKNOWLEDGMENT

First of all I would like to express my profound gratitude and sincere thanks to God who has been my source of inspiration and strength throughout this study period

My greatest thanks go to my supervisors, Dr Hafizur Rahman. I am so grateful the assistance and support in producing this work.

REFERENCES

[1] *Belinky M, Rennick, E. Veitch A. The Fintech Veitch A. 2.0 paper: rebooting financial services.Santander InnoVentures. 2015. Available from: http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf*

[2] The World Street Journal. 2016. Swift reports summer cyber attacks on three banks. [Cited 2016 Oct 9]. Available from: http://www.wsj.com/articles/swift-reports-summer-cyber-attackson-three-banks-1474924036

[3] Security Intelligence. 2016. Know your enemy, understand the motivation behind cyberattacks. [Cited 2016 Oct 11]. Available from: https://securityintelligence.com/know-yourenemy-understanding-the-motivation-behind-cyberattacks/

[4] ENISA. ENISA threat landscape 2015. European Union Agency for Network and Information Security; 2016. Available from: https://www.enisa.europa.eu/publications/etl2015

[5] Albasheer MOBashier EB. Enhanced model for pki certificate validation in the mobile banking. In: 2013 international conference on computing, electrical and electronics engineering (ICCEEE); Khartoum, Sudan; 2013 Aug 26–28. IEEE; 2013. p. 470–476.

[6] Ahamad SS, Sastry VNNair M. A biometric based secure mobile payment framework. In: 2013 4th international conference on computer and communication technology (ICCCT); Allahabad, India; 2013 Sep 20-22. IEEE; 2013. p. 239–246.

[7] Narendiran C, Rabara SARajendran N. Public key infrastructure for mobile banking security. In: global mobile congress; Shanghai; 2009 Oct 12–14. IEEE; 2009. p. 1–6.

[8] 8. Emerging Technologies, PCI Security Standards Council. 2014. PCI mobile payment acceptance security guidelines for merchants as end-users. Available from: https://www.pcisecuritystandards.org/documents/Mobile_Payment_Acceptance_Security_Guidelines_for_Merchants_v1-1.pdf?agreement=true&time=1483228800336

[9] 9. NIST. 2016. National Institute of Standards and Technology. [Cited 2016 Oct 11]. Available from: https://www.nist.gov/publications

[10] 10. Gov.uk. 2016. Cabinet office, government communications headquarters, new national cyber security centre set to bring UK expertise together.[Cited 2016 Oct 15].Available From: https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together

[11] 11. The World Economic Forum. 2016. The global risk report 2016, 11th edition. [Cited 2016 Oct 4]. Available From: https://www.weforum.org/reports/the-global-risks-report-2016/

[12] 12. World Bank. 2015. Global findex, 2014, financial inclusion. [Cited 2016 Sept 3]. Available from:http://datatopics.worldbank.org/financialinclusion/Infographics