Washington University
Global Studies Law Review

VOLUME 20 NUMBER 1 2021

THE DEVELOPMENT AND REGULATION OF MOBILE PAYMENT: CHINESE EXPERIENCES AND COMPARATIVE PERSPECTIVES

ROBIN HUI HUANG* ABBY OI LING LAMξ
ANTHEA WING TING YUψ CHRISTINE MENGLU WANGθ

ABSTRACT

China has become one of the leaders in the global mobile payment market in terms of market volume, growth rate, and innovation capability. This can be attributed to a number of enabling factors, including technological advancement in China and mobile payment's competitive advantages and wide acceptance by Chinese people. Mobile payment brings significant benefits as well as various risks and thus should be regulated in a way that reaps its benefits while containing those risks. This article critically examines China's regulatory regime for mobile payment, focusing on several key elements such as the entry and exit mechanism, management of customer reserves, anti-money laundering measures, and consumer

* Professor, Faculty of Law, Chinese University of Hong Kong; Adjunct Professor, University of New South Wales, Sydney Australia; Li Kashing Visiting Professor, McGill Law School, Montreal Canada; Honorary Professor, East China University of Political Science and Law, Shanghai, China. This research project (Project Number: 14613219) is funded by the Hong Kong Research Grants Council's General Research Fund project "The Regulation of Fintech in China.' We are grateful for the valuable comments on an earlier draft of this paper from the participants in the online symposiums at Renmin University and Chinese University of Hong Kong. Thanks also to those people who took time to participate in the interview exercise we conducted for this research project.

ξ Faculty of Law, Chinese University of Hong Kong.
ψ Faculty of Law, Chinese University of Hong Kong.
θ Faculty of Law, Chinese University of Hong Kong.

protection. A comparative study is also conducted on the regulation of mobile payment in several major jurisdictions, including the US, the UK, Singapore, and Hong Kong. Then, this article analyses the strengths and shortcomings of the regulation in China and, based on international experiences, makes relevant suggestions for improvement. China is advised to enact a unified law specifically for mobile payment and adopt a more nuanced risk-based approach in setting out regulatory requirements. There is a need to address the negative effects on competition in the mobile payment market that may be exacerbated by the high entry threshold and the centralized clearing mechanism. China should also streamline the enforcement aspect of its regulatory regime and pay particular attention to important issues of consumer protection such as data protection.

Keywords: *mobile payment, Fintech, consumer protection, China, comparative study*

I. INTRODUCTION

The last decade witnessed a profound change in the payment landscape, with the wide-spread use of mobile payment having significantly transformed our lives and habits. Although mobile payment did not originate in China, China has successfully placed itself at the forefront of the global market in terms of the scale and market volume. According to PricewaterhouseCoopers' Global Consumer Insight Survey 2019,[1] the penetration rate of mobile payment in China is 86%, while the global penetration rate stands at 34%. Mobile payments can be seen in use in almost every corner of China, accepted by both humble street vendors and luxury brand stores. Even beggars accept mobile payment by displaying a QR-code printed on cardboard to pedestrians.[2]

Probably due to the rapidly evolving nature of the mobile payment industry, however, there is today no universal definition of what exactly constitutes a mobile payment. The European Commission offers one useful definition, under which mobile payments refer to "payments for which the payment data and the payment instruction are initiated, transmitted, or confirmed via a mobile phone or device. This can apply to online or offline purchases of services, digital or physical goods."[3] Despite the large variety of forms a mobile payment may take, its essential function is to resolve the lack of trust between payors (such as consumers) and payees (such as merchants) by having the payment platform serve as an intermediary between them. The sum given by the consumer payor for the goods would be first forwarded to the payment platform and would only be transferred to the merchant payee when the transaction has been completed and confirmed by the payors.[4]

From the perspective of financial innovation and regulatory challenges, mobile payment is very different from online banking and thus both forms should be distinguished. Online banking is essentially "old wine in a new bottle," insofar as it provides traditional banking services through internet-

---

1 *It's time for a consumer-centred metric: introducing 'return on experience': Global Consumer Insights Survey 2019*, PRICEWATERHOUSECOOPERS (2019), https://www.pwc.com/gx/en/consumer-markets/consumer-insights-survey/2019/report.pdf.

2 Prachi Gupta, *Beggars with QR code: Chinese poor collect alms in mobile wallets, ditch tin bowls*, FIN. EXPRESS (July 12, 2019, 3:36 PM), https://www.financialexpress.com/industry/beggars-with-qr-code-chinese-poor-collect-alms-in-mobile-wallets-ditch-tin-bowls/1641567/.

3 *Commission Green Paper Towards an Integrated European Market for Card, Internet and Mobile Payments*, at 5, COM (2011) 941 final (Nov. 1, 2012), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52011DC0941.

4 James Schneider et al., *The Rise of China FinTech—Payment: The Ecosystem Gateway*, GOLDMAN SACHS 30 (Aug. 7, 2017), https://hybg.cebnet.com.cn/upload/gaoshengfintech.pdf.

based channels. Third-party mobile payment, on the other hand, represents an innovative and potentially disruptive financial services. Moreover, while banks have long been subject to the conventionally well-established supervisory system,[5] the emerging third-party mobile payment service providers, mainly tech firms, present new regulatory challenges. Hence, this paper will focus on the issue of third-party (non-bank) mobile payment.

The rapid development of mobile payment can be largely attributed to the significant advantages it possesses vis-à-vis the traditional payment.[6] Consumers can enjoy the convenience and speed of a cashless society, no longer restricted by geographical factors when transferring money or paying for goods. Merchants, on the other hand, can reduce their transaction costs and attract more consumers via a mobile payment platform. Meanwhile, the development of mobile payment has brought a range of legal, regulatory, and risk-management challenges, such as fund security, cybersecurity, and privacy issues.[7] Regulators are facing unprecedented difficulties as products and services related to mobile payment are increasingly complex and interdependent. It is not an easy task for regulators to balance multiple competing interests, such as financial stability, technological innovations, and consumer rights. Onerous regulations may stifle innovation and impede the growth of the industry, while loose regulations may leave consumers unprotected.

Following this introduction, Part II will first briefly introduce the current mobile payment market and then explore the key enablers that contribute to the success of mobile payment in China. It will also discuss the various risks inherent in mobile payment, risks that call for regulatory attention. Part III will give an overview of the current regulatory regime in China, focusing on four aspects: the entry threshold and exit mechanism, restrictions on the management of consumer funds, crackdown measures on financial crimes (primarily for Anti-money Laundering), and consumer protection (data security and the liability distribution upon the unauthorized payment). Although China has in many ways led the world in the

5 In general, there are three-tiered regulations over banking in China, including the legislation on banking enacted by the National People's Congress, the administrative rules and regulations enacted by the State Council, and the guidelines, notices and rules issued by the PBOC and the China Banking Insurance Regulatory Commission (the merged regulator of China's banking and insurance sectors). For further details, see Dongyue Chen & Yixin Huang, *Banking Regulation 2020 China*, *in* BANKING REGULATION 2020 (Peter Hsu & Rashid Bahir eds., 7th ed. 2020), https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/china#chaptercontent3 (last visited Sep. 19, 2020),

6 For a more detailed discussion, see *infra* Part II.B.

7 For a more detailed discussion, see *infra* Part II.C.

development of its mobile payment infrastructure, it is of crucial importance to look to the experiences of other jurisdictions, given that speed and scale do not necessarily entail quality and sustainability in the payment system. Part IV will thus examine regulations affecting mobile payment in four other jurisdictions: the US, the UK, Singapore, and Hong Kong. This is followed by Part V, which will evaluate the Chinese law from a comparative perspective, pointing out its strengths and weaknesses, as well as making suggestions for improvement. The last part will provide a unifying conclusion.

II. BACKGROUND: THE MARKET, ENABLERS, AND RISKS

A. The Market and Typology of Mobile Payment

In recent years, markets around the world have embraced the unstoppable global trend towards mobile payment. The global mobile payment market was worth USD 368 billion in 2017. Over the next two years, it surpassed USD 745.7 billion.[8] As a global frontrunner in this area, China has the biggest mobile payment market, accounting for almost half of the world.[9] In 2017, approximately 65% of all mobile users in China used their mobile phones as their wallets. Around RMB 38 trillion was spent through mobile payment in 2016.[10] According to the data of the People's Bank of China (PBOC), the Chinese central bank, China saw 101.43 billion mobile payment transactions in 2019, with a total value of RMB 347.11 trillion.[11] The US mobile payment market, although showing an incremental growth, is 6 times smaller than that of China.[12] Alipay, a Chinese mobile payment platform associated with the e-commerce giant Alibaba group, is the world's biggest mobile payment platform now with

---

8 Alex Rolfe, *Global Mobile Wallet Market Value Set to Reach $1 Trillion in 2020*, PAYMENTS CARDS & MOBILE (Feb 26, 2020), https://www.paymentscardsandmobile.com/global-mobile-wallet-market-value-set-to-reach-1-trillion-in 2020/#:~:text=According%20to%20new%20data%2C%20the,market%20reaching%20%242.1%20trillion%20value.

9 *The Age of the Appacus: In Fintech, China Shows the Way*, ECONOMIST (Feb. 25, 2017), https://www.economist.com/finance-and-economics/2017/02/25/in-fintech-china-shows-the-way.

10 *Id.*

11 *Online Payments Transactions Processed by Chinese Banks Rise 37.14% YoY in 2019, Mobile Payments up 67.57%*, CHINA BANKING NEWS (Mar. 19, 2020), https://www.chinabankingnews.com/2020/03/19/chinas-online-payments-transactions-rise-37-14-yoy-in-2019-mobile-payments-up-67-57/.

12 *Amazing Stats Demonstrating The Unstoppable Rise of Mobile Payments Globally*, MERCH. SAVVY, https://www.merchantsavvy.co.uk/mobile-payment-stats-trends (updated Feb. 2020).

over 1.2 billion active users.[13]

In general, mobile payment can be classified into two broad categories, namely: (1) remote mobile payment and (2) proximity payment. Each category can be further divided into several subgroups based on the technologies involved.

Remote mobile payment can be made through premium short message service (SMS) or the Internet. SMS payment is the simplest method of mobile payment. Consumers are required to create an account with a mobile network operator to link their accounts to their bank accounts.[14] To make a mobile payment, SMS messages are sent between users and the mobile network operator to provide transaction details; once the user verifies the payment by entering his password, the mobile network operator will transfer the funds from payor to payee.[15] Although this method is somewhat simpler than the other payment methods discussed below, SMS can suffer from transmission delays between users and mobile network operators, and even potential transmission failures,[16] which hampers the use of SMS mobile payment in the global markets.

Remote mobile payment can also be made through the Internet, namely the Wireless Application Protocol (WAP).[17] The WAP is a technical standard used in wireless devices for accessing and transmitting information over a mobile wireless network. In WAP mobile payment, mobile applications are created by financial institutions; the various players in mobile payment, such as merchants, third-party mobile payment service providers, and consumers, are all linked to these mobile applications.[18] In China, the most-used WAP mobile payment applications include AliPay and Tenpay.[19]

---

13 *Id.*

14 Menna Aharam Rajan, *The Future of Wallets: A Look at the Privacy Implications of Mobile Payments*, 20 COMMLAW CONSPECTUS 445, 448 (2012).

15 *Id.*

16 *Id.* at 450–51.

17 Tanai Khiaonarong, *Oversight Issues in Mobile Payments* 7–8 (Int'l Monetary Fund, Working Paper No. 14/123, 2014), https://www.imf.org/external/pubs/ft/wp/2014/wp14123.pdf.

18 Timothy R. McTaggart & David W. Freese, *Regulation of Mobile Payments*, 127 BANKING L.J. 485, 488 (2010).

19 Alipay was launched in 2004 by Alibaba Group to support online payment. It is run by Ant Financial Services Group, an affiliate company of the Chinese Alibaba Group. Alipay took off mainly due to its tight link to the online shopping platform, Taobao. However, Alipay did not stand still as a mere payment method, the core value of which is being part of the Alibaba ecosystem. It has introduced a wide range of services on its platform, including financial, leisure, and transportation services, in order to meet the users' daily life needs. Data from IResearch Consulting Group shows that it retains its

Proximity payment, also called 'mobile point of sale payment,' involves the use of mobile phones to pay for goods in shops: the retailer uses a piece of hardware that can interact with the hardware in consumers' mobile phones.[20] Currently, Near Field Communications (NFC) and Quick Response Code (QR code) are the most common technologies used in proximity payment.

The NFC is a "wireless protocol which allows for an encrypted exchange of payment and other data at a close range."[21] NFC hardware, embedded in the customer's mobile phone by its manufacturer, is scanned by the retailer's NFC reader installed at the point of sale. The NFC reader scans the consumer's payment account credentials when he taps or swipes his mobile phone on the reader.[22] Typically, NFC technology is used alongside some forms of mobile wallets, either prepaid cards or accounts that are saved in a mobile application. The NFC uses a "secure element" to record consumers' payment credentials on their mobile phones for access to retail shops.[23] NFC technology is considered to be the predominant mobile payment method adopted in the global market; it is used as a primary technology in Apple Pay, Samsung Pay, and Google Pay.[24]

The QR code was originally developed as a "mobile advertising tool" but has now extended to the use of mobile payment.[25] The QR code is a two-dimensional barcode where information or credentials may be encrypted; the QR code can be read by barcode or QR code readers. The

---

leadership with a market share of over 50%. IResearch, 2020Q1&Q2中国第三方支付市场数据发布报告[*China's Third-Party Payment Industry Report for the First Two Quarters*], IRESEARCH (2021), https://www.iresearch.com.cn/Detail/report?id=3601&isfree=0.

Tenpay, owned by Tencent, includes WeChat Pay and Mobile QQ Wallet, both of which are incorporated into one of the most common social media platforms in China. It launched a new product named "Red Envelope", allowing the user to give lucky money or red packets to close friends, which has successfully won popularity. Leveraging its large user network, it is a formidable competitor of Alipay in China, with a market share of around 38.9%. *Id.*

20 Chris Hill, *Mobile Payments: Technological, Contractual and Regulatory Convergence*, KEMP LITTLE ANN. UPDATE 1, 3 (Jan. 2017), https://www.kemplittle.com/wp-content/uploads/2018/12/Mobile-payments-January-2017.pdf.

21 Robert C. Drozdowski, Matthew W.Homer, Elizabeth A. Khalil & Jeffrey M. Kopchik, *Mobile Payments: An Evolving Landscape*, FED. DEPOSIT INS. CORP. (2012), https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/mobile.html.

22 Erin Fonte, *2017 U.S. Regulatory Overview of Mobile Wallets and Mobile Payments*, 17 WAKE FOREST J. BUS. & INTELL. PROP. L. 549, 559 (2017).

23 *Id.*

24 Chelsea Allison, *How Does NFC Payment Work?*, FIN (Feb, 20, 2017), https://fin.plaid.com/articles/how-does-nfc-payment-work/.

25 L. Barbero, P. Caprara, M. Infantino & S. Mancini, *Mobile proximity payment: 5 things retailers should know*, PRICEWATERHOUSECOOPERS 1, 3 (2016), https://www.pwc.com/it/it/publications/assets/docs/mobile-proximity.pdf.

use of QR codes may sometimes require the use of another type of mobile payment technology, cloud-based technology. Credentials are stored in the cloud and controlled by a third party rather than on the mobile phone itself. Using cloud-based technology, static QR codes may be used and stored in the user's mobile device. "Dynamic QR codes" are unique codes for each transaction but are linked to the user's same payment account and can be used through cloud-based technology.[26] Since QR codes can be printed and read by mobile phones instead of special devices installed at the point of sale, QR code technology is sometimes classified as remote mobile payment.[27]

Although mobile payment can be classified into different categories and different technologies can be used, these categories are not mutually exclusive and can be used by the same user or in one mobile application. For example, Apple Pay includes both remote and proximity mobile payment options, and an NFC mobile payment option is available for Apple mobile phones with NFC chips installed.[28] In short, all mobile payments discussed above contain four basic elements: (1) a handset, which can be a mobile phone or a device to read codes; (2) an account having the user's funds; (3) a means to communicate the user's request to transfer funds; and (4) a channel which connects the user's (payor's) account to the payee's account. [29]

B. The Key Enablers

Mobile payment did not originate in China, but it did take off in China's market. There are several drivers behind its rapid development, including technological advancement leading to the wide availability of accessible Internet and affordable smartphones, the wide acceptance of mobile payment by Chinese consumers, and competitive advantages of mobile payment vis-a-vis the traditional payment.

---

26 Fonte, *supra* note 22, at 560–61.
27 Barbero et al., *supra* note 25, at 3.
28 *Id.* at 9.
29 Hill, *supra* note 20, at 3.

1. Technological Advancement

With wide coverage of the Internet (around 54.6%) and high smartphone penetration (up to 56%),[30] Chinese payment service providers tried all means to render mobile payment as the first option for consumers in transferring money or paying for goods. For example, Tenpay introduced "red packet," a money transfer function that immediately went viral among Chinese users, including the elderly. Giving physical red envelopes to the younger generation during holidays or special occasions is a traditional Chinese custom. According to Tenpay's official report, around 823 million people during the 2019 Chinese Lunar New Year sent or received digital red envelopes via the WeChat platform.[31]

The use of QR codes in China has also drastically enhanced user experiences. No special equipment is needed, only software. Merchants, particularly small stores, are more willing to support QR codes in lieu of the credit card payment, given that installing the POS (point of sales) machines to support credit card payment is costly. It is much easier for merchants to keep payment records, which serve as reliable supporting documents when it comes to applying for bank loans and even initial public offerings on the securities market. Consumers also gain in convenience as payment is completed with a few taps on a mobile device. This is particularly true in the supermarket, where self-checkout has become more popular.[32]

Additionally, compared to US mobile platforms that focus more on their payment business, the majority of the Chinese mobile payment platforms offer full-service lifestyle functions. Alipay, for example, apart from being a payment channel for shopping in-store and online, is integrated with a wide spectrum of financial services, e-commerce, leisure, and travel services. The users can make financial investments, buy insurance, order food, book tickets, hail taxis, and so on.

---

30 *E-commerce Payments Trends: China*, J.P. MORGAN GLOB. PAYMENT TRENDS (2019), https://www.jpmorgan.com/merchant-services/insights/reports/china.

31 *WeChat Releases 2019 Spring Festival Data Report: 823 Million People Receive and Send Red Envelopes*, CNR NEWS (Feb. 11, 2019), https://copyfuture.com/blogs-details/202004110201030 64hr7o8bxglzn4g2t.

32 Fumiko Hayashi & Terri Bradford, *Mobile Payments: Merchants' Perspectives*, 98 ECON. REV. 33, 44 (2014).

2. *The Wide Acceptance by the Local Consumer*

While other countries have switched from cash to credit cards and are now switching to mobile payment, China's ability to skip the second step, namely the absence of a habit of using credit cards in daily consumption, has allowed it to go straight from cash to mobile payment.[33]

In addition, Chinese people are arguably less concerned with or sensitive about privacy issues than Westerners for various reasons, such as a Confucian cultural traditions and the prevalent pragmaticism adopted in the recent economic reform era.[34] Given that data privacy is one of the most serious risks of mobile payment, it is much easier for mobile payment to gain popularity in China than in Western jurisdictions.[35]

Also, one striking feature of mobile payment in China is that payment institutions can leverage their sizable customer bases in e-commerce or social media networks. This is well illustrated by some major players in the mobile payment industry, including Alipay (supported by its sister platform Taobao), Tenpay (relied on its popular social platform WeChat), JD Lingqianbao (linked with JD E-Commence platform), and Ping An's Yiqian Bao (backed up by its insurance business). This is a critical point, as one of the major difficulties in developing mobile payment is that not many people are willing to take a remote transaction without face-to-face verification, nor do they often wish to transfer money to a virtual account.[36] The third-party platforms have successfully resolved the distrust between consumers and merchants as the users have established trust on the platforms beforehand.

---

33 *The Mobile Payment Revolution in China*, ASIA PACIFIC FOUNDATION OF CANADA 1, 14, https://www.asiapacific.ca/sites/default/files/publication-pdf/mobile_payment_report.pdf.

34 *In China, Consumers Are Becoming More Anxious About Data Privacy*, ECONOMIST (Jan. 25, 2018), https://www.economist.com/china/2018/01/25/in-china-consumers-are-becoming-more-anxious-about-data-privacy. Based on our own experiences and interviews with others, there may be another reason behind the phenomenon: many Chinese people believe that the data privacy issue in China is so serious that their personal data might have already been, or would inevitably be leaked out, and thus it is not really meaningful to care about data privacy only in the context of mobile payment. Interview with two mobile payment users in Beijing, Shanghai, and Shenzhen (Sep. 18, 2020).

35 For a more detailed discussion of the data privacy issue of mobile payment, see Robin Hui Huang, Protecting Data Privacy for Mobile Payment under the Chinese Law: Comparative Perspectives and Reform Suggestions (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3767317.

36 Torben Hansen, *Understanding Trust in Financial Services: The Influence of Financial Healthiness, Knowledge, and Satisfaction*, 15 J. SERVS. RSCH. 280 (2012).

3. *Competitive Advantages over Traditional Payment Services*

There has long been a serious mismatch between consumers' high demands for payment services and banks' short supplies of such services in China. Mobile payment does not require the expensive infrastructure and buildings that traditional banks entail, and can help resolve the long-term shortage of financial services in rural areas. More generally, it offers a good alternative to unsatisfactory banking services, particularly for small consumers, as they may not be as valued by the bank as big clients are.[37] Hence, mobile payment operators have seized such an opportunity to provide convenient payment services under the rubric of an "inclusive financial system".

As noted earlier, China's mobile payment platforms are usually associated with existing business giants, which affords them the leverage required to gain the trust of consumers. Through sharing the consumer data, such as consumer patterns of behavior and preference, with their associated business, the payment service platforms can provide more targeted services to suit the needs of individual consumers.[38] In turn, this can generate more nuanced data on the consumers' creditworthiness than can traditional banking.[39] It shall be noted that in the eyes of the platform operators, mobile payment is the means and not the end, given that the profit made directly from the payment service is thin in China due to the low fees charged under fierce competition.[40] Hence, what providers are actually trying to do is to build a financial ecosystem via the gateway of the payment service.[41] The data on consumers' creditworthiness that are generated from payment services can be used for profitable consumer finance businesses.

For example, apart from payment services, Ant Group, the owner of Alipay, provides the so-called CreditTech services, including a consumer credit service called *huabei* and a consumer loan service called *jiebei*, as well as the so-called InsureTech business.[42] Further, a wealth management product called "Yu'e Bao" was introduced with Alipay acting as a conduit for consumers to invest the money left in their Alipay accounts; because it offers much better returns than the bank's savings account while having the

---

37 Dirk A. Zetsche, Ross P. Buckley, Douglass W. Arner & Janos Nathan Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, 14 N.Y.U. J. L. & BUS. 393 (2017).

38 *Id.*

39 Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data,* 18 YALE J. L. & TECH. 148 (2016).

40 Schneider et al., *supra* note 4.

41 *Id.*

42 ANT GROUP, H SHARE IPO PROSPECTUS 182 (2020), https://www1.hkexnews.hk/listedco/listconews/sehk/2020/1026/2020102600165.pdf.

same flexibility of withdrawals as the latter, it quickly gained huge popularity and became the largest money market fund in the world just four years after its introduction, surpassing JP Morgan's US government money market fund with USD 150 billion under management.[43] In recent years, the contribution of payment services to the total profit of Ant Group has been decreasing while the proportion of other Fintech platform services has been increasing. For instance, in 2017, payment services accounted for 54.9% of total profits (44.3% of total profits were from other Fintech platform services), but in the first half of 2020, the profit contribution of payment services reduced to 35.9% (the proportion of other Fintech platform services in the total profits increased to 63.4%).[44]

It is also important to note that the rapid development of mobile payment in China can be partly attributed to the issue of regulatory arbitrage. Mobile payment platforms are treated as non-financial institutions and thus are not subject to the costly banking regulation, despite the fact that they compete with banks in offering financial services. Indeed, at the initial stage of development of mobile payment in China, the third-party platforms were effectively operating in a legal vacuum, gaining competitive advantages over the traditional payment institutions in terms of regulatory burden. As the mobile payment industry grew and many problems emerged, China has since 2010 started to tighten its regulation of mobile payment by gradually introducing an array of relevant regulations and rules, as well as strengthening law enforcement.[45] In short, the initial light-touch regulatory approach was important for the take-off of the mobile payment industry in China, reflecting the policy support of the Chinese authorities for the concept of financial inclusion.[46]

---

43 Louise Lucas, *Chinese Money Market Fund Becomes World's Biggest,* FIN. TIMES (Apr. 26, 2017), https://www.ft.com/content/28d4e100-2a6d-11e7-bc4b-5528796fe35c.

44 ANT GROUP, *supra* note 42, at 316.

45 In October 2020, Jack Ma, the founder of Alibaba Group and its online finance affiliate, Ant Group, openly blasted China's regulators for stifling innovation in a forum, which led to the dramatic suspension of the planned record-breaking IPO of Ant Group. Julie Zhu, Kane Wu & Cheng Leng, *China launches antitrust probe into tech giant Alibaba,* REUTERS, Dec. 23, 2020, https://www.reuters.com/article/us-china-antgroup/china-launches-antitrust-probe-into-tech-giant-alibaba-idUSKBN28Y05T. On December 24, 2021, Chinese regulators launched an anti-monopoly investigation into Alibaba and summoned Ant Group to meet. An unnamed regulator reportedly stated that "Chinese internet firms had enjoyed unprecedented growth with light regulation for years . . . . The latest regulatory moves against them have sent out a clear message that the golden time for many of them has ended." *Id.*

46 Peter Sparreboom & Eric Duflos, *Financial Inclusion in the People's Republic of China: An Analysis of Existing Research and Public Data* 1–45 (WBG, Working Paper No. 75149, 2012), http://documents1.worldbank.org/curated/en/677591468025160550/pdf/75149020120CGA0Box03743 07B00PUBLIC0.pdf.

C. Risks of Mobile Payment

While mobile payment brings many important benefits to our society, there are serious risks associated with it, risks that call for regulatory attention. Indeed, the goal of our regulatory regime is to encourage the development of mobile payment in a beneficial way while controlling the attendant risks. It is thus necessary to examine the risks of mobile payment.

1. Unauthorized Transactions and Fraud

"Unauthorized electronic fund transfer" is defined as "electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit."[47] The degree of data security provided by a mobile payment application is closely related to the issue of unauthorized transactions and fraud. If a weak authentication system is adopted by a mobile payment application, fraudsters may easily enter into the user's account by hacking and conduct unauthorized transactions resulting in financial loss.

Unauthorized transactions have been one of the major concerns regarding mobile payment, with cases of unauthorized transactions reported in different regions in recent years. In 2017, it was reported in Guangdong province in China that around RMB 90 million was stolen through QR code scams; also, a man was arrested for stealing RMB 900,000 in the city of Foshan by replacing merchants' QR codes with fake ones which contained malware to steal consumers' personal information.[48]

Compared to traditional payment, the risk of unauthorized transactions is more serious and harder to address in the context of mobile payment. When unauthorized transactions occur, it is necessary to determine which party should be responsible for the fault and whether the user will bear the whole financial loss.[49] Since mobile payment involves multiple players including banks, mobile network operators, and third party agents, and transactions are conducted quickly with information stored

---

47 Electronic Fund Transfer Act, 15 U.S.C. § 1693(a).

48 Li Tao, *QR Code Scams Rise in China, Putting E-Payment Security in Spotlight*, S. CHINA MORNING POST (Mar. 21, 2017), https://www.scmp.com/business/china-business/article/2080841/rise-qr-code-scams-china-puts-online-payment-security.

49 Rhys Bollen, *Recent Developments in Mobile Banking and Payments*, 24 J. INT'L BANKING L. & REGUL. 454, 466–67 (2009).

in digital form in different players' systems,[50] it is difficult to trace where the problem occurred, and it can be only more difficult to determine which player is liable for the loss. Moreover, when a consumer complains that an unauthorized payment is made from his account, he may have difficulty in providing any proof because most of the data is held by mobile network operators and third-party mobile payment service providers, but not the user.[51]

Also, when an unauthorized transaction is detected, coordination among the parties in the mobile payment system plays an important role in stopping further unauthorized transactions. However, since multiple parties are involved and each of them may have different communication mechanisms and agreements with other parties, the party who detects the problem may not simultaneously notify other parties about the problem and the informed party may not take any precautionary measures to minimize the loss suffered by the users. For example, if a user loses his phone, he may try to report the loss to his mobile network operator, but the mobile network operator may not relay the message to third-party mobile payment service providers.[52]

2. *Money Laundering and Terrorist Financing*

From the perspectives of anti-money laundering (AML) and counter-financing of terrorism (CFT), mobile payment may be useful in reducing the use of cash from unknown sources, because mobile payment transactions are more traceable than traditional cash-based transactions.[53] Also, restrictions and monitoring policies can be imposed on mobile payment to make it more difficult to conduct money laundering or other illicit activities than with traditional payment methods.[54] Yet, the complexity of mobile payment and the involvement of more parties in the system provide opportunities for fraudsters or terrorists to conduct money laundering activities and terrorist financing.[55]

Similar to unauthorized transactions, money launderers and

---

50 Khiaonarong, *supra* note 17, at 6.

51 Yongqing Yang, Yong Liu, Hongxiu Li & Benhai Yu, *Understanding Perceived Risks in Mobile Payment Acceptance*, 115 INDUS. MGMT. DATA SYS. 253, 258 (2015).

52 *Id.*

53 Khiaonarong, *supra* note 17, at 17.

54 *Id.*

55 *Id.*

terrorism financiers can gain access to users' accounts by stealing mobile phones with inadequate security settings, by phishing to obtain mobile payment users' financial account information, or by hacking the mobile payment application.[56] Money launderers and terrorism financiers may then create fake transactions to transfer dirty money to a mobile payment platform and subsequently transform the dirty money into funds with an apparently legal source. For example, they may use dirty money to purchase weapons in online games and then sell those online items to earn a profit.[57]

Again, compared to traditional payment, mobile payment could be more vulnerable to money laundering and terrorism financing because of an absence of face-to-face meetings and insufficient consumer identity verification during mobile payment service registrations.[58] Also, mobile payment usually involves non-bank institutions and other players that the traditional payment system lacks. These new parties may not be regulated at all or may be regulated at a lower level than banking institutions; this may lead to insufficient "recordkeeping, screening and reporting" mechanisms to monitor money laundering, terrorism financing, and other illicit activities.[59]

3. *Data Security and Privacy Issues*

Since mobile payment involves many players and each player may require different information, a large amount of data is collected and held by different parties.[60] In a mobile payment transaction, some or even all of the players may have access to user information such as name, age, gender, identification number, bank account passwords, and so on. Notably, mobile payment also allows different players, especially mobile application providers, to collect information about users' purchasing habits which could not be easily obtained in traditional payment.

As mobile payment usually involves large amounts of data collection, it attracts fraudsters hoping to hack into the system to get

---

56 Erin Fonte, *Mobile Payments in the United States: How Disintermediation May Affect Delivery of Payment Functions, Financial Inclusion and Anti-Money Laundering Issues*, 8 WASH. J. L. TECH. & ARTS 419, 437–38 (2013).

57 James Whisker & Mark Eshwar Lokanan, *Anti-Money Laundering and Counter-Terrorist Financing Threats Posed by Mobile Money*, 22 J. MONEY LAUNDERING CONTROL 158, 160–61 (2019).

58 Khiaonarong, *supra* note 17, at 17.

59 *Id.*

60 For a more detailed discussion, see Huang et al., *supra* note 35.

data. For example, in the WAP form of mobile payment, the wireless network may be insecure, allowing malware to be secretly downloaded to a mobile phone without the owner's knowledge; as for NFC mobile payments, hackers may be able to steal user's information using an NFC reader when the mobile phone and the reader are in close distance.[61] Interestingly, according to the European Parliament, about 15% of cyber-attacks that gain access to corporate networks are done by damaging physical equipment such as storage devices, routers, and servers.[62] In 2015, it was estimated that consumers' information was stolen from around 200 online stores and payment platforms in China.[63] According to a study conducted by the U.S. Federal Reserve, 42% of consumers were concerned about data protection, and data security was the main reason why consumers did not prefer to use mobile payment.[64]

4. Operational Mistakes and Misconduct

In the ordinary course of their business, mobile payment platforms may make operational mistakes and even commit misconduct, including payment errors and misappropriation of client funds.

Payment errors, such as payment delay, overpayment, and transfer of funds to a wrong payee, may occur. These errors can be caused by user error such as entry of incorrect payee details, an incorrect payment amount, or pressing the wrong button resulting in incomplete transactions. Payment errors may also result from system errors, computer viruses, or other factors under the mobile payment operator's control. Wrong payment and delay in payment may cause a breach of the contracts entered between mobile payment users and their payees, and thus mobile payment users may be liable for damages or overdue payment fees.

Another issue lies in the management of client funds, namely the fund

---

61 Rajan, *supra* note 14, at 452–53.

62 Jane Valant, *Briefing: Consumer Protection Aspects of Mobile Payments*, EUR. PARLIAMENTARY RSCH. SERV., 4–5 (2015), https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564354/EPRS_BRI(2015)564354_EN.pdf.

63 Mo Wanyou (莫万友), *Yi Dong Zhi Fu De Fa Lu Wen Ti Ji Qi Jie Jue Ban Fa* (移动支付的法律问题及其解决办法) [*Legal Problems of Mobile Payment and Their Solutions*], 10 LANZHOU XUEKAN (兰州学刊) [LANZHOU ACAD J.] 142, 145 (2017).

64 FED. TRADE COMM'N, PAPER, PLASTIC . . . OR MOBILE? AN FTC WORKSHOP ON MOBILE PAYMENTS 11 (2013), https://www.ftc.gov/sites/default/files/documents/reports/paper-plastic-or-mobile-ftc-workshop-mobile-payments/p0124908_mobile_payments_workshop_report_02-28-13.pdf.

that is pre-received from clients to the mobile payment platform and then paid to the merchants according to the transaction order. Payment institutions can generate profitable interest rewards from the fund. Some entities seized such a lucrative opportunity to gain illicit profits by misappropriating consumer funds, which became the focus of regulators. For instance, Kayou Payment Services Co. Ltd was found to have mismanaged customer deposits and was punished by the PBOC with a fine of over RMB 25.8 million.[65]

The problem of misappropriating client funds can be more acute in relation to so-called dormant funds. User funds or assets are usually stored in the mobile payment platform until that user makes a transaction. There are various reasons why funds in mobile payment platforms can become dormant. For example, the access code or password to the mobile payment account is only known to the user, so the death of the user can lead to the loss of access to mobile payment accounts, and as a result, the funds stored in the account would remain in the mobile payment platform without notice to others.

Although the amount of funds which can be stored by each individual in their mobile wallets is relatively small, the aggregate amount of funds stored in a mobile payment platform can be enormous, especially for mobile payment platforms which have high market shares. If there is ineffective governance or regulation of dormant funds in the mobile payment platforms, the dormant funds could be vulnerable to misappropriation by the mobile payment platforms, which can harm the interests of users and reduce the credibility of the mobile payment industry.[66]

III. THE REGULATORY REGIME IN CHINA

A. Overview

There is no uniform or specific law for regulating the mobile payment industry in China. Instead, relevant rules are scattered around a wide array of laws and regulations with supervisory powers shared by multiple regulators. The overall regulatory aim is to establish a safe, robust, and sustainable mobile payment system, striking a proper balance between the

65 Quan Yue & Fran Wang, *Central Bank Fines Payment Providers for Flouting Rules*, CAIXIN (July 31, 2018), https://www.caixinglobal.com/2018-07-31/central-bank-fines-payment-providers-for-flouting-rules-101310293.html.

66 Valant, *supra* note 62, at 7.

efficiency of the system and consumer protection.[67]

The explosive growth of mobile payment is largely due to a supportive regulatory environment at the initial developing stage. It was not until 2010 that the Chinese government became aware of the risks associated with mobile payment and as a result established a systematic regulatory framework. Chief among the first set of regulations on non-bank payment services is *Administrative Measures for the Payment Services of Non-financial Institutions* (2010 Measures on Third-Party Payment Service)[68] and its implementing rules which were both issued by the PBOC in 2010. It was also confirmed that the PBOC would play a leading regulatory role, responsible for the overall regulation and supervision on the payment services of non-financial institutions (i.e., the third-party mobile payment platforms), as well as facilitating coordination and cooperation of multiple regulatory bodies in this area. Then, due to the increasing misappropriation of clients' reserve by the mobile payment platforms, the PBOC introduced a specific regulation regarding the protection of clients' reserve in 2013. To combat the problem of money laundering, the PBOC introduced a real-name system[69] and specified the daily operation requirements in terms of the large-sum transactions and suspicious transactions from 2015 to 2016.[70] Since 2017, the PBOC has made greater efforts to tighten its regulation of mobile payment, particularly in relation to the management of clients' reserve and the customer reserve requirements.[71]

---

67 ShuSong Ba (巴曙松) & Yang Biao (杨彪), *Di San Fang Zhi Fu Guo Ji Jian Guan Yan Jiu Ji Jie Jian* (*第三方支付国际监管研究及借鉴*) *The International Comparison Over Third-Party Payment*], 4 CAI ZHENG YAN JIU (财政研究) [FIN. RSCH.] 72 (2012).

68 Fei Jin Rong Ji Gou Zhi Fu Fu Wu Guan Li Ban Fa (非金融机构支付服务管理办法) [Administrative Measures for the Payment Services of Non-financial Institutions] (promulgated by the People's Bank of China, June 14, 2010) (China). Several months later, an implementing rule was issued to provide more guidance. Fei Jin Rong Ji Gou Zhi Fu Guan Li Ban Fa Shi Shi Xi Ze (非金融机构支付服务管理办法实施细则) [Implementing Rules for the Administrative Measures for Payment Services of Non-Financial Institutions] (promulgated by the People's Bank of China, Dec. 1, 2010) (China).

69 Fei Yin Hang Zhi Fu Ji Gou Wang Luo Zhi Fu Ye Wu Guan Li Ban Fa (非银行支付机构网络支付业务管理办法) [Administrative Measures for Online Payment Business of Non-Banking Payment Institutions] (promulgated by the People's Bank of China, Dec. 28, 2015), art. 6 (China).

70 Jin Rong Ji Gou Da E Jiao Yi He Ke Yi Jiao Bao Gao Guan Li Ban Fa (金融机构大额交易和可疑交易报告管理办法) [Administrative Measures on Reporting of Large-Sum Transactions and Suspicious Transactions by Financial Institutions] (promulgated by the People's Bank of China, Nov. 14, 2006) (revised Dec. 28, 2016 & July 26, 2018) (China).

71 For further details, see *infra* Part III.

B. Entry Threshold and Exit Mechanism

The primary tool to control market access is via a licensing scheme. To provide payment services, payment institutions must obtain a license pursuant to the 2010 Measures on Third-Party Payment Service.[72] They must satisfy a list of criteria, some of which are noted here. First, the company shall be a limited liability company or joint stock company established in China with the status of a non-financial legal person and with adequate registered capital.[73] The payment institutions providing national payment services shall provide minimum registered capital of RMB 100 million, while those providing province-wide services shall offer RMB 30 million.[74] Second, the major investors, those holding no less than 10% interest in the company or actually controlling the company, must have provided the relevant services and made profits for more than two years.[75] Third, the applicants shall have a robust organizational structure and internal risk control system.[76] Procedurally, the applicant shall first be examined by the local branch of the PBOC in the location where the applicant is domiciled, and then be referred to the PBOC for approval. Although the PBOC confirmed that there would be no quantitative requirements other than those specified requirements,[77] the PBOC did not approve any licensing applications over a long period of time, on the grounds that the suspension of the licensing approval was intended to restore and maintain the market order.[78] The term of the license is five years and the subsequent renewal is allowed upon the PBOC's approval.[79]

---

72 Implementing Rules for the Administrative Measures for Payment Services of Non-Financial Institutions, *supra* note 68, art. 3.

73 *Id.* art. 8.

74 *Id.* art. 9.

75 *Id.* art. 10.

76 *Id.* art. 18.

77 Zhong Guo Ren Min Yin Hang You Guan Bu Men Fu Ze Ren Jiu Fei Jin Rong Ji Gou Zhi Fu Fu Wu Guan Li Ban Fa You Guan Wen Ti Da Ji Zhe Wen (中国人民银行有关部门负责人就《非金融机构支付服务管理办法》有关问题答记者问) [PBOC Answers Questions of Reporters on Rules on the Administration of Payment Services Provided by Non-Financial Institutions] (June 24, 2010), http://www.gov.cn/zwhd/2010-06/24/content_1635734.htm.

78 Wan Jun et al., *Internet Finance in China* (2017), https://www.hankunlaw.com/downloadfile/newsAndInsights/770b77b61e634d1384389f3f5d1b2af8.pdf.

79 Implementing Rules for the Administrative Measures for Payment Services of Non-Financial Institutions, *supra* note 68, art. 13.

C. *Management of Clients' Reserves*

The PBOC has endeavored to mitigate the risk of mobile payment platforms misappropriating clients' reserves. In recent years, numerous scandals of platform collapse have harmed client funds and overall financial stability. The relevant measures taken by the PBOC in this regard are discussed below.

First, the 2010 Measures on Third-Party Payment Service confirms that customers retain the legal title of the fund and payment institutions are mere custodians.[80] The payment institutions shall open a deposit account exclusively for clients' reserves at one branch of a commercial bank.[81] The custodian service agreement shall specify rights, obligations, and responsibilities, and the related document shall be filed with the PBOC.[82] The proportion of the paid-up capital shall at least maintain 10% against its daily average balance of clients' deposits.[83] The payment institutions are not allowed to appropriate the fund in any form without approval.[84] The collaborative commercial banks also have a duty to supervise the usage of the fund and report to the PBOC when there is any suspicion.[85]

In 2013, the PBOC issued a further rule specifically governing clients' reserves.[86] The rule imposes more restrictions on payment platforms in terms of gathering, using, and transferring the clients' funds. For example, payment institutions are required to count and draw a certain percentage of risk reserves to secure the clients' reserves, the amount of which depends on the number of partner banks.[87] And the risk reserves shall likewise be preserved in the special purpose account at a reserve bank.[88] Under this rule, payment platforms were still allowed to deposit the funds in the form of time deposits, entity notice deposits, or other forms approved by the PBOC.[89] However, this method has changed dramatically since a notice discussed below was issued in 2017.

In 2017, the PBOC issued a notice requiring all online payment

---

80 *Id.* art. 24.
81 *Id.* art. 26.
82 *Id.*
83 *Id.* art. 30.
84 *Id.* art. 24.
85 *Id.* art. 29.
86 Zhi Fu Ji Go Uke Hu Bei Fu Jin Cun Guan Ban Fa (支付机构客户备付金存管办法) [Measures for the Custody of Clients' Reverses of Payment Institutions] (promulgated by the People's Bank of China, July 6, 2013) (China).
87 *Id.* art. 29.
88 *Id.*
89 *Id.* art. 16.

transactions to settle via a centralized network platform called NetsUnion (WangLian). This platform operates in the form of a company (2017 Notice).[90] The biggest shareholder of NetsUnion is the PBOC, while the remaining shares are held by private institutions.[91] This was a watershed event in the development of the mobile payment market in China, marking the end of the period when third-party payment platforms could negotiate with different banks and bargain for the best offer. After the 2017 reform, there are only two clearing options for payment institutions: UnionPay (a traditional state-backed clearance system) and NetsUnion.

The 2017 Notice was intended to address the concern that some big payment platforms were able to form closed financial ecosystems with absolute control of consumer data and thus bypass the supervision of the PBOC. The centralization of transaction settlements enables the PBOC to access relevant data, keep track of capital flows, and increase its ability to supervise the industry. More importantly, the establishment of a centralized clearinghouse symbolized the effort of the Chinese authority to take more direct control of the mobile payment industry, which had been until then dominated by private firms. Further, by engaging with private firms, the government found a new way to build the mobile payment infrastructure with mixed public and private ownership.

The payment institutions were initially required to put at least 20% of clients' reserves under central management.[92] The required amount has been increased to 50% by April 2018,[93] and then to 100% since January 14, 2019.[94] It indicated that all third-party payment institutions should cancel

---

90 Zhong Guo Ren Min Yin Hang Zhi Fu Jie Suan Si Guan Yu Jiang Fei Yin Hang Zhi Fu Ji Gou Wang Luo Zhi Fu Ye Wu You Zhi Lian Mo Shi Qian Yi Zhi Wang Lian Ping Tai Chu Li De Tong Zhi (中国人民银行支付结算司关于将非银行支付机构网络支付业务由直连模式迁移至网联平台处理的通知) [Notice on Migrating the Online Payment Business of Non-bank Payment Institutions from Direct Connection Mode to Network Platform Processing] (promulgated by the People's Bank of China, Aug. 4, 2017).

91 *Id.*

92 Zhong Guo Ren Min Yin Hang Ban Gong Ting Guan Yu Shi Shi Zhi Fu Ji Gou Ke Hu Bei Fu Jin Ji Zhong Cun Guan You Guan Shi Xiang De Tong Zhi (中国人民银行办公厅关于实施支付机构客户备付金集中存管有关事项的通知) [Notice of the General Office of the People's Bank of China on Matters concerning Implementing the Centralized Deposit of the Funds of Pending Payments of Clients of Payment Institutions] (promulgated by the People's Bank of China, Jan. 13, 2017) (China).

93 Zhong Guo Ren Min Yin Hang Ban Gong Ting Guan Yu Diao Zheng Zhi Fu Ji Gou Ke Hu Bei Fu Jin Ji Zhong Jiao Cun Bi Li De Tong Zhi (中国人民银行办公厅关于调整支付机构客户备付金集中交存比例的通知) [The Circular on Adjusting the Centralized Deposit Percentage of Clients' Reserves of Payment Institutions] (promulgated by the People's Bank of China, Dec. 29, 2017) (China).

94 Zhong Guo Ren Min Yin Hang Ban Gong Ting Guan Yu Zhi Fu Ji Gou Ke Hu Bei Fu Jin Quan Bu Ji Zhong Jiao Cun You Guan Shi Yi De Tong Zhi (中国人民银行办公厅关于支付机构客户备付金全部集中交存有关事宜的通知) [Notice of the General Office of the People's Bank of China on Matters concerning Complete Centralized Deposit of Clients' Reserves of Payment Institutions] (promulgated by the People's Bank of China, June 29, 2018) (China).

the specified account for the customer and shift the sum to the designated central bank account.[95] The PBOC initially decided that no interest would be offered for the central custody of funds, leading to a great loss for payment institutions and invoking much controversy. But then in January 2020, the PBOC announced it would pay an annual interest rate of 0.35% to the payment institutions.[96]

The PBOC also issued a notice that payment institutions should suspend service when the user account is not used for 12 months.[97] But there is no further detail as to the ownership of the asset in the deactivated account after its closure.

D. AML Measures

The Chinese AML regime is based on three overarching principles: the protection of financial integrity, anti-corruption, and harmonization with international standards. Considering the substantial incidence of money laundering via mobile payment accounts, the PBOC introduced the *Measures for the Administration on Anti-Money Laundering and Anti-Terrorist Financing through Payment Institutions* in 2012[98] in accordance with the general AML law. Simply put, the payment institutions are required to establish an effective internal risk control system, such as adequately conducting customer due diligence and making suspicious transaction reports, and set up an AML specialized agency.[99]

Another prominent rule regulating mobile payment also touches on the AML aspect, the *Administrative Measures for Online Payment Business of Non-Banking Payment Institutions (*2015 Measures), [100] which lays out

---

95 *Id.* § 2(4).

96 *Chinese Central Bank to Pay Interest on Centralised Customer Deposits of Payments Companies*, CHINA BANKING NEWS (Jan. 8, 2020), http://www.chinabankingnews.com/2020/01/08/chinese-central-bank-to-pay-interest-on-centralised-customer-deposits-of-payments-companies/.

97 Zhong Guo Ren Min Yin Hang Guan Yu Jin Yi Bu Jia Qiang Zhi Fu Jie Suan Guan Li Fang Fan Dian Xin Wang Luo Xin Xing Wei Fa Fan Zui You Guan Xiang De Tong Zhi (中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关项的通知) [Notice by the People's Bank of China of Matters concerning Further Strengthening Administration of Payment and Settlement to Prevent New Types of Telecommunications and Online Illegal and Criminal Activities] (promulgated by the People's Bank of China, Mar. 22, 2019) (China).

98 Zhong Guo Ren Min Yin Hang Guan Yu Yin Fa Zhi Fu Ji Gou Fan Xi Qian He Fan Kong Bu Rong Zi Guan Li Ban Fa De Tong Zhi (中国人民银行关于印发《支付机构反洗钱和反恐怖融资管理办法》的通知) [Notice of the People's Bank of China on Issuing the Measures for Administration of Anti-money-Laundry and Anti-terrorism by Payment Institutions] (promulgated by the People's Bank of China, Mar. 5, 2012) (China).

99 *Id.* arts. 5–6.

100 Administrative Measures for Online Payment Business of Non-Banking Payment Institutions,

specific guidance on how mobile payment business should be conducted. Particularly, payment institutions are required to follow the "know your customer" requirement, under which a real-name system should be implemented for account management.[101] Payment institutions are banned from opening payment accounts for financial institutions or other related businesses.[102] Additionally, the PBOC would evaluate AML measures via a scoring system, under which lower scorers might be subject to a higher level of scrutiny.[103]

It was not until 2016 that the PBOC extended the reporting requirement of large-sum and suspicious transactions to the non-financial institutions.[104] Payment institutions are obliged to report cash transactions exceeding RMB 50,000 or equivalent value of USD 10,000.[105] The reporting threshold set for non-natural person clients or cross-border transfer is much higher.[106]

E. Consumer Protection

After the reinforcement of the consumer identity authentication requirement, there has been an increasing demand for data protection, including the collection, processing, and transfer of the consumer's personal information as well as the data generated from the payment record.

The PBOC enacted relevant rules to safeguard the consumer's data securitity and privacy.[107] For instance, the 2015 Measures requires payment institutions to establish effective internal data management and a risk control system, and to strictly comply with the "minimal collection" principle when collecting data.[108] Also, centralized management by NetsUnion can prevent the misuse of clients' data, because the data accompanying the transaction would be transferred to NetsUnion as well.[109]

In order to strengthen the protection of personal financial information,

---

supra note 69.

101 *Id.* art. 6.

102 *Id.* art. 8.

103 *Id.* art. 32.

104 Administrative Measures on Reporting of Large-Sum Transactions and Suspicious Transactions by Financial Institutions, *supra* note 70.

105 *Id.* art. 5.

106 *Id.*

107 As the protection of data privacy is a big topic, it is impossible to do justice to it in this paper which aims to generally examine China's regulation of mobile payment. In fact, the leading author of this paper has written a separate paper to specifically examine the issue. *See* Huang et al., *supra* note 34.

108 Administrative Measures for Online Payment Business of Non-Banking Payment Institutions, *supra* note 69.

109 Notice on Migrating the Online Payment Business of Non-bank Payment Institutions from Direct Connection Mode to Network Platform Processing, *supra* note 90.

the PBOC has recently issued the *Technical Specification for Protection of Personal Financial Information*,[110] categorizing personal information into three types: C1, C2, and C3, with an increasing level of sensitivity.[111] Detailed requirements are laid out regarding the entire cycle of information handling, including collection, storage, use, sharing, and deletion of personal information.[112] No entities without relevant qualifications or licenses would be allowed to collect C2 and C3 information, despite being on behalf of the payment institutions.[113] Further, the transfer, saving, use, and deletion of C2 or C3 information are subject to the more stringent requirement as the leak of that information would cause more harm to the individuals due to increased sensitivity, particularly when there is mounting concern regarding the increasing use of facial or fingerprint recognition. Such biometric information is subject to the highest level of protection as C3 information.[114]

Some general laws also govern this aspect of mobile payment, including the PRC Criminal Law, which imposes the highest penalties for infringement of personal information.[115] *The 2016 Cybersecurity Law*,[116] as the first national-level law on data protection, focuses on information that can be used to identify individual citizens as well as information concerning the personal privacy of citizens. The legislation mainly targets the network operators and operators of 'critical information infrastructure' (CII), and mobile payment institutions are very likely to fall within the scope of the CII.

Mobile payment also increases security risks such as fraud and hacking. The rule dealing with unauthorized payment is also of primary concern to consumers. The 2015 Measures requires the payment institutions to advance

---

110 Ge Ren Jin Rong Xin Xi Bao Hu Ji Shu Gui Fan (个人金融信息保护技术规范) [Technical Specification for Protection of Personal Financial Information] (promulgated by the People's Bank of China, Feb. 13, 2020) (China).

111 *Id.* § 4.2.

112 *Id.* § 6.

113 *Id.* § 6.1.

114 *Id.* § 4.2.

115 Xing Fa Xiu Zheng An Jiu (刑法修正案(九)) [Amendments to the Criminal Law of the People's Republic of China (9) (Ninth Amendment)] (promulgated by the Standing Comm. Nat'l People's Cong., Sept. 29, 2015), arts. 253-1, 286-1 (China); *see also* Guan Yu Ban Li Qin Fan Gong Min Ge Ren Xin Xi Xings Hi An Jian Shi Yong Fa LÜ Ruo Gan Wen Ti De Jie Shi (关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释) [SPC and SPP Judicial Interpretation on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information] (promulgated on May 8, 2017, June 1, 2017) (China).

116 Zhong Hua Ren Min Gong He Guo Wang Luo An Quan Fa (中华人民共和国网络安全法) [Cyber Security Law of the People's Republic of China] (promulgated by Standing Comm. Nat'l People's Cong., Nov. 7, 2016).

full compensation for consumers' capital losses before the investigation is completed. [117] However, there is no other specific rule on this issue. In practice, the related disputes are normally addressed by the *PRC Contract Law*[118] or the *PRC Tort law*,[119] under which the burden of proof is on the plaintiff, namely, the consumer side.

IV. INTERNATIONAL EXPERIENCES

A. The US

Mobile payment is classified as a Money Service Business in the US according to the *Bank Secrecy Act*,[120] which is administered by the Financial Crimes Enforcement Network (FinCEN). Unlike similar entities in China, Money Service Business providers in the US are treated as financial institutions and are thus subject to the regulatory regime for financial institutions.

The regulatory regime for financial institutions in the US has two levels, federal and state. In respect to the entry threshold, federal and state licenses are both required for participants. The applicants shall register with the FinCEN on the online e-filing system, which is mainly used to collect initial information rather than to impose any onerous requirement in terms of bonding or net worth.[121] In contrast, states may impose substantive requirements, which are often regarded as an obstacle for payment institutions to enter the national market.[122] For example, under the *Uniform Money Service Act* (UMSA)[123], a model law adopted by 12 states,[124] applicants are required to provide security of USD 50,000, plus USD 10,000 for each location (up to an additional USD 250,000).[125] The security can

---

117 Administrative Measures for Online Payment Business of Non-Banking Payment Institutions, *supra* note 69, art. 19.

118 Zhong Hua Ren Min Gong He Guo He Tong Fa (中华人民共和国合同法) [Contract Law of the People's Republic of China] (promulgated by Standing Comm. Nat'l People's Cong., Mar. 15, 1999).

119 Zhong Hua Ren Min Gong He Guo Qin Quan Ze Ren Fa (中华人民共和国侵权责任法) [Tort Law of the People's Republic of China] (promulgated by Standing Comm. Nat'l People's Cong., Dec. 26, 2009).

120 Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (1970).

121 FIN. CRIMES ENF'T NETWORK, REGISTRATION OF MONEY SERVICES BUSINESS (RMSB) ELECTRONIC FILING INSTRUCTIONS 6 (1st ed. 2014).

122 Kathryn L. Ryan & Christopher Robins, *Navigating State Money-Transmission Laws*, C-SUITE FIN. SERVS. REV. (2018), https://buckleyfirm.com/sites/default/files/18141_BR_C-Suite_Fall18_Navigating-state-money-transmission-laws.pdf.

123 UNIF. MONEY SERVS. ACT (UNIF. L. COMM'N 2004).

124 UNIF. L. COMM'N, 2020–2021 GUIDE TO UNIFORM AND MODEL ACTS 23 (2021), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=ff9deb0c-9b0f-4f3b-1505-fdd63a9e2325.

125 UNIF. MONEY SERVS. ACT, *supra* note 123, § 204.

take the form of bonds, cash, or letter of credit.[126] A net worth of at least USD 25,000 is required as well.[127] The license granted is effective for one year and annual renewal is expected.[128]

As for the exit mechanism, Article 8 of the UMSA specifies the circumstances under which the superintendent may take disciplinary actions against the licensee, such as suspending or revoking its license. Importantly, the action shall be taken only after the hearing procedure.[129] However, if regulators reasonably hold that the business of the licensee is likely to cause irreparable and immediate harm, they can take immediate action without prior notice or a hearing procedure.[130]

Regarding the customer deposit, the "pass-through insurance" of the Federal Deposit Insurance Corporation (FDIC) can cover the fund deposited in banks, share accounts and share draft accounts at credit unions, provided that the relevant requirements are met.[131] The amount of insurance is up to USD 250,000 per depositor, per institution and per ownership category.[132] However, it does not guarantee consumer protection in the event of bankruptcy or insolvency of the payment institutions.[133] The payment institutions are also allowed to invest the fund in permissible projects that are highly liquid and safe.[134] Different states implement different unclaimed property laws concerning a dormant asset. In general, holders of tangible or intangible property which is owned by others are required to "escheate" the property to the "state comptroller, treasurer, or other designated agency" if the legal owner cannot be found within the statutory abandonment period.[135]

Further, the US has tried very hard to combat money laundering and terrorism financing. The current AML regime for payment institutions is mainly comprised of three legal instruments: the *Bank Secrecy Act*,[136] the

126 *Id.* § 204 cmt.

127 *Id.* § 207.

128 *Id.* § 206.

129 *Id.*

130 *Id.*

131 Federal Deposit Insurance Act, 12 U.S.C. §§ 1811–1835a; *see also* Robert, C. Drozdowski, Matthew W. Homer, Elizabeth A. Khalil & Jeffrey M. Kopchik, *Mobile Payments: An Evolving Landscape*, 9 SUPERVISORY INSIGHTS 1, 3–11 (2012).

132 For a more detailed discussion, see the guidance provided by FDIC, available at https://www.fdic.gov/deposit/diguidebankers/documents/single-accounts.pdf (accessed on Aug. 3, 2020).

133 Drozdowski et al., *supra* note 131, at 9.

134 UNIF. MONEY SERVS. ACT, *supra* note 123, § 701.

135 Fonte, *supra* note 22, at 586.

136 Bank Secrecy Act of 1970, *supra* note 120.

Money Laundering Suppression Act,[137] and the *USA PATRIOT Act*.[138] Given the complexity and intricacy of the AML process, all investigatory agencies, including federal, state, local and even foreign law agencies, can request that FinCEN share certain information obtained from financial institutions.[139]

Finally, consumer protection in the US is secured by the existing legal regime, under which the level of protection largely depends on the method of payment.[140] For instance, if a mobile payment is linked to a credit card account, the transaction would be governed by the *Federal Truth in Lending Act* (TLA)[141] and *Regulation Z*.[142] If the payment is made through a debit card or bank account, then it is protected under the federal *Electronic Funds Transaction Act* (EFTA),[143] which is further implemented by *Regulation E*.[144]

In terms of an unauthorized payment, if a phone is lost or stolen, the consumer might be liable for USD 50 if reporting to the institution within two business days, while the maximum amount would extend to USD 500 if there is any undue delay.[145] If the unauthorized payment occurs on the bank statement and no phone is missing, then the consumer would take no liability provided notification is given within 60 days.[146] To address the uncertainty and ambiguity of the statute, the Consumer Financial Protection Bureau (CFPB), which is responsible for the US consumer protection in the financial sector, has the authority to interpret the relevant rules and determine relevant issues on a case-by-case basis.[147]

The issues of data privacy and security are dealt with under the *Gramm-Leach Bliley Act*.[148] Notably, clients are entitled to reject the request of their payment institutions to share their personal information with third parties. Such an option must not be excluded in the consumer service agreement.[149]

---

137 Money Laundering Suppression Act of 1994, Pub. L. No. 103-325, 108 Stat. 2243 (1994).

138 U.S. Patriot Act of 2001, Pub. L. No. 107-56, 115. Stat. 272 (2001).

139 *Id.* § 314(a). For more details, see FinCEN official website, available at https://www.fincen.gov/resources/law-enforcement-overview.

140 Suzanne Martindale & Gail Hillebrand, *Pay at Your Own Risk? How to Make Every Way to Pay Safe for Mobile Payments*, 27 BANKING & FIN. L. REV. 265, 271–79 (2011).

141 15 U.S.C. §§ 1601–1666(j) (2012).

142 12 C.F.R. §§ 226.1, 226.59 (2012).

143 15 U.S.C. §§ 1693a–1693p (2012).

144 Electronic Fund Transfers (Regulation E), 12 C.F.R. pt. 1005 (2017).

145 *Id.* § 1005.6(b).

146 *Id.*

147 Fonte, *supra* note 56, at 426.

148 15 U.S.C. §§ 6801–6809 (2012).

149 *Id.* § 6802(b).

B. The U.K.

Mobile payment in the U.K. is mainly governed by the *Payment Services Regulations 2017* (PSR 2017)[150] and *the Electronic Money Regulations 2011* (EMR).[151] The Payment Systems Regulator (PSR), established in 2013 as a subsidiary of the Financial Conduct Authority (FCA), is an independent regulator that oversees the payment systems industry in the UK. Notably, the FSR is the world's first dedicated regulator for the payment sector, and is charged with both competition and regulatory powers, aiming to "ensure that payment systems are operated and developed in a way that considers and promotes the interests of all the businesses and consumers that use them," "promote effective competition in the markets for payment systems and services," and "promote the development of and innovation in payment systems."[152]

To provide payment services, institutions shall first comply with the registration or authorization requirement under the PSR 2017 and EMR unless they fall within an exemption.[153] The registration category and the specific application requirement depend on the type and scale of the business involved.[154] For instance, a mobile payment services provider with a considerable scale of business would apply for the status of the Electronic Money Institution (EMI), as the electronic storage of funds would fall under its definition. Apart from assessing the relevant information listed in the statutory form, the regulatory authority can request additional information if necessary.[155] An intentional or reckless material fault or misleading information disclosure may expose the applicants to the criminal offense.[156] In addition, payment service providers are required to meet the initial capital requirement.[157] A normal-sized EMI is required to hold at least EUR 350,000.[158] It must also satisfy the minimum capital requirement at all times.[159] The additional amount of capital would be required if the EMI

150 The Payment Services Regulations 2017, SI 2017/752 (Eng.).

151 The Electronic Money Regulations 2011, SI 2011/99 (Eng.).

152 See the official website of the PSR, https://www.psr.org.uk/ (last visited July 18, 2020).

153 Payment Services Regulations, *supra* note 150, art. 6, sched. 2; Electronic Money Regulations, *supra* note 151, art. 6.

154 *Id.*

155 FIN. CONDUCT AUTH., PAYMENT SERVICES AND ELECTRONIC MONEY–OUR APPROACH, chs. 3.10–20 (June 2019).

156 Payment Services Regulations, *supra* note 150, art. 142; Electronic Money Regulations, *supra* note 151, art. 66.

157 Payment Services Regulations, *supra* note 150, art. 6(3), sched. 2; Electronic Money Regulations, *supra* note 151, art. 6.3, sched. 1.

158 FIN. CONDUCT AUTH., *supra* note 155, ch. 3.46.

159 *Id.* chs. 3.46–48.

increases the provision of an unrelated payment service.[160]

To safeguard customer funds, the payment institutions shall fulfill the safeguarding obligations in two ways: segregating the fund or offering the insurance or comparable guarantee.[161] Any segregated funds shall be kept in a separate account with an authorized credit institution or shall be invested in secure liquid assets.[162] In exceptional circumstances, other investment forms may be approved with sufficient justification.[163] Unlike in China, there is no requirement of one specific account for storing the clients' funds. One payment institution may have several accounts, but its associated companies cannot share the accounts.[164]

Regarding the AML approach, in addition to the PSR 2017 and the EMR, there are some other legislations that the payment institutions shall comply with.[165] The most typical one is *the Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017*.[166] The novelty of the system is that it does not merely rely on the public effort, but also the participation of private sectors. The Joint Money Laundering Steering Group (JMLSG) is a private association that consists of all the UK's leading trade associations in the financial industry.[167] The JMLSG publishes guidance to the firms regarding how to fulfill their AML obligations. The guidance is not mandatory but still important as a benchmark of industry practice for the court and the regulatory authorities to refer to.

The protection of consumers is of great priority for the UK regulators. Except for the security of consumer funds and the minimum capital required in the license as mentioned above, the law also provides a detailed list of business conduct requirements that the institutions shall comply with.[168] They can be broadly summarized into two categories: (1) information disclosure before and after the transaction; and (2) the rights and obligations of respective parties. Besides, consumer rights are protected for unauthorized payment. As in the US, consumer liability would be capped at

---

160 *Id.*

161 FIN. CONDUCT AUTH., *supra* note 155, ch. 10.29.

162 *Id.* ch. 10.35.

163 *Id.* chs. 10.46–48.

164 *Id.* chs. 10.41–44.

165 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692 (Eng.); Commission Regulation 2015/847, 2015 O.J. (L 141).

166 Money Laundering, *supra* note 165. For more details, see FIN. CONDUCT AUTH., *supra* note 155, ch. 8.57.

167 See the official website of The Joint Money Laundering Steering Group (JMLSG), available at https://jmlsg.org.uk/joint-money-laundering-steering-group-jmlsg/about-us/who-we-are/ (last visited July 18, 2020).

168 FIN. CONDUCT AUTH., *supra* note 155, ch. 8.

GBP 35 in the case of the mobile device being stolen or lost.[169] Consumers are also given the right to rectify unauthorized transactions and defective transactions if they notify the relevant service provider within a certain period.[170] In principle, consumers would not be liable for any loss unless otherwise proved by the payment institutions.[171] Further, if there is any complaint or dispute, the consumer can address their problems through various channels. They can complain to the payment institution, which must respond within a specified time limit.[172] Other options include the financial ombudsman service, a statutory or informal dispute-resolution forum.[173]

The consumer data is protected by the PSR 2017, the Data Protection Act 2018,[174] and the *General Data Protection Regulation* (GDPR).[175] The GDPR is claimed to be the world's most far-reaching data privacy regulation, setting out considerable provisions to safeguard data protection and provide individuals with stronger rights. In general, it introduced six vital data processing principles. For example, personal data must be processed lawfully, fairly, and transparently, and must be collected for a legitimate and necessary purpose. Compared to other jurisdictions, the GDPR is claimed to impose much more onerous obligations on the payments service providers. For instance, prior consent is needed before collecting any personal data, and the users' right to withdraw their consent at any time is also highlighted.[176] Any breach of the GDPR may incur significantly high administrative fines. For breach of certain important provisions, the fines can amount up to EUR 20 million or 4% of global annual turnover.[177]

C. Singapore

Singapore, striving to become a Fintech hub, was one of the earliest countries to respond to the development of Fintech with regulation.[178] The primary legal instrument is the *Payment Services Act 2019* (PSA), which

---

169 *Id.* ch. 8.218.

170 Payment Services Regulations, *supra* note 150, art. 74.

171 *Id.* art. 77.

172 FIN. CONDUCT AUTH., *supra* note 155, chs. 11.16–21.

173 *Id.* ch. 11.

174 Data Protection Act 2018, c. 12 (UK), https://www.legislation.gov.uk/ukpga/2018/12/contents.

175 Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, art. 20.

176 *Id.* art. 7.

177 *Id.* art. 83.

178 Sei Fan Pei, *Singapore Approach to Develop and Regulate FinTech*, *in* 1 HANDBOOK OF BLOCKCHAIN, DIGITAL FINANCE, AND INCLUSION 347–57 (2018).

came into effect on 28 January 2020. The PSA and its implementing rules together lay out a comprehensive regulatory regime for mobile payment in Singapore. The Monetary Authority of Singapore (MAS), which is the central bank and integrated financial regulator in Singapore, is the main regulator regarding mobile payment.[179]

The PSA introduces two parallel regulatory frameworks: a licensing regime and a designation regime. Under the licensing regime, there are three kinds of licenses, namely money-changing licenses, standard payment institution licenses, and major payment institution licenses, according to the types and numbers of the services provided, and the business volume of the firms. Besides, the MAS is empowered to designate a payment system for four statutory reasons: financial stability, public confidence, public interest, and the efficiency and competition of the payment service. Hence, the MAS adopts a risk-based approach under which only those posing significant risks would be required for licensing, while the low-risk firms are exempted, to build a more accessible payment ecosystem.[180] The MAS can designate a payment institution to meet the licensing requirement in the public interest if it is satisfied that they may pose risks to the system even though they may otherwise be not subject to the licensing requirement.[181]

To safeguard consumer interest from flight risk, the MAS requires the payment institutions to submit a certain amount of security for the due performance of their obligations.[182] The MAS has clarified that the security was not intended to cover all losses of the customers, which otherwise, might impose too high of a burden on the businesses.[183] Regarding the clients' reserve, the major payment institutions are required to adopt safeguard measures: a deposit in a trust account, an undertaking or guarantee by a safeguarding institution, or any other prescribed manner by the MAS.[184] Furthermore, the MAS imposes a cap on the amount of funds that the consumers can store in their e-wallet accounts to maintain the crucial economic function that the banks perform in the financial system.[185]

In relation to the settlement of unauthorized transactions, the *E-*

---

179 The MAS official website, https://www.mas.gov.sg/who-we-are/What-We-Do.

180 MONETARY AUTH. SING., PAYMENT SERVICES ACT 2019: FREQUENTLY ASKED QUESTIONS (FAQS) ON THE PAYMENT SERVICES ACT (PS ACT), at 8 (May 11, 2020), https://www.mas.gov.sg/-/media/MAS/Fintech/Payment-Services-Act/Payment-Services-Act-FAQ-11-May-2020.pdf.

181 *Id.* at 6.

182 Payment Services Act 2019, § 22, https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220. Flight risk refers to the risk that someone accused of a crime will try to escape out of the country or area before their trial begins.

183 MAS, *supra* note 180, at 17.

184 Payment Services Act 2019, Act 2 of 2019 (Sing.).

185 MAS, *supra* note 180, at 23.

payments User Protection Guidelines[186] identifies the situations where users and payment institutions should take liability arising from unauthorized transactions respectively. For example, the user will bear the actual loss if the loss is mainly caused by the user's recklessness,[187] while mobile payment platforms will be liable for loss caused by fraud, negligence, or non-compliance of regulations imposed by the MAS.[188] Besides, if the user's account has a balance of more than SGD 500 at any time and is used for electronic payments, the user will not be liable for any loss in an unauthorized transaction which does not exceed SGD 1,000.[189]

To address the cybersecurity concern, the MAS issued several guidelines, including the *Notice PSN05 Technology Risk Management*[190] and the *Notice PSN06 Cyber Hygiene.*[191] PSN05 sets out that payment institutions should maintain a sufficiently high degree of availability and recoverability in the critical systems (the failure of which may cause significant disruption to the operation of payment service).[192] The specific measures the payment institutions shall take include restricting the maximum unscheduled downtime for each critical system of not more than 4 hours, reporting the relevant incidents in time, and implementing IT controls to protect customer information. PSN06 aims to protect users from cyber threats. The payment institutions are required to implement and maintain robust security for IT systems via timely updates to address the security flaws, and strengthen user authentication.

The last highlight is the MAS's solution to reduce the fragmentation of the payment industry.[193] The MAS launched the Singapore Quick Response Code (SGQR), the world's first unified payment code that combined multiple payment codes into a single one. Merchants can use a single QR code to link with different payment service applications. The customers can check the merchant name and choose one of the payment platforms—such

---

186 MONETARY AUTH. SING., E-PAYMENTS USER PROTECTION GUIDELINES, https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Payment-and-Settlement-Systems/PSOA-Guidelines/E_payments-User-Protection-Guidelines-WEF-28-January-2020.pdf (updated Jan. 28, 2020).

187 *Id.* §§ 5.2–5.4.

188 *Id.* §§ 5.5–5.6.

189 *Id.*

190 *Notice PSN05 Technology Risk Management*, MONETARY AUTH. SING. (Dec. 5, 2019), https://www.mas.gov.sg/regulation/notices/psn05.

191 *Id.*

192 The definition of critical system is further explained in MAS, RESPONSE TO FEEDBACK RECEIVED – CONSULTATION PAPER ON THE NOTICE ON TECHNOLOGY RISK MANAGEMENT 3, https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/Response-to-Consultation-Paper_TRM-Guidelines.pdf. (last visited Apr. 24, 2020).

193 MAS, *supra* note 180, at 19–20.

as Alipay, Remo, and EZ-Link—that the merchant has contracted with. Under the PSA, the MAS has further power to impose interoperability measures, including requiring the large institutions to allow the third parties to access their system; mandating any major payment institutions to participate in a common platform or adopt common standards such as the SGQR.[194]

In short, the MAS attempts to build a simple, secure, and accessible payment regulatory regime, streamlining the regulation under one single legislation with other accompanying instruments. The MAS adopted a risk-based approach to regulation, and maintains the flexibility to deal with the particular circumstances of individual cases.

D. Hong Kong

Hong Kong, one of the world's top financial hubs, has been criticized for being too slow to embrace advanced digital payment technologies.[195] The lukewarm attitude towards mobile payment in Hong Kong is partly due to the deep-rooted customer payment habits of using credit cards and the local Octopus card.

Mobile payment platforms or applications are normally within the category of multi-purpose stored value facility (SVF) under the Hong Kong regulatory regime. Apple Pay is not considered an SVF, as it does not perform any stored value function and users complete the transactions via the credit card.[196] Since the introduction of the *Payment Systems and Stored Value Facilities Ordinance* (SVF Ordinance)[197] in 2015, the SVF has been supervised and regulated by the Hong Kong Monetary Authority (HKMA) which is the central bank as well as the banking regulator in Hong Kong. Under the SVF Ordinance, all SVF must obtain a license unless falling within the exemption.[198] To obtain a license, the applicant must satisfy several requirements. First, the principal business should be issuing SVF and not engaging in other irrelevant business without the approval of the HKMA.[199] Second, the applicant should own a paid-up capital not less than HKD 25 million or other equivalent convertible currency.[200] However, the

---

194 *Id.*

195 Robin Hui Huang, Cynthia Sze Wai Cheung & Christine Meng Lu Wang, *The Risks of Mobile Payment and Regulatory Responses: A Hong Kong Perspective*, 7 ASIAN J.L. & SOC'Y 325 (2020).

196 *Part 1: Smart Tips on Using Stored Value Facilities*, H.K. MONETARY AUTH. (Aug. 23, 2016), https://www.hkma.gov.hk/eng/news-and-media/insight/2016/08/20160823/.

197 The Payment Systems and Stored Value Facilities Ordinance, (2015) Cap. 584 (H.K.).

198 *Id.* § 8F.

199 *Id.* pt. 2(1), sched. 3.

200 *Id.* pt. 2(2), sched. 3.

HKMA might impose a higher amount in light of the risk and scale of the business of the particular applicant.[201]

Third, to ensure robust corporate governance, the SVF must implement appropriate risk management policies and procedures, as well as sound and prudent operating rules.[202] As such, the appointment of each chief executive, director, and controller of the applicant shall obtain prior consent from the HKMA.[203] Regarding the public concern over the safety of clients' funds particularly in the event of insolvency of the SVF, licensees are required to keep all funds for prescribed usage only and always maintain a sufficient deposit to redeem the outstanding stored value.[204] Furthermore, the trust arrangement supported by legal opinion shall be put in place to guarantee the priority of the users if the SVF goes bankrupt.[205] Fourth, the HKMA adopts a risk-based approach to address the global concern of money laundering, under which the applicant is required to take preventive measures and establish an AML/CFT monitoring system proportionate to the risks exposed.[206] The HKMA retains the power to revoke or suspend the license as a penalty if the licensee fails to comply with the requirements.[207] Fifth, apart from the SVF Ordinance, the SVF must fully comply with the *Personal Data (Privacy) Ordinance*[208] in relation to privacy protection.

To address the issue of market fragmentation, on September 17, 2018, the HKMA launched the Faster Payment System (FPS), representing a watershed in the development of mobile payment in Hong Kong. The FPS removes the stumbling block to the popularization of e-wallets, enabling fund transfers to be made anytime and anywhere across the banks and the SVF via a phone number or email address.[209] Additionally, the HKMA and other interested parties, including the payment network operators and the bank industry, have worked on a common QR Code Standard for retail payment.[210]

---

201 *Id.*

202 *Id.* pt. 2(5), sched. 3.

203 *Id.* pts. 2(2)–(3), sched. 3.

204 *Id.* pt. 2(8), sched. 3.

205 *Id.*

206 H.K. MONETARY AUTH., GUIDANCE PAPER: TRANSACTION SCREENING, TRANSACTION MONITORING AND SUSPICIOUS TRANSACTION REPORTING (2018), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20180510e3a1.pdf.

207 The Payment Systems and Stored Value Facilities Ordinance, *supra* note 197, sched. 5.

208 The Personal Data (Privacy) Ordinance, (1996) Cap. 486 (H.K.).

209 Michael Yu, *E-Wallets in Hong Kong*, LEGIS. COUNCIL H.K. SPECIAL ADMIN. REGION CHINA (Aug. 1, 2018), https://www.legco.gov.hk/research-publications/english/essentials-1718ise08-e-wallets-in-hong-kong.htm.

210 H.K. MONETARY AUTH., IMPLEMENTATION GUIDELINE (EFFECTIVE FROM 17 SEPTEMBER

V. ANALYSIS AND SUGGESTIONS

A. Overview

1. Strengths of the Chinese Law

The common goal for all jurisdictions in regulating mobile payment is to strike a proper balance between consumer protection and business development/technology innovation. As discussed above, similar to China, all our examined overseas jurisdictions have covered the four main regulatory elements, but each jurisdiction shows some distinctive features in their regulatory regimes.

The U.S., on the one hand, emphasizes minimum intervention by setting a relatively low entry requirement. On the other hand, the U.S. still emphasizes consumer protection via extending coverage from the FDIC and insisting on limiting the liability of consumers for unauthorized payments. The U.S. also has a well-established legal framework in relation to the issues of AML, CFT, and consumer protection. The U.K. puts much effort into strengthening consumer rights and protection via comprehensive and systematic regulations. Singapore emphasizes proportionality and flexibility by adopting a risk-based approach, while Hong Kong is dedicated to establishing a secure and suitable regime for mobile payment.

China largely took a hands-off approach in the early stage of mobile payment development, a decision that has proved to be one of the key drivers for the rapid growth of mobile payment in China. As the problems and risks associated with mobile payment gradually emerged, China responded quickly by establishing a comprehensive regulatory regime, including a licensing regime and a set of stringent requirements in relation to important issues such as clients' fund management and AML measures. By comparison with other jurisdictions, China sets a relatively high entry threshold to screen out unqualified candidates at the entry stage. Further, China seems to have paid more attention to the safety of clients' funds by establishing a centralized clearinghouse, which represents a significant development of the infrastructure used to operate the payment systems. In regard to the issues of AML and data protection, a large number of rules have been put in place by various regulators.

2018): COMMON QR CODE FOR RETAIL PAYMENTS IN HONG KONG (2018), https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/infrastructure/retail-payment-initiatives/Implementation_Guideline_on_Common_QR_Code.pdf.

B. Weaknesses of the Chinese Law

Although the Chinese regulatory regime for mobile payment has many merits, there are some shortcomings that need to be properly addressed if China wishes to bring its mobile payment industry to a higher level.

Overall, China's mobile payment is governed by a patchwork of administrative rules issued over the last decade by various regulators in a piecemeal manner. This has made it difficult for market participants to understand and comply with the relevant rules, and also has led to gaps, overlaps, and inconsistency in the regulatory framework.[211] In one sense, the piecemeal approach is practical as it allows China to efficiently respond to emerging issues in a fast-changing setting like the mobile payment market. Wile this may be appropriate for the initial stage of market development, it can become problematic once the market has grown to a more advanced stage. China now has one of the largest markets of mobile payment in the world, which plays a very important role in the financial system. However, its current regulatory regime has evolved in an accretive way in response to problems, without any real focus on the overall mission in the long term.

The time has come for China to enact a unified law specifically for mobile payment to improve regulatory coherence, consistency, and efficacy. The absence of such a law presents a threat to the sustainable development of mobile payment in China. In this regard, Singapore provides a good example to follow. As discussed earlier, Singapore streamlines its regulatory regime by incorporating and integrating all payment-related matters into one overarching piece of legislation and then specifying details through implementing rules. In doing so, the Singapore's regulator has absorbed public and industry opinions via public consultation from time to time, which helps ensure the suitability of the law to meet the market needs.[212]

With regard to its regulatory approach, China traditionally tends to apply regulatory requirements in a sweeping fashion, which can lead to the dangers of a "one-size-fits-all" approach. Indeed, as exceptions are prone to

---

211 Zhou Xue Dong Dai Biao : Ying Jin Kuai Chu Tai Fei Jin Rong Ji Gou Zhi Fu Fu Wu Guan Li Tiao Li (周学东代表：应尽快出台《非金融机构支付服务管理条例》) [*The Call from Representative Zhou Dongxue: Regulations on Payment Services Provided by Non-Financial Institutions Should Be Promulgated*)], CAIXIN (财新网) (Mar. 4, 2015), http://topics.caixin.com/2015-03-04/100787732.html.

212 *Id.*

abuse, Chinese regulators usually prefer the so-called "one clean-cut" (yi dao qie) approach. This may make it easy, and sometimes seemingly fair, to regulate the relevant entities, but it may come as a problematic Procrustean bed to the market. For example, China prescribes only one unitary standard of capital requirement for all third-party payment institutions, regardless of their size and risk level of the activities involved. Hence, the risk-based approach as adopted in Singapore and Hong Kong may be worthy of consideration for China in setting out specific regulatory requirements. The next part will conduct a more detailed discussion of the specific regulatory requirements and relevant suggestions.

C. Improvement Suggestions

1. Entry Threshold and Exit Mechanism

Controlling market access is one of the common regulatory measures in China. However, the licensing threshold in China may have chilling effects on the new entrants. It was predicted that at least half of the participants providing payment services had to leave the market due to the promulgation of the 2010 Measures on Third-Party Payment Service.[213] The minimum capital requirement for getting a payment service license in China[214] is around 37 times that of the UK[215] and 556 times that of the US.[216] Given the high level of concentration in China's mobile payment market, Alipay and Tenpay together enjoy an effective monopoly in the payment market with more than 90% of the market share.[217] The high entry threshold may reinforce market concentration and impede small participants from entering the market. This may eventually trap policymakers in the "too big to fail" pitfall.[218]

Further, the capital requirement in China is based on static registered capital, while the U.S. instead refers to dynamic corporate net worth. Registered capital cannot accurately reflect the assets of the company and

---

213 Yingzhi Fang(方盈芝), Fei Jin Rong Ji Gou Zhi Fu Fu Wu Guan Li Ban Fa Jie Du Bao Gao (非金融机构支付服务管理办法》解读报告) [*An Evaluation Report on Rules on the Administration of Payment Services Provided by Non-Financial Institutions*] (June 26, 2010), CHINA E-COM. RSCH. CTR. (中国电子商务研究中心), http://b2b.toocle.com/detail--5232440.html.

214 See *supra* Part III.A.

215 See *supra* Part IV.B.

216 See *supra* Part IV.A.

217 *Mobile Finance Got A Shrinking Share in China's Third-party Mobile Payment Market*, IRESEARCH (Mar. 12, 2019), http://www.iresearchchina.com/content/details7_52849.html.

218 Nicola Cetorelli & James Traina, Staff Report, *Resolving 'Too Big to Fail'*, FED. RSRV. BANK N.Y. STAFF REPS. (2018), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr859.pdf.

thus may be insufficient to protect consumer interests.[219] Another problem with the Chinese law on market entry is illustrated by the validity term of the license. Given the rapidly evolving landscape of the mobile payment market, the international practice to renew a license in one year appears to be more pragmatic and effective. Last but not least, the way in which the licensing authority grants approval seems inconsistent and unpredictable, subject to heavy policy influence. This has caused much volatility and speculation in both the licensing price and the payment market itself. The suspension of license granting since 2016 led to scarcity, driving the market price of a license in private transactions to more than RMB 1 billion in 2017, [220] before the price plunged by half in 2018 due to tight regulation.[221]

As discussed before, the PBOC has the power to terminate a license if there is any serious violation of the law, but there is no further detail on how the exit mechanism works. [222] This means that the insolvency or termination of payment institutions would be subject to the general law, including the *PRC Company Law*[223] and the *PRC Bankruptcy Law*.[224] However, payment institutions are different from ordinary companies, in that they usually involve a large amount of capital and a great number of customers. Therefore, there is a call for further guidance as to the exit of payment institutions, so as to minimize the negative impact on society. In this regard, lessons can be learned from the UK and the US, such as setting up an insurance system similar to the FDIC to safeguard the customer interest upon the bankruptcy or insolvency of the payment institutions.

---

219 Su Pan(苏盼), Mei Guo Di San Fang Zhi Fu Zhou Fa Jian Guan Zhi Du Shu Ping Ji Qi Shi (美国第三方支付州法监管制度述评及启示) [*The Comment on the American Third-Party Payment State Regulation and the Lesson from It*], BEIJING UNIV. FIN. L. 202, 206 (2016).

220 Liao ShuMin, *China's Internet Payment License Prices Are Geyser to USD92.3 Million*, YICAI GLOB. (Sept. 20, 2017), https://www.yicaiglobal.com/news/china-internet-payment-license-prices-are-geyser-to-usd923-million.

221 Emma Lee, *Prices of China's Third-Party Payment Licenses Plunge by Half*, TECHNODE (Nov. 6, 2018), available at https://technode.com/2018/11/06/payment-licenses/.

222 See *supra* Part III.A.

223 Zhong Hua Ren Min Gong He Guo Gong Si Fa (中华人民共和国公司法) [Company Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Oct. 26, 2018) (China).

224 Zhong Hua Ren Min Gong He Guo Qi Ye Po Chan Fa (中华人民共和国企业破产法) [Enterprise Bankruptcy Law of the People's Republic of China] (promulgated by the Nat'l People's Cong., Aug. 27, 2006) (China).

2. *Management of Clients' Reserves*

One of the most striking features of China's regulatory regime is the centralization of the settlement of clients' reserves and the "no interest" policy. It deals a blow to the small and medium payment service providers by cutting off a large source of revenue. And placing a great sum of money idle in the centralized settlement account might be a great waste of social resources.[225] It may threaten the survival of many small and medium payment institutions. Further, it is not in line with international practice. It is also problematic, particularly after China has promised to open the payment market to foreign-invested enterprises.[226] In the UK and the US, for example, payment institutions can invest clients' reserves in certain low-risk projects, allowing for a better balance between business efficiency and consumer protection.

Regarding the problem of dormant assets in payment accounts, the Singapore approach provides a good example to follow. The PSA prescribes a maximum amount of funds that can be stored in an e-wallet,[227] and may therefore help to limit the total amount of dormant assets in a mobile payment platform. Further, the PSA impliedly determines the ownership of dormant assets, in that payment platforms are not allowed to on-lend the user's money[228] and thus the ownership of the funds goes to the user. However, as Singapore does not provide details on returning the dormant asset to users, China is advised to further consider the US experience. Apart from setting a maximum amount of funds that can be stored in e-wallets, the US law requires that payment platforms shall transfer the funds in a dormant account to a designated agency if the user cannot be found within a certain period.[229]

---

225 ShuSong Ba(巴曙松), Yang Biao(杨彪), Di San Fang Zhi Fu Guo Ji Jian Guan Yan Jiu Ji Jie Jian(第三方支付国际监管研究及借鉴) [*The International Comparison Over Third-Party Payment*], 4 CAI ZHENG YAN JIU(财政研究) [FIN. RSCH.] 72, 74 (2012).

226 Zhong Guo Ren Min Yin Hang Gong Gao (2018)Di Qi Hao ——Guan Yu Wai Shang Tou Zi Zhi Fu Ji Gou You Guan Shi Yi Gong Gao De Gong Gao中国人民银行公告(2018)第7号——关于外商投资支付机构有关事宜公告的公告(Announcement No. 7 [2018] of the People's Bank of China—Announcement on Matters concerning Foreign-funded Payment Institutions, Mar. 19, 2018).

227 MONETARY AUTH. SING., PAYMENT SERVICES ACT 2019: FREQUENTLY ASKED QUESTIONS (FAQS) ON THE PAYMENT SERVICES ACT (PS ACT), at 28 (Apr. 13, 2020), https://www.mas.gov.sg/-/media/MAS/Fintech/Payment-Services-Act/Payment-Services-Act-FAQ-13-April-2020.pdf.

228 *Id.* at 27.

229 Fonte, *supra* note 22, at 586.

3. *AML*

AML is a global issue in the mobile payment sector. And China's AML regime is in line with international standards, thanks to the introduction of an array of AML measures. The most significant one should be the full implementation of the "real-name" system. However, there are still some remaining enforcement issues that should be addressed.

The major shortcoming is the decentralized supervision structure, under which enforcement is fragmented and the division of power amongst various regulators is not sufficiently clear. The Financial Action Task Force (FAFT), a global watchdog for the AML and the CFT, has pointed out that China should make better use of financial intelligence in the AML investigation and enhance coordination between different agencies.[230] For instance, China may consider learning from the UK approach under which private sectors can also be involved to achieve self-discipline.[231] And the US approach that a single authority is responsible for the sharing of the investigatory information among different regulatory agencies, is also highly recommended.[232]

4. *Consumer Protection*

There are some important issues of consumer protection that China needs to address. For instance, data privacy and security challenges are faced by all countries when embracing the era of the data-driven economy. The US and the UK have traditionally established a robust regime for data protection in the general setting. They have further strengthened the protection in the specific context of mobile payment. In comparison, China has a lot of work to do both in terms of the rules and enforcement.[233] For instance, China introduces the "minimal collection" principle for data collection, but payment institutions have discretion over the degree of "minimum."[234] By contrast, the US law entitles the users to refuse to give or share personal information, enabling the consumers to determine who

---

230 Ben AuYeung & Yaqi Bao , *FATF Report a Wake-Up Call for China on AML and Terrorist Financing*, WOLTERS KLUWER (June 24, 2019), https://www.wolterskluwer.com/en/expert-insights/fatf-report-a-wake-up-call-for-china-on-aml-and-terrorist-financing.

231 See *supra* Part IV.B.

232 See *supra* Part IV.A.

233 As noted earlier, it is beyond the scope of this paper to provide a more detailed analysis of the big issue of data privacy, and in fact, the leading author of this paper has chosen to specifically examine it in a separate paper. See Huang et al., *supra* note 35.

234 See *supra* Part III.D.

can have access to their data.[235]

Another issue of consumer protection lies with unauthorized payments. It is onerous for consumers to bear the burden of proof in bringing an action against the payment institution, because most of the evidence about the payment transaction is stored in the internal system of the payment institution.[236] And this is not in line with the international practice that consumers are protected unless there is gross negligence on their part.[237]

VI. CONCLUSION

By allowing for payments via a mobile phone or device, mobile payment is a disruptive innovation in payment systems, that has fundamentally changed the payments industry and the people's way of life. China, albeit not the originator of the mobile payment, has become a frontrunner in the global mobile payment markets, in terms of market volume, growth rate, and innovation capability. This can be attributed to a number of enabling factors, including technological advancement in China such as the high penetration of smartphones and wide Internet coverage, mobile payment's competitive advantages over the traditional payment in terms of convenience and flexibility, as well as the distinctive Chinese local context where the people are more receptive to the mobile payment due to a lack of credit card engagement and relative insensitivity to data protection issues.

While mobile payment brings important benefits to society, it does not come without risks. It is thus important to find an effective way to regulate mobile payment so that its benefits can be reaped while risks are contained. Over the past decade, China has made great efforts to gradually establish a regulatory framework for mobile payment. There are four main regulatory elements, namely, controlling the market access through a licensing regime, imposing requirements on the management of clients' reserves, combating money laundering and terrorist financing, and strengthening consumer protection.

To better evaluate Chinese regulation, a comparative study is conducted

---

235 See *supra* Part IV.A.

236 Luo Pei-Xin (罗培新), Wu Tao (吴韬), Fei Shou Quan Jiao Yi Zhong Di San Fang Zhi Fu Ji Gou De Fa Lu Ze Ren (非授权交易中第三方支付机构的法律责任) [*The Legal Liability of the Third-Party Payment Institutions in Terms of Unauthorized Transaction*], 20 Hua Dong Zheng Fa Da Xue Xue Bao(华东政法大学学报) [J. E. CHINA UNIV. POL. SCI. & L.] 83, 86–87 (2017).

237 *Id.*

on the regulation of mobile payment in several major jurisdictions, including the US, the UK, Singapore, and Hong Kong. From a comparative perspective, the Chinese regulatory regime has its distinctive features with both strengths and weaknesses. Drawing on international experiences, a number of suggestions are made for China to improve the efficacy of its regulatory regime for mobile payment. In general, China is advised to enact a unified law specifically for mobile payment, as its current regulatory regime has evolved in an accretive way in response to problems without any real focus on the overall mission in the long term. Further, China should discard the "one-size-fits-all" approach in favor of a more nuanced risk-based approach in setting out regulatory requirements.

More specifically, China sets a relatively higher entry threshold to control the market access, which admittedly may help screen out risky platforms from the market, but may also intensify the problem of market monopolization. While China's establishment of a centralized clearinghouse represents a significant development of the infrastructure used to operate the payment systems, it may, coupled with the no-interest policy, raise fairness concerns and threaten the very survival of small or medium payment institutions. Despite strong AML measures, there are problems with the cooperation amongst various enforcement agencies and thus China needs to streamline its enforcement regime. Finally, there remain important issues of consumer protection such as data protection and unauthorized payment that need to be addressed by reform of relevant laws.