

Policy and Law on Digital Banking in Some Countries

Author's Details:

(1)Thi Thu Huyen Tran (2)Thi Thanh Tan Pham

(1) (2) University of Economics - Technology for Industries, Vietnam

Correspondence: Thi Thu Huyen Tran, 456 Minh Khai, Hai Ba Trung, Ha Noi

Abstract:

Digital technology is gradually changing the form of providing financial and banking services. The development of banking services based on digital technology can help banks innovate comprehensively from the process of providing products and services, innovating the distribution channel system, expanding the product portfolio, providing Service level to a wider range of customers at a lower cost. This article will introduce the basic concepts of digital banking, international experience in digital banking development, and lessons for Vietnamese banks.

Keywords: Digital banking, policy and law.

1. Introduction

In the world, the trend of digitizing banking activities is getting stronger and clearer. According to experts in the financial sector, the development of banking services based on digital technology can help banks innovate comprehensively from the process of providing products and services, innovating the distribution channel system. coordinate, expand the product portfolio, provide services to a wider range of customers at lower costs. Digital technology is also an opportunity for countries to promote financial inclusion, towards providing appropriate and convenient financial services for all individuals and organizations, especially for those with Low and vulnerable incomes are aimed at increasing access to finance, contributing to the creation of opportunities for livelihoods, investment flows and savings in society, thereby promoting economic growth.

Specifically, experts say that the application of digital technology to banking operations will increase costs by about 31% but also increase net profit by about 43%. Figures published at Vietnam Retail Banking Forum 2017 under the theme "The future of retail banking and payment services during the 4th Industrial Revolution" show that in 2018, there will be 44% of sales. Banking revenue comes from digital banking services. The application of digital technology also helps the bank increase 45% of profit opportunities in the retail segment, reduce costs, improve service quality, thereby maintaining a sustainable competitive advantage compared to competitors. no ability to compete with digitalization throughout (Nguyen Van Chuong, 2018).

2. Policy and Law on digital banking in some countries

2.1. European Union

According to Master Card's EU Digital Banking Study, more than 90% of people in EU are interested in digital banking solutions or have positive feeling about the increasing of new banking solutions which is attributed to time-saving (70%) and ease of use (59%) (Master Card, 2017).

In 2017, total value of card transactions is €69.2 billion. The importance of transactions initiated electronically continued to increase, with the number of electronic transactions is as ten times as paper-based ones. Besides, the total number of ATMs decreased by 1.0% to 0.43 million, while the number of POS terminals increased by 9.9% to 13.5 million. Mobile wallet transactions in EU are expected to grow at 61.8% during 5 years period from 2016 to 2021 (European Central Bank, 2018).

Policy on cash payment limit has been imposed in many European countries. Take an example of payment policy in Italy, any and all purchase agreement with total value of €1,000 or more must be carried out by electronic payment method. The government of France and Spain has put lots of effort in encouraging their citizens changing payment method from cash and cheques to digital payment by decreasing transaction fees.

The Payment Services Directive (PSD1) was first promulgated in 2007 to increase competition in payments amongst banks and non-banks, as well as protect consumer rights by applying the same rules across

EU market. In addition to banks, central banks, government bodies, PSD1 define new legal concept, namely “payment institution” which can provide payment services by providing for the authorisation subject to a number of strict and comprehensive conditions. However, PSD1 only governs payment within the European countries, but not cover transactions to or from third countries and PSD1 exemptions on payment activities leave customers unprotected. Hence, Payment Services Directive (PSD2) was enacted by the Council of the European Union in 2015 to better protect customers, improve the cross-border payment system in EU and encourage innovation in digital banking. Under PSD2, banks are required to follow technical standards which are established in multiple layers. The first layer is about the basic compliance. In the second layer, banks are subject to several standards on liabilities, disputes, refusals, refunds. The third layer sets out additional optional services. PSD2 is considered as the legal basis for third party service providers to use open APIs to collect customers’ data if such collection has been prior approved by customers. Customer identification information can be provided to third parties by banks in order to shorten the customer identification term. Fintech and non-bank financial services providers’ activities are also added to govern subject of PSD2 which is said to be the biggest amendment in PSD2.

Electronic Identity and Electronic Services (eIDAS) which was enacted to increase digital growth among EU countries entered into force on 17 September 2014. It provides requirements on electronic transactions, advanced electronic signature, qualified electronic signature, qualified digital certificate, and trust services in order to facilitate secure and seamless electronic interactions between businesses, citizens and public authorities. EU members must ensure the establishment of a common framework that will recognize eIDs from other member states as well as its authenticity and security. Accordingly, the electronic signature shall have the same legal validity with the text signature and digital service providers in EU states shall recognize electronic identification from all EU member states as of September 29, 2018.

Up till January 2019, there are 5 of 28 Member States including Denmark, the Netherlands, Poland and the UK having established the Regulatory sandboxes which is a closed environments allowing testing of innovations by financial institutions under the regulator’s supervision. In the case of the UK, the UK Financial Conduct Authority has enacted the Innovate Regulatory Sandbox in 2016. Under the Financial Conduct Authority’s Regulatory Sandbox, the process for a financial institution to apply the regulatory sandbox including 7 steps, including: (i) Firm proposal to use sandbox; (ii) Financial Conduct Authority assessment; (iii) Firm and Financial Conduct Authority collaborate and agree the testing approach; (iv) delivery of sandbox option and; (v) testing and monitoring; (vi) firm submits final report for Financial Conduct Authority’s final review; and (vii) firm decides whether it will offer solution. In general, the financial institution’s new solution must be proved to meets the criteria by several tests. If the final report on such new solution is approved by Financial Conduct Authority, the financial institution shall make decision on whether it will offer the new solution outside the sandbox or not. Regulatory sandbox enable the financial institutions to reduce cost related to compliance consultants and lawyers as well as fast-track the regulatory process while offers a safe space with safeguards to customer using new financial services and products.

Regarding the payment security, the European authorities have enacted several guidelines to provide the legal basis for all payment services providers in EU member states. In 2014, Guidelines on Security of Internet Payment was promulgated by the European Banking Authority to enhance the understanding of issues on the security of electronic retail payment services. This guideline enables secure and efficient internet payments amongst EU market which force payment service providers to implement strong customer authentication. Accordingly, to prevent fraud and cybercrime when performing banking services through internet or mobile banking, payment service providers are required to perform know your customer process before carry out an online payment. All of the payment service providers across the member states shall be subject to minimum security standard prescribed by Guidelines on Security of Internet Payment from August 2015.

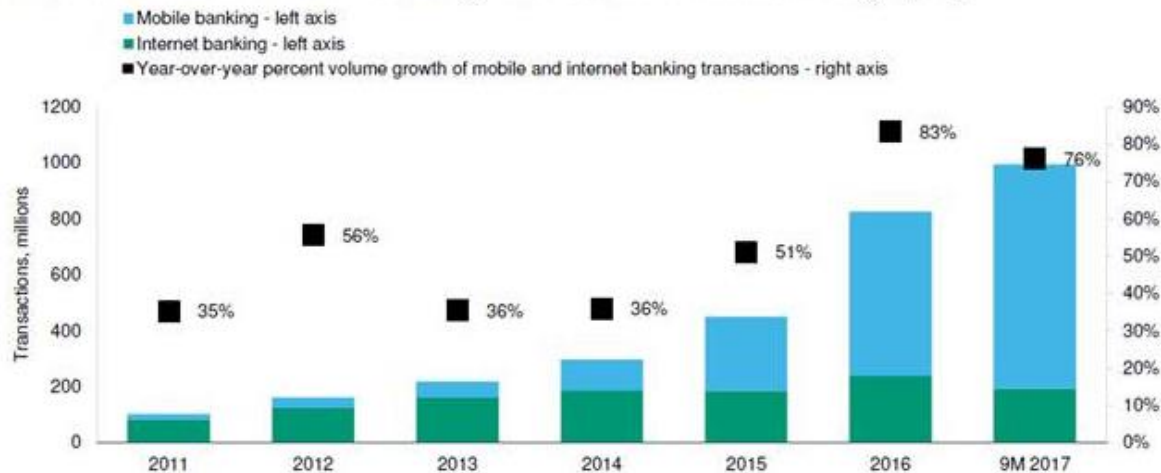
Regarding data privacy, the first regulation on data protection and security was EU directive on data protection 1995. With the blooming of the internet usage and digital era, General Data Protection Regulation (GDPR) which was promulgated in 2016 shall emphasize individuals’ right to control their own personal data as of 25 May 2018. The GDPR set out rules and requirements applied to data “controllers” (i.e. banks, fintechs)

and “processors” (i.e. third-party vendors, including mobile banking platforms, other service providers) across EU member states. The governing subject of GDPR has also been covered any business that may involve processing European citizens’ data even if such business have no physical presence in EU. According to GDPR, the controllers shall have to build products and services which set out data protection safeguards at the earliest stage of development. The controllers reserve the right to share the customers’ data to processors only after they have prior consent from customers by means of a statement or clear affirmative action. As required by GDPR, upon request of customer, data controllers should give their customers access to any of personal data in the course of data processing as well as transfer the data to any service providers following the direction of the customers. If any security gives rise to a risk to the European customers, data controllers shall have to notify a designated data protection authority within 72 hours and to the affected customers without undue delay. Any controllers or processors which are failure to perform GDPR obligations shall be subject to administrative fees which may be up to a maximum of EUR 20 million or 4 per cent of the global annual revenue – whichever is higher.

2.2. 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).

Thailand’s internet and mobile banking transaction volume is increasing rapidly



Source: Bank of Thailand

Fig. 1: Thailand’s internet and mobile banking transaction volume

Source: BOT (2017)

It can be seen from Fig. 1 that the volume of internet banking transactions increased slightly from the year 2011 to 2017. Besides, Thailand witnessed a significant rise in mobile banking transactions during the same period. 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.

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.

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.

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.

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.

2.3. 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 1: Top 5 Centers in GFCI 24

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

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).

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 (Eillen 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.

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.

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 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.

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.

2.4. South Korea

South Korea is well known for its technological advances with over 94% smartphone penetration according to a survey conducted by the US-based Pew Research Center (Sohn Ji-Young, 2018). Korea is also one of the first countries to have real digital banking. However, there are still hurdles Korea must overcome to promote the development of digital banking.

When foreign banks such as Citigroup and Standard Chartered launch their branches in Korea, two newly established online banks (K Bank, Kakao Bank) have attracted millions of customers to open their accounts.

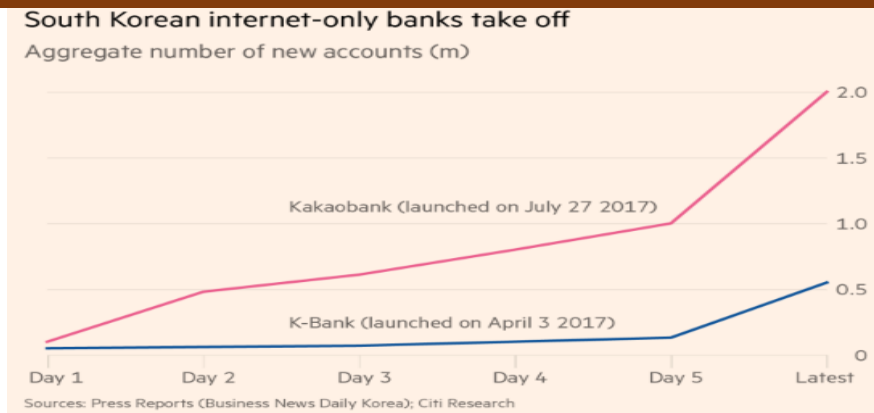


Fig. 2: South Korean Internet-only banks take off

Source: Press Reports (Business News Daily Korea) Citi Research (2017)

April 2017 marked the opening of the first digital bank in Korea. K Bank was the first bank in Korea to have no transaction points, no bank tellers, all banking operations such as account opening, money transfer or lending were conducted entirely by means of smartphones and internet.

At the same time, Kakao Bank of Daum Kakao, the owner of Kakao Talk, also launched its Kakao Talk application in July 2017. In the first month Kakao Bank attracted 3 million users, with deposits of up to 2 trillion won (\$ 1.78 billion) and loans of up to 1.8 trillion won (Yoon Yung Sil, 2017). Kakao Bank provides basic traditional banking services such as account opening, bank transfer, loans. Kakao's attractiveness comes from its easy-to-open account procedure, loans' low interest rates, savings deposits' high interest rates, and low transfer fees. In addition, Korea has extremely rapid growth in the number of people using the smartphone using 3G/4G. With such favorable conditions, the number of Kakao Bank's customer is expected to grow even further. Kakao Bank's customer identification process is quite different from that of traditional banks. Accordingly, customers do not need to have a face-to-face meeting with Kakao Bank staff when opening accounts such as traditional banks. In case the customer already has an account with another bank, the customer can choose to provide the account information to Kakao Bank, and then the bank will transfer a small amount of money (i.e. 1 won) to the account provided with the transfer content is the confirmation code. The customer will enter this confirmation code into the Kakao Bank phone application to complete the identification process. For customers who have never opened an account at any bank in Korea, customers can choose to make a video call to Kakao Bank employees after sending a copy of identification card via email or application to complete the identification process. Kakao Bank does not have to maintain physical trading offices with a large number of staff so Kakao can offer its customers anytime, anywhere, on a fast-paced platform, with competitive interest rates and fees compared to traditional bank rivals.

Regarding the Policy on finalizing infrastructure, the payment system in Korea consists of a large-value payment system (LVPS) and other retail payment systems (RPS). The LVPS system in Korea or Financial Wire Network (BOK-Wire+) is named after Bank of Korea. Retail payment systems are primarily managed by the Korea Financial Telecommunications & Clearings Institute (KFTC), which was established by the BOK and operates under the non-profit mechanism. Recent years have seen remarkable developments in the Korean payment system. With LVPS, BOK has added real-time money transfer features in 2009. With low-value payment systems, there is a remarkable development in credit card (with local card brands), electronic money (electronic wallet for carriage payments), prepaid tools and mobile banking services (using apps). KFTC has recently developed its 24/7 payment gateway, namely BankPay, to enable buyers to make payments to merchants, online shops through bank transfer. In April 2016, KFTC launched the Bank Wallet service that allows the use of smartphones to pay for small amounts of money between phone numbers (without a bank account) at convenience stores and online transactions.

The establishment of digital banks (K Bank or Kakao Bank) is relatively new in South Korea. The establishment will be reviewed by the Financial Supervisory Service on a case by case basis and according to market demand. All digital banking operations are still in compliance with the rules set for traditional banks.

Accordingly, the establishment, operations of banks is governed by several laws and regulations, including Bank of Korea Act 2016, Financial Investment Services and Capital Markets Act 2007, Electronic Financial Transaction Act 2006, Regulation on the Operation and Management of Payment and Settlement Systems 2001.

Two digital banks (K-Bank and Kakao Bank) are founded and operated under the same regulations as existing banks (i.e. traditional banks). Even so, the emergence of a full-scale bank like the two above mentioned banks has shown that the Korean government is actively promoting the development of digital banking in the country. Institutional support to promote sound competition between digital banks and traditional banks is said to be provided by the Korea financial authorities. In such context, consumers can have another choice when using banking service while the traditional banks held a monopoly in the past. Relevant laws and regulations is revised to facilitate activities of digital banking such as payment gateway system, debit card payment using a bank network, mobile remittance using smart phones, credit card, investment consulting, insurance, real-time Q&A responses provided by the Chat-bot service of machine learning and artificial intelligence; assessment of loan applications without submission of document using scraping techniques.

In Korea, there are 3 acts governing the protection of personal data. The first one is the Personal Information Protection Act (PIPA), which regulates collection, usage, disclosure and other processing (collectively, processing or process) of personal information by governmental and private entities. More exactly, all governmental agencies, legal entities, organizations and persons that process personal information in organized methods (the data handler, similar to the concept of the ‘controller’ under EU Directive No. 95/46/EC (General Data Protection Regulation) are subject to the PIPA. To process sensitive information or unique identification information, the data handler must obtain the data subject’s express consent separate from the consent to the processing of other personal information.

2.5. *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.

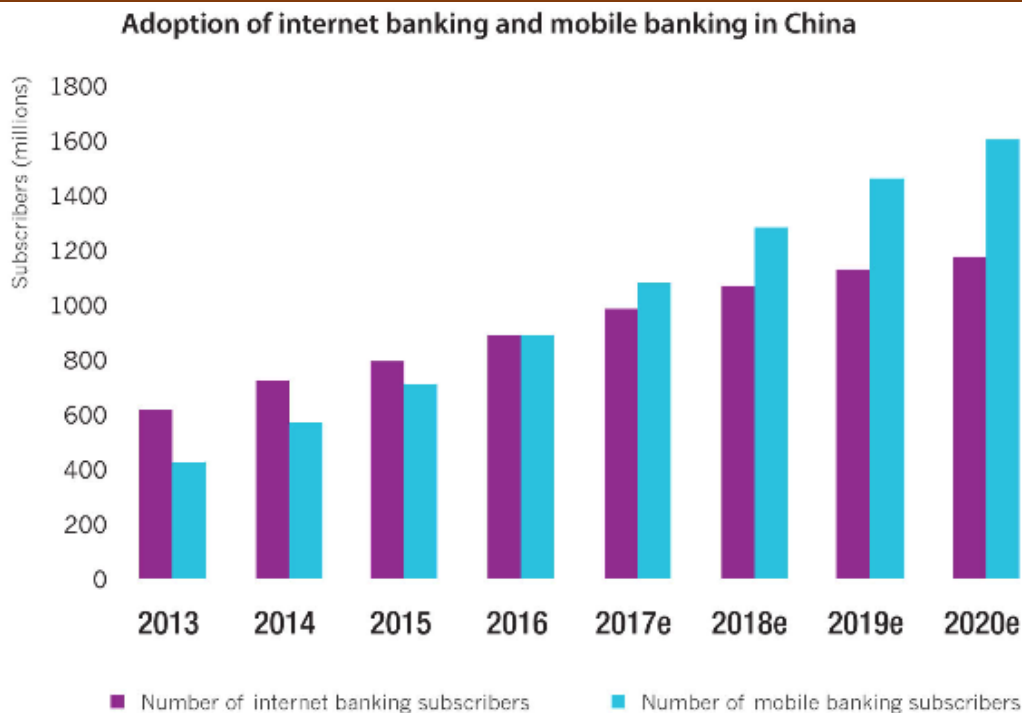


Chart 3: Adoption of internet banking and mobile banking in China

Source: Asian Banker Research (2017)

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.

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 manage 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.

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.

3. Experiences for Vietnam

As a very first step of the process between banks and customers in payment transactions, e-KYC and e-ID have been used by banks as mechanisms in digital platform to ensure effective and accurate identification and verification of customers. This identification and verification method has been applied in almost selected countries. Besides, setting up a limit on payment transactions' value is another fundamental mechanism which has been chosen by the governor of the selected countries in their digital banking law. In particular, any and all purchase agreement with total value of €1,000 or more must be carried out by electronic payment method in Italy – an EU Member States where the payment system in Korea consists of a large-value payment system (LVPS) and other retail payment systems (RPS).

In Vietnam, the Government and Payment Department under the State Bank of Vietnam is responsible for guidance as well as supervision on the legal regulations on digital payment transaction. Due to the habits of using cash in payment as well as limited knowledge of digital banking services, customers do not get used to digital banking payment system. Because of such gaps, the Government has issued the Plan on non-cash payment in Vietnam in the 2016-2020 period approved by the Prime Minister, by the end of 2020, the ratio of cash transactions should be reduced to below 10% in order to orient the state agencies as well as the commercial banks. Regarding the identification and verification method, the draft of the amended Decree No.116/2013/ND-CP dated 4 October 2013 of the Government detailing the implementation of a number of articles of the Law on money laundering prevention and control is being amended to enable banks to implement eKYC, eID to facilitate the provision of products and services to customers, minimizing unnecessary procedures. Besides, as the governor, the Payment Department under the State Bank of Vietnam has hold a number of workshops with the participant of commercial banks and experts from countries having successfully implemented the law on digital banking in term of payment system to train the Government and SBV's officers as well as enable commercial banks to learn experiences in providing the digital services, Vietnam has the opportunity to achieve the target of Plan on non-cash payment in Vietnam in the 2016-2020 period.

Innovations and new technologies shall obviously reduce the cost of providing specific services for the financial institution. However, it also give rise to greater financial risk including financial crises, higher banks' fragility; excessive credit expansion. As a result, the selected countries have paid attention to the regulatory sandboxes which enables live testing of new technologies by fintech under the strict supervision of the regulator.

In Vietnam, the State Bank of Vietnam is in the course of drafting legal framework on regulatory sandbox for fintech activities in Vietnam including several issues such as agency banks, crypto currencies, policies on banking operations. SBV in collaboration with the Asian Development Bank (ADB) and VinaCapital Ventures, organized a workshop on “International Experience in Fintech Regulatory Sandbox” on September 25, 2018 with the participation of relevant ministries and agencies in order to acquire in-depth understanding of the model of Fintech Regulatory Sandbox in other countries and the possibilities of application and formulation of a similar model in Vietnam. Thus, Vietnam should pay attention to the conditions for participant to participate in the regulatory sandbox as well as procedure to approve the test of the innovations. Besides, based on the innovation and new technologies compared with the risk management mechanism, SBV should consider to which risk appetite is acceptable, whether the participants shall comply with prevailing laws and regulations or may be exempted from some strict regulations.

Vietnam has witnessed significant growth in fintech companies. As of September 2018, there have been 78 institutions licensed by the SBV to provide online payment services, 41 institutions providing mobile payment solutions, 27 institutions providing payment intermediary services, and 12 banks implementing the QR Code payment services with 5000 points accepting QR Code payments (SBV, 2018). As a result, Vietnam has the ability to learn from international experience in legal framework and risk management from selected countries.

Peer-to-peer (P2P) business loans have grown rapidly in recent years in helping small and medium enterprises grow. The lessons learned from China's P2P lending fraud (Ezubao) will help regulators in Vietnam avoid making the same mistakes while preventing malpractices in the P2P industry. Regulators in selected countries (i.e. South Korea and China) have made a number of attempts in implementing multiple new policies and laws to control these risks arising out of the P2P lending. At the very first step of P2P lending process, e-KYC and anti-money laundering regulations should be a prerequisite condition. Accordingly, the identity of the borrower or investor must be verified by the P2P platforms by means of their passports, drivers' licenses, or a government-issued ID. E-KYC plays an important part in the success of P2P transactions due to the fact that P2P lending are carried out online and without direct face-to-face contact between the lenders and borrowers. In addition, several measures obligatory have been imposed on the lenders. For example, MAS requires that escrow accounts must be used by P2P lenders. 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.

In Vietnam, there are 40 P2P companies providing lending platform for investors and borrowers. However, the operation of a number of such service providers have been proved to violate the prevailing laws of Vietnam, including: providing inaccurate information related to risks; falsely advertising profits, lending at very high interest rates (i.e. exceeding the interest rate cap of 20 per cent per year). According to Deputy Prime Minister Vuong Dinh Hue, before officially promulgating a specific law governing the P2P lending transactions, the Government will soon issue a decision to allow a pilot implementation of peer-to-peer (P2P) lending in the country. Accordingly, P2P lending would be restricted to connecting lenders and borrowers during the pilot operation. P2P lending companies which are regarded as intermediaries to connect lenders and borrowers would not be allowed to mobilise capital from the credit institutions. At the same time, financial institutions will not be allowed to take part in P2P lending transaction during the trial operation. However, following the model in selected countries mentioned above, banks may participate in the P2P lending transaction as a custodian of customer funds in the near future. As the lesson learned from China's P2P lending

crisis, the Decision on P2P lending Pilot does not mean that Vietnam's regulators limit the development of the new lending method but a due and necessary step before the official law on P2P lending.

Contribution: Thi Thu Huyen Tran 65%, Thi Thanh Tan Pham 35% of job.

References:

- i. *ATKearney (2013) Banking in a Digital World, Available at <https://www.atkearney.com>*
- ii. *Citigroup (2018), Bank of the future, Available at <http://www.vostokemerging-finance.com/content/uploads/2017/05/Citi-GPS-Bank-of-the-Future.pdf>*
- iii. *Can Van Luc (2018), The success factor in digital banking transformation. State Bank of Vietnam: Banking Vietnam 2018. Hanoi, July 2018*
- iv. *Delloit (2018). EMEA Digital Banking Maturity 2018. Internal reports.*
- v. *Nguyen Van Chuong (2018). Current situation and solutions for developing digital banks in Vietnam. Financial Magazine July 7/2018.*
- vi. *IDRBT (2016). Digital Banking Framework. Institute for Development and Research in Banking Technology. Reserve Bank of India*
- vii. *Pham Tien Dung (2018). Development orientation of digital banking in Vietnam. Paper presented Banking Digitizing Workshop - Breakthrough Opportunities, SBV, November 2018.*
- viii. *Pham Thi Bich Lien, Tran Thi Binh Nguyen (2018). Developing digital banking for Vietnamese commercial banks, National Economics University: Industrial Revolution 4.0 and innovations in the field of finance and banking (pages 72-86). Hanoi, June 2018*
- ix. *Le Nhan Tam (2018). Reproducing numbers and views of IBM Paper presented Banking Digitizing Workshop - Breakthrough Opportunities, SBV, November 2018.*
- x. *Le Cong and Dam Nhan Duc (2016), Digital banking trends and mobile banking initiatives: international experience, current situation and recommendations for the Vietnamese banking system. State Bank of Vietnam: Banking Vietnam 2016 (pages 274-285). Hanoi, May 2016.*
- xi. *LBP Research. (2018, January 25). India's experience in digital banking management and development. Retrieved from research.lienvietpostbank.com.vn*
- xii. *VP Bank (2017). What is digital banking? There is like internet banking. Access at <https://timo.vn/blog/thu-vien-timo/digital-banking-la-gi-co-giong-internet-banking/>*
- xiii. *Vu Hong Thanh (2016). Digital banking - A new development direction for commercial banks in Vietnam. Banking Journal, 21, 32-40.*