Policy and Law on Digital Banking: Experience from Some Countries

Author’s Details: (1) Thi To Phuong Nguyen (2) Thi Thu Hien Phan  
(1)(2) University of Economics – Technology for Industries  
Correspondence: Thi To Phuong Nguyen, 456 Minh Khai, Hai Ba Trung, Ha Noi  
E: nttphuong@uneti.edu.vn; T: +84 (0) 942. 848. 666

Abstract:  
In Vietnam, the Prime Minister has approved Decision No.986/QD-TTg on the Development Strategy of the Vietnam Banking Sector to 2025, with orientations to 2030 which also aims to develop digital banking in order to create a basis for improving access to banking services, in particular, broadening the network of traditional channels in combination with enhancing the development of modern banking channels (electronic banking, mobile banking, internet banking, etc.,) through the application of technical advances. Policies on digital banking are made up of two components, namely the digital banking policy and law; and the application of technical advances. Researching policy and law governing digital banking is meant to be the fundamental and priority condition to facilitate both components. This research selected policy and law in Singapore, Thailand, and China as the mirror for Vietnam thereby giving some recommendations for Vietnam Government to amend and supplement policy and law on digital banking.  
Keywords: Digital banking, policy and law on digital banking

1. Introduction
The world is coming to a new era of innovation that will change the relationships between banks and their customers. Old-fashioned banks suffer from numerous drawbacks because they are far behind the latest technological breakthroughs in the 21st century’s digital economy. Thanks to innovations in information technology and mobile telecommunications adoption, there is an increasing trend in digital banking solutions. Digital banking is a valuable investment opportunity because traditional banks or even online banking are no longer able to adequately service their customers’ requirements in the digital revolution. Customer needs cannot be satisfied by traditional banks which is unable to catch up with the digital ages. The customers prefer digital banking to traditional banks due to their convenience and time savings. In Vietnam, according to a survey conducted by IDG Vietnam, 81% of surveyees responded that they used digital banking solutions in 2017 compared to 21% in 2015 (Fintechnews Vietnam, 2018).

Digital banking not only offers great opportunities for banks but also brings many challenges for both banks and state agencies. Banks shall have to clarify how to meet the high expectations of customers; utilize new technologies, prevent network security threats and protect customers’ information while the state agencies are being challenged by the protection of consumer interests, dealing with the risk of network security/data privacy and balancing management with innovation and competition.

In order to meet market demand and international integration timely, many domestic banks have actively applied new technological solutions to simplify the process and increase the coverage of products and services efficiently. However, the implementation of these solutions faces many challenges due to incomplete legal corridors. Therefore, the adjustment and updating of policy and laws in line with the inevitable reform of banking technology are really necessary and decisive for the long-term development of digital banking in Vietnam.

2. Literature review
2.1. Digital banking
In the mid-1970s, the automated teller machine (ATM) was first launched at a branch of Barclays bank which is considered as the earliest forms of digital banking. The electronic ATM is developed by John Shepherd-Barron, the De La Rue Company Limited. Thanks to ATM, customers could conduct banking transactions including cash withdrawals and check deposits (Linda Rodriguez McRobbie, 2015).

It was not until 1980s that the online banking is introduced to the customers. Together with the blossoming internet, producers started to sell their products online which give rise to the appearance of the Internet banking or online banking. Online banking allows customers to conduct several banking transactions such as money transfer, bank statements, and electronic bill payment through the internet by means of banks’ website or app. The modern digital banking world today was attributed to the development of the ecommerce systems in the early 2000s. Browser-based website and smartphones’ apps of banks gave customers easy access to banking transactions on the go beyond ATM machines and banking branches. In 2017, over 60% of consumers use their smartphones as the preferred method for digital banking (Jim Marous, 2017).
Customer behavior is changing rapidly, especially the younger generation of consumers, who regularly use smartphones and the internet to make purchases online. Banks which want to retain existing customers and attract new customers have to quickly digitize existing banking operations and move on to a completely new digital business model. As a result, digital banking appears and enables almost banking transactions to be carried out through electronic devices such as smartphone, tablet, and laptop without presence of customer at banks’ branch. In other words, the traditional banking model that is dependent on the branch network will eventually be transformed into an integrated model of digital banking.

Digital banking and electronic banking are two concepts that are gradually gaining popularity among customers because of its convenience and efficiency compared to traditional channels. Basically, these two types are quite similar in many respects, but in reality, there are still significant differences. Electronic banking was launched in Vietnam when the Internet usage is blooming. Banking transactions such as balance inquiry, withdrawal, money transfer, and savings are replaced by online operations (i.e. internet banking, mobile banking) as long as the customer is connected to the Internet. However, electronic banking is still only an alternative solution under the control of the traditional bank. Applications of digital banking will have all the functions of a real bank as mentioned above. All transactions are conducted online and you can send inquiries, questions only by mobile device. In general, electronic banking is just a utility of the bank, concentrating only on digitizing some of the core features of the bank, while digital banking embraces every programs and activities undertaken by banks and their customers. That is the difference between the two concepts Digital Banking and electronic banking. It can be said that digital banking is the trend of the future because this form of banking will help customers as well as financial institutions save, reduce costs and time significantly.

2.2. Law on digital banking

Digital banking is able to carry out most banking transactions automatically through the internet. Customers who conduct bank transactions by digital banking do not have to go to a bank branch and minimize the paperwork involved. At the same time, the digital banking features can be implemented at any time, regardless of space, so customers are completely active. With digital banking, only by financial application or website you can use all features such as: bank remittance, money transfer; pay the bill; loans; savings deposits; engage in financial products such as insurance, investment, personal finance and corporate finance. There are many definitions of digital banking, for examples:

“Digital Banking - a new concept in the area of electronic banking, which aims to enrich standard online and mobile banking services by integrating digital technologies, for example strategic analytics tools, social media interactions, innovative payment solutions, mobile technology and a focus on user experience.” (Paper of 5th International Conference on Governance in India Financial Services Sector: Reform and Remedies, 2018, p.125) This concept clearly states that digital banking is a higher stage of online banking and mobile banking. By listing solutions and services offered through digital banking, this definition still emphasizes the purpose of digital banks to increase user experience.

Contrary to this definition, Fivedegree took a completely different approach when it came to arguing that digital banking is the digitalization of all products and services as well as the traditional banking process and the further development of online banking or mobile banking. This definition clearly states that the bank requires each step of the bank's operation process to be automated and specifically: “Digital banking means the full digitization of banks and all its activities, programs and functions. It’s not just about digitizing your services and products - the front-end that customers see - but also about automating your processes (the back-end) and connecting these worlds with middleware. Digital banking is about the automation of every step of the banking relationship, and it goes way beyond an online or mobile banking platform.” (Fivedegree, 2018).

Another definition which focuses on benefits of digital banking for both commercial banks and customer has been explained by Rajendra Kumar Tolety. In particular, “Digital Banking is the application of technology to ensure seamless end-to-end (STP in the ‘old’ jargon) processing of banking transactions and operations; initiated by the client, ensuring maximum utility to the client in terms of availability, usefulness and cost; to the bank in terms of reduced operating costs, zero errors and enhanced services.” (Rajendra Kumar Tolety, 2018, p.2).

Bearing all of the above mentioned objective, features, characteristics as well as benefits of digital banking, from the author’s point of view, Digital Banking is a combination of emerging new technologies (i.e. eKYC, big data, API, artificial intelligence, etc.), in financial services organizations to accommodate changes in internal and external relationships that improve service and experience of customers in order to adapt to the highly competitive business environment and improve the business management capability of commercial banks in the near future. As a result, Law on digital banking is a system of rules on Digital banking that are created and enforced by a state to regulate behavior amongst state agencies (i.e. government, state bank), credit institution (commercial banks, fintech) and customers including but not limited to (i) the establishment, operation, management of digital banks; (ii) requirements and
conditions for the credit institution when providing digital banking product and services; (iii) rights and obligations of the customer when using digital banking product and services.

3. Policy and Law on Digital Banking in some countries

3.1. Thailand

The future for banking in Thailand is clearly digital with more and more technology investment and policy support. Thailand has always been one of the leader in digital banking transformation of East Asia. Thus, almost banks in Thailand are in the course of digitalization to improve customers’ experience. KBank, one of the pioneers in term of digital transformation, has begun to invest in digital technology services with total investment of THB480 million annually. There are 7.3 million customer using mobile banking services of KBank which increase number of transactions from 300 million in 2014 to 3 billion in 2017 (Somruedi Banchongduang, 2018). THB40 billion was also used by Siam Commercial Bank Public Company Limited to develop its digital banking platform in 2017. Bank of Ayudhya took its very first step in the course of digital transformation by investing THB20 billion to enhance technology infrastructure of the bank (Somruedi Banchongduang and Oranan Paweewun, 2018).

![Figure 1: Thailand’s internet and mobile banking transaction volume](source)

As reported by the BOT, the total value of mobile banking transactions up to June 2018 is 1,269 Billions of Baht and internet banking transactions’ value is 2,187 Billions of Baht.

**a. Policies on digital banking development**

In the development of the policy framework in digital banking development, the Bank of Thailand (BOT) has promulgated Financial Sector Master Plan in three phases, in particulars: Phase I (2004-2008), Phase II (2010-2014), Phase III (2016-2020). Phase I set out a number of measures regarding post-1997 financial crisis “house-cleaning” including: structural improvement and re-organization of Thai financial institutions, with the main goals of improving risk management and governance practices, as well as expanding the public’s access to financial services. Phase II provides guidance on access to financial services and effective risk management measures were still key considerations in this second Master Plan. The State Bank of Thailand also sets out the Financial Sector Master Plan Phase III for the period from 2016 to 2020, with the participation of government agencies to grant access and data connection to the data system, the promoting of coordination among financial institutions and electronic payment service providers, and the establishment of a legal framework, technology infrastructure for services and delivery electronic transactions. Key considerations in Phase III are not only promoting electronic financial and payment services but also supporting financial service providers to develop infrastructure and offer financial products and services that meet customers’ needs.

Besides, National e-Payment Plan which launched by the government will also be supported by the BOT in 2017. Accordingly, risk and fraud also pose a threat to the development on the digital banking which leads to BOT’s policies on ensuring stability of financial institutions by improving risk management and supervision. Commercial banks is requested
to promulgate strategies and regulation on operation management, special examination, analysis and monitoring as well as conduct onsite examination and risk assessment for significant activities and information technology.

In addition, Thailand has proved its leading position in digital transformation by adopting and applying block chain technology for banking application. Under Thailand’s central bank’ disclosure on March 14 2018, Thailand Block chain Community Initiative including 14 Thailand top banks have been established to develop Linux Foundation’s Hyperledger Fabric, a block chain-based platform designed by IBM block chain services to digitize letters of guarantee and other documents. The service will be tested in regulatory sandbox to streamline data verification, prevent fraud information, simplify the normal process, and increase the efficiency for business.

The latest project of Thailand or the so called Project Inthanon has been launched in August 2018 to create a new way of conducting interbank settlement using wholesale central bank digital currency - Thailand national digital currency. Accordingly, prototype will be built on open-source block chain namely Corda, a distributed ledger technology (DLT) platform developed by R3, an US fintech company. This project aims to raise the Thai financial sector’s technological readiness in adopting new financial technologies to enhance operational efficiencies.

b. Legal Framework

The State Bank of Thailand issues Notification SorNorSor 7/2559 guiding financial institutions on accepting deposits or receiving money from the public. Accordingly, banks are allowed to use mechanisms in digital platform to ensure effective and accurate identification and verification of their customers (electronic – know your customer or eKYC). In eKYC process, banks can use the following methods: (i) video camera which interact with bank teller via video channel during the account opening process; (ii) electronic documents having the same legality with traditional documents; (iii) electronic signature of the customer; (iii) Authentication of customer information and identification documents shall be made by means of smart card reader and/or through personal information systems, identity card or fingerprint identification. As provided by Notification SorNorSor 7/2559, eKYC process must meet the same standards as KYC on a face-to-face basic and be applied for individual customers using electronic devices such as computers, telephones or other electronic devices. Before implementing eKYC, banks and financial institutions must establish the effective risk management process and be approved by the State Bank of Thailand. At present, Thai banks are still hesitant in implementing eKYC because they are still in the process of research and searching for new technology solutions. Therefore, there are no Thai banks officially put eKYC into use.

In order to encourage the development of financial technology innovations, Bank of Thailand established a regulatory sandbox on 21 December 2016. Accordingly, the regulatory sandbox specifies qualifications for participation and rules to be followed once permission is granted to operate within the regulatory sandbox. This regulation enable participants such as financial institutions, fintech firms, and general tech firms to test new technology in financial services including lending, payment, or any other type of transaction within the scope of authority of the Bank of Thailand. Besides, participants are still required to have licences that are necessary to conduct their intended businesses as well as comply with the laws that are beyond the authority of the BOT, such as laws relating to electronic transactions, anti-money laundering, and anti-terrorism. In granting permission to participate in the regulatory sandbox, participants shall have to set out measures to manage corporate governance, security and integrity of IT systems as well as protection of customer information.

PromptPay which is a part of Thailand national e-payment scheme, is an electronic wallet product developed by the State Bank of Thailand from 2016, allowing individuals and organizations to make quick and easy transfer while using their personal telephone number or identification number instead of the current account number. As one of the Thailand 4.0 initiatives, PromptPay is expected to move Thailand towards a cashless society and create a value-based economy driven by innovation, technology and creativity. According to a survey published by Bangkok Post, there have been 37 million savings accounts which lead to 97 million transactions, totaling 370 billion Baht in transfers. 12 million of those accounts were opened with mobile phone numbers and the rest with citizen ID numbers (BangkokPost, 2018). In the first stage, PromptPay only performs peer-to-peer transactions (P2P) and then rolls out to enterprise customers. In the near future, Thai government hopes to use PromptPay for social benefits, financial assistance and tax refunds for citizens. To sign up for PromptPay, Thai citizens need to provide their current account number, telephone number or identification number. Telephone number or identification number will only be associated with a current account number. Registration can be made at bank branches, ATMs, mobile banking or internet banking. With the launch of PromptPay, Thai government expects to encourage people to use banking services, reduce cash expenditures, increase efficiency and accuracy, and reduce the burden on the payment system and increase the competitiveness of the country.

c. Protection of customers’ information and transactions’ security

As a matter of fact, Thailand does not have any specific law governing data protection. Up till now, the draft of the Law on Personal Data protection published on September 2018 still needs the approval of National Legislative
Assembly to be implemented. The pending approval of Thailand government on the draft Law does not mean that there is no protection for personal data protection. On the contrary, service providers in some sectors including banking and finance, insurance, telecommunication, and health care, electronic payment service are still imposed to take the responsibilities on customer data protection. The collection, storage and use of customer information in banking and finance service is regulated by Financial Institution Business Act BE 2551 (amended), as well as Royal Decree on Electronic Payment (Decree). Accordingly, data is kept within the course of banking trading and only used for the purpose of its operation. In other words, customer information which are protected by banks as the service provider shall not be disclosed unless banks have prior approval by the customer. Financial institution must observe and comply with the regulation of the Central bank, i.e BOT on transferring the customer information to a third party. In the event that it breaches its obligation regulated by laws, it may have to notify BOT. Besides, as prescribed by Decree, an applicant for an electronic payment license must explain how it will protect service users’ information, including how such information will be stored which constitutes a condition for the license to be effective.

Under the rule of BOT, where electronic money card service provider outsource a service relating to information technology or any support functions to another service provider, the providers shall have a responsibility for customers with the security. Each electronic money card service provider shall have security policy over its services to ensure the control and integrity of system and data, customer authentication and non-repudiation, data confidentiality, system availability, system monitoring and resolution and report of loss incident or more than 24 hours of system disruption. At least once per year, the electronic money card service provider has to examine its information technology systems and evaluate to check whether those systems be consistent with the Bank of Thailand’s policies and measures on security of information system. After completing the examination, the electronic money card service provider shall submit a copy of report to the Bank of Thailand within 30 days.

3.2. Singapore

According to the Global Financial Centers Index 24 released in September 2018, Singapore had ranked fourth globally, and the second largest in Asia where many banks and financial institution choose to relocate their headquarters in Asia.

<table>
<thead>
<tr>
<th>Centre</th>
<th>GFCI 24 Rank</th>
<th>Rating</th>
<th>GFCI 23 Rank</th>
<th>Rating</th>
<th>Change in Rank</th>
<th>Change in Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hong Kong</td>
<td>3</td>
<td>783</td>
<td>3</td>
<td>781</td>
<td>0</td>
<td>▲2</td>
</tr>
<tr>
<td>Singapore</td>
<td>4</td>
<td>769</td>
<td>4</td>
<td>765</td>
<td>0</td>
<td>▲4</td>
</tr>
<tr>
<td>Shanghai</td>
<td>5</td>
<td>766</td>
<td>6</td>
<td>741</td>
<td>▲1</td>
<td>▲25</td>
</tr>
<tr>
<td>Tokyo</td>
<td>6</td>
<td>746</td>
<td>5</td>
<td>749</td>
<td>▼1</td>
<td>▼3</td>
</tr>
<tr>
<td>Sydney</td>
<td>7</td>
<td>734</td>
<td>9</td>
<td>724</td>
<td>▲2</td>
<td>▲10</td>
</tr>
</tbody>
</table>

*Source: The Global Financial Centers Index 24 (2018)*

Known as the smart country, all of Singapore's digital economy and e-commerce initiatives are at the forefront in the Asia Pacific. According to the data provided by MasterCard Advisors analytics, Singapore shows that the estimated share of payments done by non-cash methods accounted for 61% which ranked the first place in the most cashless nation in the world (MasterCard, 2017). Developed economic and political environment, favorable tax and law policies, and the enforcement of financial crimes have contributed to help Singapore become the Asia's largest commodities and foreign exchange with about 117 foreign banks and 6 local banks dominating the banking sector, managed by the Monetary Authority of Singapore (MAS). MAS play an active role in providing financial support and finalizing legislation to facilitate Singapore's rapid adoption of financial technologies. In 2015, MAS committed US$ 166 million over five years to promote technological innovation in the financial sector (Cambridge Center for Alternative Finance, 2017).

a. Policies on digital banking development

Singapore has built MyInfo - a centrally managed personal data platform. The data stored includes the government-verified personal details such as passport number and residential status, to contact information including mobile number, e-mail address, and billing address. MyInfo enables Singapore citizens to provide personal information only once for the government instead of repeating this in every e-transaction. This digitized database extracts information from the relevant state agency to produce a basic citizen record for one day. MyInfo which was accessed in May 2017 was available on 24 e-government services, with another 140 to be added by 2018. However, in order to retrieve personal information to facilitate 19 online services, such as credit card application, explicit user consent had to be provided (Eileen Yu, 2017). Citizens can use their MyInfo profile to fill out forms in transactions, including banking, extremely fast and
convenient. For more efficient KYC using trusted government collected personal data, four banks including DBS and Standard Chartered have been allowed to use this database to help customers fill in their individual account opening forms and will soon expand their card issuance or loan applications. As for the banks, they do not have to get their customers fill in forms and provide hardcopy documents for manual verification. The customer finds it very convenient for them when using banking services. MyInfo had garnered 200,000 enrolments, according to GovTech. By December 2017, this number would be significantly boosted when entire 3.3 million Singpass users, an electronic portal linked to hundreds of e-services provided by 60 state agencies deployed in 2003, would automatically be linked to their MyInfo profiles. In addition, the Singapore government is building and developing a virtual ID - digitally identifying Singaporean citizens (Wong Casandra, 2017). Besides, in July 2016, the GovTech has assigned Gemalto to pilot electronic security systems for the medical and financial sectors to identify individuals using the Internet as digital identity for every citizen. A digital ID is said to better protect customers from threats such as online fraud and theft. Furthermore, digital ID facilitate the customers to get rid of the trouble of remembering different usernames and passwords.

b. Legal Framework

The Singapore government is actively supporting the development of digital banking. In November 2016, MAS issued Regulatory Sandbox guidelines that enabled registration of initiatives that are more widely applicable in Singapore and globally. A sandbox is a software-enabled environment which is under strict control, limiting the functionality of a piece of code, granting some code to perform only some functions. Therefore, it is not possible to perform other interventions that may harm the user's computer. Sandbox includes appropriate safeguards, maintaining the safety and integrity of the financial system. Banks and FinTech can register with MAS to test new technologies without worrying about compliance with current regulations. In addition, MAS can also support the reduction of some strict requirements for the product during the test. After successful testing, FinTech companies or banks will be fully compliant with regulations promulgated by the MAS. All products that FinTech companies or banks are testing are publicly available on the MAS website for the public to know.

In the context of the globalization in financial sector and the development of digital banking, MAS has proposed a policy framework to support and encourage financial institutions to invest in information systems and reduce risks caused by technology. MAS requires banks to apply rules relating to information security and risk management in order to (i) establish a robust and sustainable technology risk management framework; (ii) Enhance security, reliability, usability and system resiliency; (iii) implement encryption and authentication mechanisms to protect customer data and transactions. MAS has developed revised Internet Banking and Technology Risk Management Guidelines to provide guidelines for dealing with threats and cyber-attacks, including popular network attacks such as MITM attack. A guide to the introduction of advanced technology risk management requirements to enhance the security of data systems and IT infrastructure, and to detail the system development process as well as secure privacy MAS clearly defines the responsibilities of the Board of Directors and the Board of Directors in managing and controlling technological risks in banking business. Board of Management of the bank must continuously monitor the suitability, effectiveness of risk management and information security practices as well as implement compliance and audit procedures to ensure compliance of the control measures. MAS also encourages financial institutions and industry associations to take the lead in raising awareness of the benefits and risks of digital banking. This will help to create a sense of information security environment and improve the trust of service users in online financial systems.

In addition, Singapore has issued additional regulations guiding the risk management and mitigation in the KYC process, such as the Sound Management of Risks related to Money Laundering and Financing of Terrorism (updated June 2017) which requires banks to develop processes, regulations on classification of risk and authentication of customer identity. Besides, a Payments Council, comprising 20 leaders from banks, payment service providers, businesses, and trade associations was proposed to be established by MAS on 2 August 2017. This is intended to allow the establishment of a more efficient management mechanism, based on the performance of payment service providers rather than individual payment systems. The setting up of the Payments Council will also create new payments legislation to safeguard consumer interests and facilitate innovative payment solutions.

Regarding lending-based crowd funding or the so called P2P lending, the lending is carried out by means of online platform which is regulated under the Securities and Futures Act (Cap.289) and the Financial Advisers Acts (Cap. 110). In Singapore, P2P lending allows many investors lend sums of money to a enterprise (which is not an individual) and the lender shall receive such enterprise’s legally-binding commitment to repay the loan at pre-determined time and specific interest rates. Accordingly, the operator of the lending platform is required to hold a license namely capital markets services under Securities and Futures Act. Besides, an invitation to lend a sum of money of a company is also regarded as the debentures, which is a type of security. In such context, to be funded by the investors, borrower shall have to prepare and register a prospectus with MAS in accordance with Securities and Futures Act unless it take the advantages.

http://www.ijmsbr.com
of several prospectus exemptions including (i) small offers ($5 million within 12-month period); or (ii) private placements (issuing debentures to no more than 50 person within 12-month period); or (iii) offers of debentures to investors such as institutional investors and accredited ones. In order to protect the investor from the risks beyond their actual capacity where their funds may wiped out, lenders on P2P platforms must be accredited investors whose net worth of at least SG$2 million or an income of at least SG$300,000 in the past 12 months.

c. Protection of customers’ information and transactions’ security

Section 47 of Banking Act (Cap 19, 2008 Rev Ed.) regulates that Singapore’s banks are consistent with statutory obligation of security of customers and their accounts. Section 47 also allows banks may disclose customers’ information in some cases. Accordingly, customer information shall not, in any way, be disclosed by a bank (a bank incorporated in Singapore or the branches and offices located within Singapore of a bank incorporated outside Singapore) or any of its officers, to any other person except as expressly provided in the Banking Act. Consequently, the confidentiality obligation under section 47 extends to the bank as well as its officers. An ‘officer’ is defined in section 2(1) of the Banking Act (Cap 19, 2008 Rev Ed) to include a director, secretary, employee, receiver, manager and liquidator. This obligation continues after termination of the recipient’s appointment, employment or other office in which the information was received.

In addition, banks have to observe and comply with following obligations under the Personal Data Protection Act 2012 (PDPA): (i) Banks may only collect, use and disclose personal data of an individual with the individual’s consent, and for a reasonable purpose which the organization has made known to the individual; (ii) Personal data must not be transferred outside Singapore except in accordance with requirements of the PDPA. In short, banks are to provide a standard of protection to the transferred personal data comparable to the protection granted under the PDPA; (iii) Except in certain circumstances (which is discussed below), banks must accede to an individual’s right of access and correction in respect of his personal data that is in the bank’s possession. The individual has a right of action for relief against a bank for losses or damages suffered directly as a result of the contravention by the bank of its personal data protection obligations.

Upon contravening statutory obligations of banking secrecy, an individual may be punished with a fine not exceeding S$125,000, or imprisonment for a term not exceeding three years, or both. In the case of a corporation, a fine not exceeding S$250,000 may be imposed.

3.3. China

China began to develop digital financial services later than other countries, with significant developments beginning in the late 1990s. Further, the boom of financial and digital banking began only about five years ago. However, the country has taken advantage of the latter and is growing faster than most other countries in the world.

Digital banks rely on commercial banks to meet the requirements of the People's Bank of China to KYC when opening bank accounts while commercial banks use advances in digital finance to develop product quality and expand customer base. Thus, a number of banks in China have cooperate with fintech to take the advantages of new technology and innovation. China Construction Bank formed a strategic partnership with Alibaba and its subsidiary Ant Financial in 29th March 2017. Under the partnership agreement, China Construction Bank shall be provided the wealth management products through Ant Financial’s Alipay and Ant Fortune platforms. In June 2017, Agricultural Bank of China Ltd and China’s major internet search engines Baidu had signed agreement to build intelligent bank using big data, artificial intelligence and cloud computing. In September 2017, Bank of China cooperated with Tencent to establish a joint financial technology laboratory focus on cloud computing, big data, block chain and artificial intelligence.

It can be seen from Chart 3 that there is a remarkable rise in the number of internet banking and mobile banking subscribers from 2013 to 2020. In 2018, mobile banking consumers are 1300 million and it is expected to hit a peak of 1600 million by 2020 while the number of internet banking users reaches the highest of 1200 in 2020.

http://www.ijmsbr.com
Figure 2: Adoption of internet banking and mobile banking in China
Source: Asian Banker Research (2017)

a. Policies on digital banking development

The Chinese government has developed a comprehensive regulatory framework for digital banking by issuing the Guidance on Promoting internet Finance’s Healthy Development 2015. In general, this Guidance sets forth key regulatory, including: internet payment services, online lending services; internet security and information safety; anti money laundering activities and prohibition of financial crimes; the protection of consumers, etc., Accordingly, digital finance transactions including internet payment services, peer to peer lending and micro-loans, and online equity crowdfunding services is limited to small value. This prevents risks resulting from larger transactions as well as secures the efficiency and cost-effectiveness of digital finance. Besides, the Guidance has set out the division of responsibilities between the relevant regulatory authorities which will facilitate the coordination between the authorities in supervising digital finance activities.

In order to manage the risk of accumulations that affect the legitimate rights and interests of investors as well as the reputation and development of the financial industry, the Government issues the Action Plan on Thematic Regulation of Internet Finance Risks in 2016. The goal of the Action Plan is to standardize the management and oversight of digital finance by balancing the conflicting objectives of protecting consumers and encouraging financial incentives and plans for start-up. Regulatory concern in every Internet finance subsector is also identified in the Action Plan.

b. Legal Framework

With regard to internet banking, Rules on the Administration of Electronic banking (the “Rule”) was enacted by China Banking Regulatory Commission in 2006 in order to strengthen the risk management in conducting electronic banking transactions as well as protect the rights and interests of the customers. Accordingly, electronic banking services provided by the banks through internet, telephone, mobile phone and other digital devices and networks shall have to meet the requirement of the Rule. In general, there are several conditions which the service providers must comply with, including: (i) seeking for CBRC’s approval before conducting domestic and/or cross-border electronic banking business; (ii) setting up the internal and external risk management and evaluation as well as establishing the risk department. Within the scope of domestic e-banking businesses, banks are required to have plans and strategy, competent personnel and internal system to control and mange risks associated with the operation of e-banking businesses; and protect the legitimate rights of their customers. In addition to the requirements mentioned above, when doing cross-border e-banking businesses which mean that a Chinese bank using e-banking platform to provide e-banking services to customer, banks shall have to comply with the laws of the country where the customers reside. Besides, Chinese banks take the responsibilities to report to China Banking Regulatory Commission the detail of the cross-border banking transaction including: (i) scope of services; (ii) contractual agreement with the customers. Besides, under the Rule, banks are required
to report to China Banking Regulatory Commission regarding the development, operation, profitability, and internal risk management and external professional evaluation of their e-banking businesses. Together with the self-evaluation of each financial institution, each bank have to engage a third party which is an independent qualified valuation firm recognized by China Banking Regulatory Commission to carry out a security evaluation of their e-banking system. The Rules also set out provision which impose the banks’ liabilities for any damages suffered by the banks’ customers in the event if the damages is not caused by factors attributable to consumer, including illegal operation of e-banking systems, or security problems of such banks.

Regarding third party payment service, China Government has issued Rules on the Administration of Payment Services Provided by Nonfinancial Institutions and Measures on the Implementation of the Rules on the Administration of Payment Services Provided by Non-Financial Institutions in 2010. Third party payment services are non-financial payment services, including online payment, issuance and acceptance of prepaid cards, acceptance of bank cards, and other payment services. In order to provide these services, the non-financial institution must apply for a payment service business license from the People's Bank of China. Accordingly, service providers must meet a number of requirements, such as: minimum capital requirements (i.e. RMB 100 million for the provision of payment services nationally or RMB 30 million for the provision of payment services at provincial levels); having measures on anti-money laundering; having payment system; personnel, organisational and facility requirements. Payment service regulations also set a limit on the total amount of payment each year depending on the method of authentication of the customer. Since 2015, the People's Bank of China also requires non-financial institutions to provide payment services that comply with customer authentication, protection and money laundering regulations.

Besides, peer-to-peer lending (known as P2P lending) which has grown rapidly in recent years in China is a new method of debt financing that allows customers to borrow and lend money through lending intermediaries but a financial institution. With peer-to-peer lending, lending intermediaries often establish a P2P online platform for both borrowers and investors to finance a loan. In particular, the borrowers shall provide their profile, loan amount while the individual investors shall assess such profiles and review the loan amount to consider granting a decision to offer a loan to a borrower for an agreed interest rate. In peer-to-peer lending, a loan may be granted from one or more investors and the borrower has to repay the debt to each of the investors. In order to govern the increasing P2P lending, China Government has issued Circular on Risks Associated with Peer-to-Peer Lending 2011. However, the Circular has been proven ineffective to control these risks due to lack of specific rules and requirements on P2P lending which give rise to increasing risks and illegal activities. For example, the famous P2P lending platform namely Ezubao has proven to be the Ponzi scheme and became the biggest financial fraud in Chinese history when it lost 59.8 billion yuan ($9.14 billion) from more than 900,000 investors by the end of 2015 (Neil Gough, 2016). Thus, Action Plan on Regulation of Online P2P Lending Risks has been issued in April 2016 to regulate P2P lending activities and lending intermediaries’ activities. As a result, lending intermediaries must obtain a Telecommunications business license and appoint a bank to serve as a custodian of customer funds.

c. Protection of customers’ information

As customers’ information protection has become a global issue in the digital banking sector, several laws and regulations have been promulgated by China Government such as Criminal Law 1979, Law on Protection of Consumer Rights and Interests 1993 amended in 2014, General Rules of Civil Law 2017, Cyber Security Law 2017. Since the enactment of the Cyber Security Law in 2017, the legal framework on protection of customers’ information is said to be comprehensive and clear. Accordingly, banks as the service provider are required to obtain their customers’ consent before disclosure of customers’ information as well as disclose the purpose, means and scope of information’s use to their customers. Banks are also restricted to collect any more personal information than necessary. After being used and processed for the purpose of the transaction, the personal information should be deleted or anonymised. Following the enactment of the Cyber Security Law, an interpretation of existing legal protections of customers’ information and penalties for violation is issued by China’s Supreme People’s Court and China’s Supreme People’s Procuratorate in June 2017. In banking industry, China Banking Regulatory Commission also promulgate E-banking Rule which requires e-banking services providers to enter into a contract with their customers and to disclose to matters such as risks, rights and obligations.

4. Conclusion

According to analysis and factual data from selected countries and the world, it can be concluded that it rarely exists a country having developed digital banking without a new policy and a law allowing the application of technical advances (eID, eKYC, Blockchain, AI, API, Big data). As mentioned above, Policies digital banking are made up of two components, namely the digital banking policy and law and the application of technical advances. Researching policy and law governing digital banking is meant to be the fundamental and priority condition to facilitate both components.
Vietnam has a number of basic regulations in the field of digitalization in financial and banking transactions. However, regulations in digital banking have not kept pace with the rapid development in practice. In particular, the legal corridor for digital banking is generally incompatible with the digital context which has focused on the payment service but there are no specific regulations for electronic savings deposits, electronic loans of the commercial bank as well as operations of Fintech. Existing regulations on data security and money laundering should also be strengthened to protect consumers when using new technology services while increasing customers’ awareness of digital banking are important conditions to facilitate the development of digital banking in Vietnam.

In the transformation from the traditional model to digital ones, the commercial banks are said to (i) set digital transformation strategy with a staged approach (standardization of banking governance and operations; partial digitizations; traditional and digital banking service de...); (ii) focus on risk management solutions, security and confidentiality solutions to secure users’ data; (iii) emphasize on investment into technology infrastructure, IT applications, leverage on the available technology platforms; and (iv) human resource training and allocation plans to step-by-step execute digital transformation.

5. References


xix. Financegenius, 2016, 7 Reasons to Put the Loan Origination System (LOS) in the Cloud, page 23.


