Asian Journal of Law and Society, 7 (2020), pp. 325–343
doi:10.1017/als.2019.30

First published online 09 June 2020

The Risks of Mobile Payment and Regulatory Responses: A Hong Kong Perspective•

Robin Hui HUANG*, Cynthia Sze Wai CHEUNG**, and Christine Meng Lu WANG***
Chinese University of Hong Kong

Abstract
Mobile payment generally refers to transactions made through the applications of a portable electronic gadget without the transfer of cash. As one of the most disruptive technologies for finance, mobile payment has been rapidly transforming the traditional financial industry. While it brings important benefits, there are also various risks, in terms of liquidity, security, and data privacy, that call for adequate regulatory responses. As a global financial centre, Hong Kong has gradually established a regulatory framework for mobile payment, addressing the relevant risks with rules on payment and privacy. However, there is still room for further improvement, in terms of measures to deal with cybersecurity issues and strengthen the protection of personal data. The Hong Kong experiences suggest that, to regulate a new and fast-growing industry such as mobile payment, the regulatory regime needs to be improved continuously to alleviate the risk concerns, so as to enhance the protection of financial consumers and society at large.

Keywords: mobile payment, FinTech, financial regulation, cybersecurity, data privacy, Hong Kong

1. INTRODUCTION

Financial technology, namely FinTech, is one of the most popular notions in the twenty-first century and has been reshaping both the future of finance and the way in which people live. One of the most disruptive innovations of this concept is mobile payment, which covers any transaction made through the applications of a portable electronic gadget without the transfer of cash. This includes payments effected via smartphone applications, transmitted through the Internet, as well as wireless transactions made through the Near Field Communications (NFC) protocol or scanning of QR codes. Such rapid evolution of technology has brought great convenience and significant business opportunities to society. However, following an explosive growth in the industry, there is also growing concern from the public on the risks and vulnerabilities that come along.

• This research received support from a Direct Research Grant at the Chinese University of Hong Kong and also from the Hong Kong Research Grants Council's General Research Fund project 'The Regulation of Fintech in China'.

* Professor of Law, Faculty of Law, Chinese University of Hong Kong. Correspondence to Hui Huang, Faculty of Law, Room 521, Lee Shau Kee Building, Chinese University of Hong Kong, Shatin, New Territories, Hong Kong. E-mail address: robinhuang@cuhk.edu.hk.

** Research Fellow, Faculty of Law, Chinese University of Hong Kong.

*** PhD Candidate, Faculty of Law, Chinese University of Hong Kong.

In this paper, we will investigate the existing regulatory framework of the mobile-payment industry in Hong Kong. Section 2 will first give a brief overview of the market and an analysis of the benefits and risks of such technology. Section 3 will then introduce two major regulatory instruments governing the industry, namely the "Payment Systems and Stored value Facilities Ordinance (Cap. 584)" and the "Personal Data (Privacy) Ordinance (Cap. 486)." Lastly, we will discuss whether such regulations have sufficiently addressed three major risks of the business, namely liquidity risk, cybersecurity risk, and data-privacy risk, and make a comparison with their counterparts in other jurisdictions, notably Europe, the US, Singapore, and South Korea. The conclusion we have reached is that, although Hong Kong has in place a regulatory framework for mobile payment, the privacy law in Hong Kong is already out of date, calling urgently for amendment. The newly enacted mobile-payment regulation seems to be adequate at the moment, but supplementary measures concerning security and liquidity risks could be adopted to offer additional protection and foster the confidence of the general public.

2. BACKGROUND

2.1 Development of Mobile Payment in Hong Kong and Overseas

Hong Kong has long been criticized for lagging behind Mainland China and major rival Singapore in developing its financial-technology market. One major reason is that the city was once highly successful with its locally developed gadget, the Octopus card, which was opined as a pioneered invention when it was first introduced in Hong Kong in 1997. With nearly 99% coverage, the Octopus card has dominated the daily life in Hong Kong and there is little incentive for people to embrace a new, complex technology that brings security risks and privacy concerns while providing only similar functions to existing facilities. However, given the threat of losing its status as a leading international financial hub, the Hong Kong government has recently tried to recover its "lost ground" by actively encouraging the public to embrace the new technology.

Since the commencement of the "Payment Systems and Stored Value Facilities Ordinance" (PSSVFO) on 13 November 2015, the Hong Kong Monetary Authority (HKMA) has issued 13 stored value facility (SVF) licences to non-bank institutions.[1] These include the platforms operated by two Chinese financial giants, namely Alipay and WeChat Pay—an invention from the Octopus Company "O! ePay" and some other local operators. They provide services covering peer-to-peer payments as well as merchant payments. On the other hand, the traditional banking industry is also striving to share the market. The dominating bank of the city, HSBC, launched "PayMe"[2] in 2017, allowing consumers to attach their credit cards to their account to transfer money to their friends. However, since funds could not be transferred across different platforms and users are generally reluctant to download so many applications, the development of the market has been obscured. In view of this, the HKMA launched a real-time financial-payment system in 2018, the "Faster Payment System" (FPS), which allows users to initiate payment and

1. HKMA (2019b).
2. HSBC (2019).

transfer funds across banks and different SVF by a registered mobile number or e-mail address.[3] This has successfully connected the dispersed innovations in the market and provided more options to the consumers.

Although the market is undergoing fierce competition, the attitude of the general public is not keen. According to a survey conducted by the Hong Kong Internet Registration Corporation (HKIRC) in 2018, despite a majority of support towards a large-scale adoption of mobile payment in the city, more than half of the respondents stated that concerns over personal cybersecurity risk and privacy issues have hindered them from adopting the technology. Furthermore, around 83% of respondents were of the opinion that the government should adopt more policies to regulate the mobile-payment industry including limiting the collection of personal data and penalizing cybercrime.[4] In view of this, the private sector has developed various technologies to enhance public confidence, such as adopting the two-factor authentication before and after a payment transaction. Some mobile-payment developers also co-operate with smartphone companies so that users can lock their sim card[5] or remove data remotely from their stolen smartphones.[6] Moreover, both Alipay HK and WeChat Pay HK have adopted intelligent real-time security-monitoring systems to analyze suspicious transactions. Once a potentially risky transaction is identified, additional account-protection procedures will be automatically activated to verify the identity of the users or to block such a transaction.[7]

Contrary to such a conservative approach, Mainland China has been actively embracing the innovation and is currently the world's largest mobile-payment user.[8] Payment by smartphones has already become commonplace in China and even taxi drivers would be surprised if one were still to pay by banknotes. Such a transition dated back to 2004 when Alibaba, an e-commerce service provider, established Alipay to provide a better payment solution to their clients. Following the tremendous growth in the smartphone industry, Tencent also decided to take a bite of the market and set up WeChat Pay in 2013, taking advantage of its large customer base as a major social-media-application operator. Since then, the two giants have been fiercely competing against each other through a strong marketing campaign of mobile payment. According to the *Payment System Operations Report* published by the People's Bank of China, back in 2013, there were only 1.674 billion mobile-payment transactions, with a total value of RMB 9.64 trillion.[9] The year of 2018, in contrast, recorded 60.531 billion transactions totalling RMB 277.39 trillion in value, meaning that the transaction amount underwent a 27-fold increase within only five years.[10] Given such heavy reliance on mobile-payment technology, Alipay has adopted innovative measures to enhance customer protection. This includes providing free insurance of up to RMB 1 million to every user, which covers any loss resulted from fraud. The insurance plan could also be upgraded

3. Hong Kong Interbank Clearing Limited (2019).
4. Hong Kong Internet Registration Corporation Limited (2018).
5. Apple (2018).
6. Legislative Council (2018).
7. Alipay HK (2019); WeChat Pay (2019).
8. Statista (2019).
9. People's Bank of China (2014), p. 5.
10. People's Bank of China (2019), p. 4.

with a minimal fee to cover up to RMB 5 million.[11] Also, users are allowed to opt out of instant transferral and choose to delay their remittance for 48 hours. If the deal is later found to be suspicious, users could submit evidence to the police within 48 hours to freeze the transaction.[12] These customer-protection policies have greatly boosted the public's confidence in the technology, but are only offered for the version of Alipay Wallet available in Mainland China.

On the other hand, being the world's largest economy and a well-developed country, the US was much slower in pace. Even though over three-quarters of adults in the US own smartphones,[13] research shows that around 89% of Americans still prefer cash, credit, or debit card over mobile payment, with security concerns being the major issue.[14] In 2018, the mobile-payment user-penetration rate of the US was only 27.4%—much lower than that of China, which is at the top of the league at more than 80%.[15] Similarly, Europe is also slow in adopting the new technology due to their reliance on credit cards. Among the European countries, Sweden has the highest percentage of respondents saying they preferred using mobile payment. Denmark ranks second in terms of the number of citizens who made at least one proximity mobile payment in 2018. It is expected that the number will soar in the coming few years.[16]

2.2 Benefits of Mobile Payment

New technology always comes with convenience. Mobile payment allows customer to pay for goods and services easily by a few clicks of buttons without having to worry about leaving a credit card of a particular bank at home. It also allows friends to share the cost of a dinner without the hassle of dealing with coins. The payment record inside the application also allows users to instantly review their spending or to trace their past expenditure.

Moreover, some operators allow business owners to integrate an incentive or loyalty programme into the mobile-payment application. Coupons will be automatically issued when a customer has made enough spending or when they are near a particular area. Business could also track and analyze customer behaviour easily with the data, which are automatically captured during payment. With such information, they could understand their customers better and improve their products to increase sales.

Third, the use of mobile payment facilitates the movement of funds. Unlike in the old days, when customers would be charged for interbank-fund transfer, no extra fee would be induced when transferring money through most of the mobile applications. In order to compete with these third-party financial platforms, many banks in Hong Kong have also begun to waive such service charges recently, providing customers with a more flexible and friendly investment environment.

11. Alipay (2019).
12. Zhu (2018).
13. Pew Research Centre (2019).
14. Simon-Kucher & Partners (2019), p. 3.
15. PwC (2019), p. 6; McNair (2018).
16. Merchant Savvy (2019).

2.3 Risks of Mobile Payment

There are in general three major risks associated with mobile payment, notably cybersecurity risk, liquidity risk, and data-privacy risk.

Being a product of information technology, it is always a fear that hackers and identity thieves would attack the transaction process in various ways such as phishing or malwares. Outdated or insufficient maintenance of the infrastructure may also attract intrusions that lead to fraud. With little knowledge of the technology, both customers and business owners could only rely on the expertise of the service providers and may not realize the existence of such vulnerabilities until great loss has occurred. Moreover, unlike credit cards, which are always placed safely in the wallet, the smartphone is a multitasking gadget that is frequently used for different purposes. It is therefore common for users to drop their phones in restaurants or public washrooms and this provides opportunities for unscrupulous persons to take advantage of others' property through an unsecured smartphone that contains all the essential credentials to access a bank account.

Other than the above, liquidity is also a major concern. Since mobile-payment operators are usually holding money in trust for users, it is crucial that they have sufficient cash in hand to serve any withdrawal or transferral request in a timely manner. Similarly to traditional financial institutions, failure to meet payment obligations will lead to crisis of confidence. As most of the third-party-payment platforms and financial institutions are highly integrated, such a crisis may also affect the whole financial industry.

Last but not least, customers may also be exposed to data-privacy risk when using mobile payment. In order to effect transaction in a timely manner, service providers usually require customers to open an account to store all data and transaction records. With insufficient control, such information might be used by unauthorized third parties for unwanted purposes. Not only would the customer's daily life be disturbed; it also provides opportunities for identity theft to gain financial advantages illegally.

In view of these risks, it is therefore essential for regulators to establish a stringent regulatory regime to supervise such complex payment activities. A comprehensive framework can not only foster the confidence of the general public, but also facilitate the development of such technology. Hence, the next section will turn to the regulatory requirements of mobile payment in Hong Kong.

3. HONG KONG LAW: RESPONSES TO THE RISKS OF LIQUIDITY AND SECURITY

3.1 Overview

The mobile-payment industry in Hong Kong is currently classified into two categories. The first type, a "stored value facility" (SVF), allows customers to store money in their accounts to make future payments for goods or services or to another person. Customers will be allowed to make payments up to the amount stored in the facility[17] and the unused amount will then be held by the SVF operators.[18] This type of operators is currently regulated by the

17. PSSVFO (Cap. 584), Pt 1, s. 2A.
18. Legislative Council, *supra* note 6.

PSSVFO, which will be looked into in more detail later. On the contrary, a "non-stored value facility" does not require customers to deposit money in advance.[19] It covers platforms that only facilitate the transmission of payment information such as credit-card details to the merchants and does not involve any storage of value. Companies operating these facilities are not required to obtain a licence and are not regulated by the PSSVFO. Instead, the credit-card-issuing banks should comply with the Supervisory Policy Manual Module on "Risk Management of E-banking"[20] issued by the HKMA, which is not the focus of this paper.

In 2015, the Hong Kong Legislative Council (LegCo) passed an Amendment Bill to rename the "Clearing and Settlement Systems Ordinance" as the "Payment Systems and Stored Value Facilities Ordinance" (PSSVFO), which delegates power to the HKMA to oversee all SVFs.[21] In general, the ordinance has provided the HKMA with the power to (1) decide whether a licence should be granted, (2) conduct ongoing supervision of the licensees, and (3) conduct investigation and impose sanctions on licensees when it sees fit. Most importantly, the HKMA will also scrutinize the level of cash in the facilities to ensure that there is adequate protection of the float to prevent any liquidity risk.[22]

As the supervisory body of the SVF, the HKMA has the power to ensure that the SVF complies with the PSSVFO[23] and take action if there is any violation. According to Part 2B of the PSSVFO, the HKMA may request information from licensees and examine its books and transactions. If the HKMA has reasonable cause to believe that the PSSVFO has been contravened, it may conduct investigation on the licensee.[24] If the HKMA is satisfied that the regulated person has contravened the ordinance or opined that the business is carried out in a detrimental manner after an investigation,[25] it may instruct the licensee to take immediate action to rectify the issue or appoint a manager to take over the affair with assistance from the court.[26] For serious offence, the HKMA could restrict the licensee from expanding business or disposing assets, impose sanctions, forbid the licensee from carrying on business, or ultimately revoke the licence.[27] The responsible person may also face penalties including fines and imprisonment.

3.2 The Payment Systems and Stored Value Facilities Ordinance (PSSVFO)

3.2.1 Licensing and Ongoing Supervision

The HKMA has power to assess whether an application for an SVF licence should be accepted and to perform ongoing supervision on the licensees. Part 2 of Schedule 3 to the PSSVFO provides the minimum criteria that an applicant should fulfil before submitting an application. These include: first, the principal business of the applicant is the issue of

19. Cheng (2016).
20. HKMA (2015b).
21. HKMA (2015a).
22. HKMA (2019a).
23. PSSVFO, s. 9.
24. *Ibid.*, s. 33B.
25. *Ibid.*, s. 8ZE.
26. *Ibid.*, s. 8ZR.
27. HKMA, *supra* note 23, p. 39.

the SVF under a SVF licence[28]; and, second, most of the resources will only be used for SVF business.[29] Further, the chief executive, director, and controller of the applicant should be a fit and proper person[30]; and their appointment should only be made after acquiring the HKMA's approval.[31] There should also be in place an appropriate risk-management system[32] and sufficient control to combat against money laundering.[33]

After a licence has been granted, the licensee should observe not only those criteria, but also additional requirements that have been supplemented by the Guideline on Supervision of Stored Value Facility Licensees ("The Guideline").[34] The Guideline gives detailed explanation on the principles that the HKMA adopts to supervise a licensee; for example, a company should properly maintain its documentation for periodic review by independent auditor[35] and at least one-third of the board should be composed of independent non-executive directors to ensure sufficient checks and balances on the company.[36] In general, the HKMA will consider the applicant's overall financial strength, scale of business, effectiveness of risk management, and internal control environment to decide whether a licence should be granted or allowed to stand.

3.2.2 Addressing Liquidity Risk

The HKMA has set out a few requirements on the capital and assets of the SVF to mitigate potential liquidity risk in order to ensure the soundness of the SVF. First, the paid-up share capital of a licensee should not be less than HKD 25 million.[37] Second, it is not allowed to engage in business not relating to the operation of the SVF. This is to ensure that the financial resources of the service provider will not be dispersed, but only applied to the SVF business.[38] The licensee is also forbidden from relying on investment returns from the float as a significant source of income to avoid market risk. If it would like to hold a proportion of the deposit in low-risk financial assets other than cash or bank deposits, it must obtain the HKMA's prior written consent.[39]

In terms of internal control, the HKMA requires the licensee to implement effective liquidity-management policies and controls to manage the float. It should always separate the deposit from funds received from other channels. The account ledgers of all users should be maintained in an accurate and timely manner, and there should always be sufficient funds in the facilities ready for redemption. The licensee should implement a robust system to protect the deposits against claims by other parties such as creditors. This includes establishing an effective trust arrangement to protect the legal rights and priority claims of the float by

28. PSSVFO, Sch. 3, Pt 2, para. 1.
29. *Ibid.*, para. 2.
30. *Ibid.*, para. 3.
31. HKMA, *supra* note 23, p. 18.
32. PSSVFO, Sch. 3, Pt 2, para. 5.
33. *Ibid.*, para. 6.
34. Guideline on Supervision of Stored Value Facility Licensees ("The Guideline").
35. The Guideline, para. 2.2.1.
36. *Ibid.*, para. 3.2.3.
37. PSSVFO, Sch. 3, Pt 2, para. 2.
38. HKMA, *supra* note 23, p. 17.
39. The Guideline, para. 6.4.2.

users during insolvency. Proper legal authorizations should also be in place to ensure a smooth and efficient refund process.[40] If there is a loss of value due to the lack of robustness of the system, the licensee should bear the full loss.[41]

3.2.3 Addressing Cybersecurity Risk

In order to prevent the SVF against cyberattacks and fraud, the licensee must have in place proper risk-management policies and controls that are proportionate to the size and nature of its business.[42] It is the licensee's responsibility to monitor the latest trend in cyberthreats, implement adequate protective measures, and perform periodic testing. The licensee should ensure that (1) it has adequate IT controls, (2) the computer systems are robust, and (3) the operation of the SVF is safe and efficient. In order to achieve this, there should be appropriate segregation of database and access controls to prevent unauthorized access to data.[43] There should also be adequate policies and controls to protect the confidentiality and integrity of the information collected throughout its business. In order to detect fraudulent transactions, the licensee should implement sufficient payment-security controls to ensure the authenticity and traceability of payment transactions. Timely notification should be sent to the customers before completing any high-risk transactions.[44]

3.2.4 Other Requirements

Other than the above, the HKMA will also assess whether the licensee has in place adequate arrangements to supervise and enforce the compliance of its rules. To mitigate any loss resulted from operational disruptions, the HKMA has required the licensee to establish an incident-management framework. This includes timely reporting to the HKMA of any security breaches and instant communication with stakeholders to address their concerns.[45]

Furthermore, while the licensee may outsource parts of its operations to third parties, it should be ultimately responsible for the security, robustness, and stability of the outsourced activity as well as the integrity protection of information of the outsourced service.[46] When any material incidents occur, the licensee should immediately submit information to the HKMA.

3.3 Evaluating the PSSVFO

3.3.1 Security Loopholes

At a brief glance, the PSSVFO seems to cover most of the risks of a mobile-payment business and does give the authority power to enforcement. A study initiated by the Consumer Council also shows that mobile-payment applications in the market generally have in place the basic security precautionary measures. Users will generally receive notification after a

40. *Ibid.*, para. 6.3.
41. *Ibid.*, para. 8.3.5.
42. *Ibid.*, para. 7.1.1.
43. *Ibid.*, para. 7.2.
44. *Ibid.*, para. 7.3.
45. *Ibid.*, para. 7.2.2.
46. *Ibid.*, para. 3.4.2.

transaction and could check their past transaction records.[47] However, despite such seemingly comprehensive regulation, in September 2018, a month after the launch of the FPS, fraudulent cases were reported concerning the use of the mobile-payment device covering an amount of around HKD 180,000.[48] Fraudsters were found to have stolen the victim's personal data, activated the electronic direct-debit-authorization (eDDA) feature of the application, and transferred money from the victims' accounts to their own wallet through the FPS.[49] This reveals the security loophole involving account opening. Many licensees only require customers to provide a mobile number for account opening and to verify their identities with a copy of their identity cards. No other "Know Your Customer" (KYC) procedures are required. It is therefore possible for fraudsters to open an account with a pre-paid sim card and connect it to the victim's bank account with a stolen copy of an ID card and account number. As there are agreements between banks and licensees, the former will not further verify the user's identity and accept any transfer or payment request. Since no instant message has been sent to the users for verification, the victims could only discover such fraud after receiving their financial statements.[50]

Addressing such incidents, the LegCo has raised the question of whether the HKMA would consider making it mandatory for all licensees to adopt two-factor authentication for verifying a user's identity before processing any online transactions. This includes measures such as requiring users to input a one-time password received through instant message or generated by security tokens. The government has, however, replied that, due to the different nature of the SVF businesses, it would not be appropriate for the HKMA to mandate all licensees to adopt such measures. Licensees are only required to implement measures deemed appropriate by themselves. As long as users do not act fraudulently or with gross negligence, they will not be held liable for the unauthorized transactions.[51]

Although the last line of the government's reply does protect the general public from bearing the loss that is not caused by their fault, it does not fully resolve the problem. Some may argue that, since customers would eventually tilt towards licensees with better security measures, and then service providers with insufficient protection would be weeded out by competition, it is not necessary for the government to mandate two-factor authentication. However, it is not uncommon for users who have been attracted by cash rewards to open a mobile-payment account without carefully studying the types of security measures that have been adopted. Such loopholes would not be discovered until another unauthorized transaction occurs, which would further hamper the public's confidence. It is therefore inappropriate for a competent regulator to sit back and wait for the magic of the market, but it should actively take up the responsibility of safeguarding the interest of its citizens. In view of this, the HKMA could take reference from the policies applied in other jurisdictions. In China, users are required to register their identity with their phone numbers.[52] This could prevent fraudsters from opening fake accounts with mobile numbers that cannot be traced.

47. Consumer Council (2016).
48. Hong Kong Business (2018).
49. Ejinsight (2018).
50. Peng (2018).
51. HKSAR Government Press Releases (2018).
52. On.cc (2017).

However, this would place a heavier burden on personal-data protection and should only be implemented after the PDPO has been revised and upheld to a more stringent level. On the other hand, the EU has recently introduced the Second Payment Services Directive (PSD2) with the hope of promoting the European mobile-banking market by establishing a better-regulated business environment. In order to address the additional security risks, strong customer authentication has been made mandatory to all remote-electronic-payment transactions exceeding EUR 30 with few exceptions.[53] It requires operators to implement authentication that comprises two or more elements that are categorized as knowledge, possession, and inherence. The code should be dynamically linked to the transaction and could only be accepted once, and new codes should not be able to be generated based on knowledge of previous codes. Such authentication can only be valid for five minutes and must be blocked if it has been failed five times.[54] These enhanced protective measures are practical and could remediate the loophole created by unsatisfactory KYC and due-diligence work, and should be considered seriously by the HKMA.

3.3.2 Market-Stability Issues

Currently, the PSSVFO has stipulated that only applications with paid-up share capital of not less than HKD 25 million could apply for a PSSVFO licence and, once a licence has been issued, the minimum ongoing capital should also be kept at HKD 25 million. This has attracted criticism from some stakeholders who find this requirement to be too restrictive and impose an unnecessary market-entry barrier[55] compared to other jurisdictions such as in Singapore, where multi-purpose prepaid service providers that hold a stored value of less than SGD 30 million do not need to register with the Monetary Authority of Singapore (MAS). These service providers only have to indicate in their service clearly that they do not require the approval of the MAS and could apply to upgrade its status after the stored value exceeds the threshold. It was said that such a policy could provide small and newly developed players to enter the market and develop their businesses.[56]

In view of this, the HKMA has explained that the intention of the high threshold in Hong Kong is to provide the SVF with a financial buffer to absorb unexpected losses and also any losses in the case of winding-up. As it is important to protect customers and such a requirement is in line with the Multi-purpose Stored Value Card regime, it is reasonable to keep the threshold at such a high level. Moreover, looking at the flourishing SVF market with 13 existing non-bank licensees, it seems that such a requirement is not over-demanding.

However, if the HKMA would like to offer more protection to the mobile-payment users, it could make reference to Google's self-motivated insurance programme. Although Google is not a banking institution, it is keeping the funds in its Goggle Wallet in banks insured by the Federal Deposit Insurance Corporation (FDIC).[57] This means that, if the IT giant fails

53. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 on supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, Art. 16.

54. *Ibid.*, Art. 4.

55. Financial Services and the Treasury Bureau & Hong Kong Monetary Authority (2014).

56. Payment Systems (Oversight) Act (Cap. 222A) (2006), Art. 33; Ejinsight (2016).

57. Woodruff (2015).

one day, the US government would pay the users back up to USD 250,000 without requiring the users to go through legal proceedings. Since a similar "Deposit Protection Scheme" is in place in Hong Kong, which offers protection to bank depositors at HKD 500,000 per scheme member, the government could also consider extending such protection to SVF licensees such that citizens will be more confident to place their money in an SVF.

3.3.3 Hidden Third-Party Risk

From the various incidents that happened, it could be observed that third-party risk also poses a significant threat to the soundness of mobile payment. The fraudulent claims through FPS show that the biggest threat is neither the design nor the maintenance of the system itself,[58] but the banks' or operators' reliance on the identity-verification work performed by third parties to save cost and time. Such risk is not limited to account-opening service providers, but covers any business partners that are in some way connected to the transaction. A good illustration would be the data breach of British Airways in 2018 from which professionals inferred that the incident was caused by the use of embedded code from third-party suppliers during settlement.[59] All these incidents demonstrate how most of the digital-banking and mobile-payment services are highly integrated into each other and the negligence of one party will create a loophole and easily "infect" the whole service chain. It is therefore essential for the regulators and market participants to acknowledge the risk generated from such closely linked business relationships[60] and formulate appropriate third-party risk-management policies and controls.

4. HONG KONG LAW: RESPONSES TO THE DATA-PRIVACY RISK

4.1 Overview

Although there are different types of mobile-payment service providers in the market, as long as the business involves the collection of personal data, all financial facilities are regulated by the "Personal Data (Privacy) Ordinance" (PDPO).[61] The HKMA maintains regular liaison with the Office of the Privacy Commissioner for Personal Data (PCPD),[62] which remains the sole regulator of issues relating to data privacy. All SVF licensees are required to comply with the PDPO and the relevant guidelines issued by the PCPD,[63] such as issues relating to the collection of identity-card numbers and other personal identifiers during account opening.[64] The PDPO itself is a principle-based ordinance that is more instructive rather than prohibitive. It sets out six fundamental principles of data protection that cover the whole life-cycle of the personal data from its collection until destruction.[65] The six major principles are as follows.

58. Mingbao (2018).
59. BBC (2018).
60. Xu (2018).
61. Personal Data (Privacy) Ordinance (Cap. 486) (1996) (PDPO).
62. HKSAR Government Press Releases, *supra* note 51.
63. The Guideline, para. 3.4.4.
64. PCPD (2016).
65. Wong & Zhu (2016), p. 2.

4.2 Major Principles of the Personal Data Protection Ordinance (PDPO)

4.2.1 Principle 1: Purpose and Manner in Data Collection

In general, Principle 1 requires that the data controller should only collect personal data in a lawful and fair way and for a purpose directly related to the activity concerned. The data collection should not be excessive. The data controller bears the responsibility of taking reasonable steps to inform or notify customers of (1) the purpose of the collection, (2) whether such a collection is compulsory, (3) whom their data may be transferred to, (4) their right to correct the data, and (5) the identity of the individual handling the request.[66] With reference to past complaints handled by the Administrative Appeals Board (AAB), the Commissioner has supplemented that the clauses covering the information of possible data transferees should not be too loose. Terms such as "Our Partner" and "third parties" are not allowed.[67] In order to determine whether the notification is effective, the Commission will assess how the information is presented and whether the language used is easily comprehensible and intelligible.[68]

Moreover, before the collection of data, the data controller should consider whether such a collection is necessary and whether there are any other less privacy-intrusive ways to achieve the same purpose.[69] If ID information is to be collected, it should follow the "Code of Practice on the Identity Card Number and other Personal Identifiers," which states that licensees should not compulsorily require the users to submit a copy of their HKID or ID number unless (1) required by law, such as for anti-money-laundering purposes, (2) for the prevention of crime, (3) to advance the interest of the ID holder, (4) to safeguard against any damage to the holder, and (5) to establish a legal right.[70]

4.2.2 Principle 2: Data Accuracy and Retention

Principle 2 requires a data controller to take practicable steps to ensure the accuracy of personal data and the information should not be kept for longer than is necessary to fulfil its purpose.[71] A bank was found to be in breach of Principle 2 and S26(1) of the PDPO by retaining a customer's bankruptcy information for 99 years. The bank was then required to revise its policy.[72]

4.2.3 Principle 3: Data Use

Principle 3 states that the personal data must only be used for the purpose stated during collection. If the data controller would like to use it for a new purpose, it must obtain explicit and voluntary consent.[73] This is one of the most controversial principles and receives the largest number of complaints, as it is common for data controllers to frame the purpose as wide as possible for flexibility. The Commissioner will, however, not only look at the

66. PDPO, Sch. 1, s. 1.
67. PCPD (2012).
68. Wong & Zhu, *supra* note 65, p. 63.
69. *Ibid.*, p. 38.
70. PCPD, *supra* note 64, para. 2.3.
71. PDPO, Sch. 1, s. 2.
72. PCPD (2011a).
73. PDPO, Sch. 1, s. 3.

wording used, but also give fair consideration to the reasonable expectation of the customer to determine whether new consent should be obtained.[74] Moreover, a licensee should not transfer data that are not necessary for the transferring purpose. Excessive disclosure to a third party might violate Principle 3, as the latter might utilize the information for other purposes. A bank has been found to contravene such a regulation by providing personal data from credit cards to an insurance company for marketing.[75]

4.2.4 Principle 4: Data Security

In general, the data controller should take practicable steps to protect the personal data from unauthorized access or processing.[76] This includes the control of people accessing the data online and the physical protection of data storage. The more sensitive the data obtained, the higher the degree of care required.[77] If a third party is engaged to process the data, the data controller must adopt contractual or other methods to prevent unauthorized access. The PDPO, however, does not mandatorily require the data controller to report any data breach to the Commissioner. It has instead issued a guidance document that gives recommendation on steps to be followed after a data breach.[78]

4.2.5 Principle 5: Openness of Data

The data controller must take practicable steps to disclose its personal-data policies and practices to the public. This includes informing the public of the personal data held by the company and also the purpose of such storage.[79] Although it is not mandatory, the controllers are recommended to issue a Privacy Policy Statement that covers the data-retention policy, data-security measures, and data-breach-handling methods, and is available to the public in an easily accessible manner.[80]

4.2.6 Principle 6: Data Access and Correction

The data controller must allow its customer to access and make correction to the data if the information is inaccurate.[81] However, such a request should not be accepted if the requester's identity is in doubt.[82]

4.3 Evaluating the Data-Protection Regime

Although there seems to be comprehensive coverage of the PDPO, there are actually a few loopholes in the ordinance that are urgently calling for amendments to catch up with the latest development of the market.

74. PCPD (2010).
75. PCPD (2011b).
76. PDPO, Sch. 1, s. 4.
77. Wong & Zhu, *supra* note 65, p. 104.
78. PCPD (2019a).
79. PDPO, Sch. 1, s. 5.
80. Wong & Zhu, *supra* note 65, p. 124.
81. PDPO, Sch. 1, s. 6.
82. Wong & Zhu, *supra* note 65, p. 146.

4.3.1 Lack of Mandatory Notification for Data Breach

As mentioned above, under Principle 4, a guidance document has been issued to set out recommendations on what a licensee should do in case of a data breach, such as notifying the privacy Commissioner and data subjects. However, the document does not carry the force of law and there are no penalties or sanctions on the controllers who fail to make such notification. This drawback was manifested in the recent data breach of Cathay Pacific. The breach happened in March 2018 and affected 9.4 million passengers, but the carrier only reported the breach in October 2018, even though it had already confirmed such a leakage in early May.[83] This unreasonable reporting duration of seven months has drawn serious criticism from the public, as such delays have hindered customers from taking any countermeasures. A strong voice has been heard, requesting the government to revise the PDPO and make such notification compulsory.

With respect to this problem, other jurisdictions have more stringent regulations. The EU adopted the General Data Protection Regulation (GDPR) in 2018, which requires both data controllers and data processors to report any data breach within 72 hours to the authority after the breach is discovered.[84] If the breach is likely to result in a high risk to the rights and freedom of customers, the data controller is also obliged to notify the data subject of such a breach.[85] Under the South Korean privacy data law, the Personal Information Protection Act (PIPA), which is one of the world's strictest privacy regimes, stipulates that the data controller must notify the data subject without delay when a breach occurs. If the breach exceeds the scale prescribed by Presidential Decree, the data controller must report to the authority and the authority will provide technical assistance to prevent further damage.[86] The Notifiable Data Breaches Scheme in Australia also mandates data breaches that are likely to result in serious harm to be reported to the Commissioner and the data subject.[87]

4.3.2 Insufficient Penalty

Although the PDPO has been enacted for a certain period of time, it lacks the teeth to regulate the industry due to the minimal penalty it posts on any offender. Under the current regulatory regime, any breach of the PDPO will not automatically constitute an offence or lead to any penalty. It is an offence only when a data controller refuses to rectify the situation after the PCPD issues an enforcement notice against its breach of the ordinance or intentionally repeats the same breach after complying with an enforcement notice.[88] Moreover, the maximum penalty that the PCPD can impose on an offender is only limited to two years of imprisonment and a fine of HKD 50,000. If more than one enforcement notice has been breached, the penalty would become three years of imprisonment and a fine of HKD 500,000.[89]

83. Lum & McCarthy (2018).

84. Regulation (EU) 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 (GDPR), Art. 33.1.

85. GDPR, Art. 34.1.

86. Personal Information Protection Act (PIPA Korea), Art. 34.

87. Office of the Australian Information Commissioner (2019).

88. PDPO, s. 50A.

89. PCPD (2019b).

The penalties under the PDPO are minimal compared to the sanction imposed by the GDPR in which a breach could trigger the authorities to impose a fine of 4% of the total worldwide annual turnover or EUR 20 million.[90] The maximum penalty in Korea in the case of a data breach also reaches KRW 500 million if the data controller is to be blamed for the incident[91] and any fraudulent offence relating privacy data might result in imprisonment limited to ten years and a fine not exceeding KRW 100 million.[92] Strict enforcement of such regulations has been observed. In 2016, KRW 42 million was levied from five Korean corporations as fines for negligence in handling personal data, and colleges and hospitals were fined up to KRW 157 million in 2014 for breach of the PIPA.[93] Such a big deviation in fines indicates that the trivial penalties in the PCPD have no avail at all and should be revised and strengthened.

4.3.3 Insufficient Coverage

As illustrated above, under the current PDPO, data controllers are held to be ultimately responsible for any breach of the ordinance. If there is any transfer of data to third parties for processing, those processors are only liable for the contractual arrangement between the data controllers and the processors.[94] This might not be fair, as it is difficult for the data controllers to exert control on how the data processors handle the data. It is therefore reasonable that these processors should also be held equally liable for any breach, but not only limited to the responsibility under a contract.

Unlike in Hong Kong, the GDPR has already imposed liability on data processors that are now directly responsible for any breach of regulation. They are especially required to maintain records of processing, ensure the processing of data secured, and report any data breaches to the authority.[95] Customers could bring an action directly against these data processors if they are found to breach the GDPR. In Korea, there is no difference between data controllers and processors, and all parties are directly liable to uphold the PIPA.[96] By increasing the accountability of data processors, it is likely that they will be more motivated to co-operate with data controllers to ensure compliance with law and this will therefore improve the soundness of the industry.

4.3.4 Additional Rights that Should Be Protected

Compared to the PDPO in Hong Kong, the GDPR also grants additional protection to the rights of its citizens. This includes the right to erasure (right to be forgotten)[97] and the right to restriction of processing.[98] Currently, there are no such rights in Hong Kong and data controllers are only restricted by Principle 2 of the PDPO, which stipulates that any personal

90. GDPR, Art. 83.
91. PIPA Korea, Art. 34-2.
92. PIPA Korea, Art. 70.
93. Ministry of the Interior and Safety (2019).
94. PDPO, Sch. 1, s. 4.2.
95. GDPR, Arts 30, 32, 33.
96. PIPA Korean, Art. 2.5.
97. GDPR, Art. 17.
98. GDPR, Art. 18.

data shall not be retained for a period longer than necessary. However, according to a study in October 2016, the Consumer Council discovered that it is the practice of three mobile-payment service providers to retain users' data for up to seven years and one of them to keep the data permanently.[99] This shows that the PDPO fails to protect the subsequent rights of users. The information submitted for account opening might, as far as prior consent has been given, still be used for the advertising purpose or transferred to third parties even after the accounts have been left dormant or deleted. To tackle such a problem, the GDPR allows users to erase their personal data and restrict further data processing if such data are considered unnecessary in relation to the purposes of collection or when consent has been withdrawn. Service providers are only allowed to keep those data if there is any "legitimate interest."[100] Such a rule not only gives a rigid deadline to service providers in storing transaction information, which should converge to the accounting or legal requirements of the jurisdiction, but also allows users to erase themselves completely from databases that have no transaction history or to flexibly amend their privacy consent. Other than the above, it is also reasonable to allow data subjects to restrain their own data from being processed if they are doubtful on the accuracy of data or when the processing of such data is contested to be unlawful. The government should consider extending protection to such rights if the PDPO is to be amended.

4.3.5 Other Recommendations on Data Protection

Other than the shortcomings illustrated above, the government could also consider additional steps or plans that could better protect the personal data of consumers.

First, the government could consider classifying personal data into different groups according to their sensitivity. Currently, all personal data are treated in the same way in Hong Kong, with ID numbers being given a slightly stricter protection. The GDPR has currently classified personal data into two types where information such as ethnic origin and biometric data belong to "special categories" and the processing of such data is only allowed under specific circumstances.[101] Such a categorization allows institutions to tailor different security measures and offer a higher level of protection to data with a more "sensitive" nature.

Second, the Hong Kong government could observe the "Decode Project" initiated by the European Commission and being tested out in Barcelona and Amsterdam. It is a pilot scheme that aims to give data owners control of how the data are accessed and used by utilizing the latest blockchain technology. Private data would be searchable on public domains but only those parties that have been granted permission could access such information. The ultimate goal is to create a decentralized ecosystem that allows users to manage the data they generate in real time without relying on a centralized third party.[102] It is hoped that such an innovation could uphold data protection and foster confidence in digital transactions.

---

99. Consumer Council, *supra* note 47.
100. GDPR, Art. 17.
101. GDPR, Art. 9.
102. Decode Project (2019); European Commission (2019).

5. CONCLUSION

As a main form of FinTech, mobile payment is a fast-growing industry, with the great potential of rewriting the ecosystem and business model of the traditional financial industry. While it brings important benefits, there are also various risks, in terms of liquidity, security, and data privacy, which call for adequate regulatory responses.

In general, Hong Kong has gradually established a regulatory framework for mobile payment, including the PDPO to address the issue of data protection and the PSSVFO to deal with the issues of liquidity and security. While this regulatory framework represents great efforts made by Hong Kong to respond to the risks of mobile payment, there is room for further improvement. For instance, it is necessary to amend the PDPO to date and address the numerous vulnerabilities identified in this paper to provide users with sufficient protection on personal-privacy data. In terms of the newly implemented PSSVFO, the government should consider the practicability of strengthening the customer-authentication requirement as well as issuing more guidelines to assist the industry in mitigating third-party risk. By providing a sound and effective regulatory environment, concerns over the various risks of mobile payment will be alleviated, which will help enhance public confidence in embracing the mobile-payment technology and promote better development of the market.

REFERENCES

Alipay (2019) "Shenme Shi Zhanghu Anquan Xian? Baozhang Fanwei Shi Shenme? [What Is Account Security Insurance? What Is the Insurance Coverage?]," https://cshall.alipay.com/lab/help_detail.htm?help_id=510475 (accessed 1 October 2019).

Alipay HK (2019) "Account Security," https://www.alipayhk.com/en/account-security (accessed 1 October 2019).

Apple (2018) "Set up a SIM PIN for Your IPhone or IPad," https://support.apple.com/zh-hk/HT201529 (accessed 1 October 2019).

BBC (2018) "British Airways Breach: How Did Hackers Get In?," 7 September, https://www.bbc.com/news/technology-45446529 (accessed 1 August 2019).

Cheng, Henry (2016) "Part 1: Smart Tips on Using Stored Value Facilities," https://www.hkma.gov.hk/eng/key-information/insight/20160823.shtml (accessed 1 August 2019).

Consumer Council (2016) "Get to Know Your Data Protection Rights before Using Mobile Payment Services," https://www.consumer.org.hk/ws_en/news/press/480/mobile-payment-services.html (accessed 1 August 2019).

Decode Project (2019) "Have More Questions," https://decodeproject.eu/have-more-questions (accessed 1 August 2019).

Ejinsight (2016) "Payment System Regulations: Blessing or Curse for Mobile Sector?," http://www.ejinsight.com/20160928-payment-system-regulations-blessing-or-curse-for-mobile-sector/ (accessed 1 August 2019).

Ejinsight (2018) "HKMA Receives Complaints of Fraudulent Use of Newly Launched FPS," http://www.ejinsight.com/20181025-hkma-receives-complaints-of-fraudulent-use-of-newly-launched-fps/ (accessed 1 August 2019).

European Commission (2019) "Decentralised Citizens Owned Data Ecosystem," https://cordis.europa.eu/project/rcn/206387/factsheet/en (accessed 1 August 2019).

Financial Services and the Treasury Bureau & Hong Kong Monetary Authority (2014) "The Proposed Regulatory Regime for Stored Value Facilities and Retail Payment Systems in Hong Kong Consultation Conclusion," https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2014/20141031e4a1.pdf (accessed 1 August 2019).

HKMA (Hong Kong Monetary Authority) (2015a) "Regulatory Regime for Stored Value Facilities and Retail Payment Systems Commences Operation," https://www.hkma.gov.hk/eng/key-information/press-releases/2015/20151113–3.shtml (accessed 1 August 2019).

HKMA (2015b) "Supervisory Policy Manual TM-E-1: Supervision of E-banking," https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-E-1.pdf (accessed 1 August 2019).

HKMA (2019a) "Explanatory Note on Licensing for Stored Value Facilities," https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/retail-payment-initiatives/Explanatory_note_on_licensing_for_SVF.pdf (accessed 1 August 2019).

HKMA (2019b) "Register of Stored Value Facility Licensees," https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/regulatory-regime-for-svf-and-rps/regulation-of-svf/register-of-svf-licensees.shtml (accessed 1 August 2019).

HKSAR Government Press Releases (2018) "LCQ21: Regulation of Third-party Payment Platforms," https://www.info.gov.hk/gia/general/201806/20/P2018062000299.htm (accessed 1 August 2019).

Hong Kong Business (2018) "Hong Kong Suspends E-wallet Top-Ups Amidst Fraud Reports in Blow to Smart Banking Push," https://hongkongbusiness.hk/financial-services/news/hong-kong-suspends-e-wallet-top-ups-amidst-fraud-reports-in-blow-smart-banki (accessed 1 August 2019).

Hong Kong Interbank Clearing Limited (2019) "FPS," https://fps.hkicl.com.hk/eng/fps/index.php (accessed 1 August 2019).

Hong Kong Internet Registration Corporation Limited (2018) "HKIRC Announces the Results of the 'Mobile Payment: Digital Transformation from Customers to Merchants' Survey," https://www.hkirc.hk/content.jsp?id=63#!/&in=/company_info/pressrelease.jsp?item=535 (accessed 1 August 2019).

HSBC (2019) "PayMe Help," https://payme.hsbc.com.hk/help (accessed 22 November 2019).

Legislative Council (2018) "E-wallets in Hong Kong," https://www.legco.gov.hk/research-publications/english/essentials-1718ise08-e-wallets-in-hong-kong.htm#endnote7 (accessed 1 August 2019).

Lum, Alvin, & Simone McCarthy (2018) "Cathay Pacific Data Leak: Airline Warns Customers to Guard against Phishing Attempts," *South China Morning Post*, 28 October, https://www.scmp.com/news/hong-kong/law-and-crime/article/2170573/cathay-pacific-data-leak-airline-warns-customers-guard (accessed 1 August 2019).

McNair, Corey (2018) "Global Proximity Mobile Payment Users," https://www.emarketer.com/content/global-proximity-mobile-payment-users (accessed 1 August 2019).

Merchant Savvy (2019) "30 Amazing Stats Demonstrating the Unstoppable Rise of Mobile Payments Globally," https://www.merchantsavvy.co.uk/mobile-payment-stats-trends/ (accessed 1 August 2019).

Mingbao (2018) "Dianzi Qianbao Xian Loudong, Shimin Bei Touqian Baojing, Jinguanju Jiaoting Dianzi Zhijie Kouzhang Shouquan Fuwu [The Citizens' Money Was Stolen Because of Vulnerabilities in E-wallet, HKMA Has Suspended the eDDA Service]," 25 October, https://news.mingpao.com/pns/經濟/article/20181025/s00004/1540405551317/電子錢包現漏洞-市民被偷錢報警-金管局叫停電子直接扣帳授權服務 (accessed 1 August 2019).

Ministry of the Interior and Safety (2019) "Administrative Penalties," https://www.privacy.go.kr/eng/enforcement_02.do (accessed 1 August 2019).

Office of the Australian Information Commissioner (2019) "When to Report a Data Breach," https://www.oaic.gov.au/privacy/notifiable-data-breaches/when-to-report-a-data-breach/ (accessed 1 August 2019).

On.cc (2017) "Peihe Neidi Dianhua Shimingzhi, Gangren Yonghu 7 Yueqian Xu Dengji [Hong Kong Users Must Register before July to Cooperate with the Telephone Real-Name System in Mainland China]," 1 February, https://hk.on.cc/hk/bkn/cnt/news/20170201/bkn-20170201000458157–0201_00822_001.html (accessed 1 August 2019).

PCPD (Privacy Commissioner for Personal Data) (2010) "The Collection and Use of Personal Data of Members under the Octopus Rewards Programme Run by Octopus Rewards Limited," https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R10_9866_e.pdf (accessed 1 August 2019).

PCPD (2011a) "Prolonged Retention of Customers' Bankruptcy Data by Hang Seng Bank Limited," https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R11_6121_e.pdf (accessed 1 August 2019).

PCPD (2011b) "Transfer of Customers' Personal Data by CITIC Bank International Limited to Unconnected Third Parties for Direct Marketing Purposes," https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R11_1745_e.pdf (accessed 1 August 2019).

PCPD (2012) "The Collection and Use of Personal Data of Members under the MoneyBack Program Run by A.S. Watson Group (HK) Limited through 'PARKnSHOP'," https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R12_3888_e.pdf (accessed 1 August 2019).

PCPD (2016) "Code of Practice on the Identity Card Number and Other Personal Identifiers," https://www.pcpd.org.hk/sc_chi/files/faq/picode_e.pdf (accessed 1 August 2019).

PCPD (2019a) "Guidance on Data Breach Handling and the Giving of Breach Notifications," https://www.pcpd.org.hk//english/resources_centre/publications/files/DataBreachHandling2015_e.pdf (accessed 1 August 2019).

PCPD (2019b) "The Ordinance at a Glance," https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html (accessed 1 August 2019).

Peng, Lifang (2018) "Wudingxiang Xuetang: Zhuanshukuai Jie Dianzi Qianbao Loudong, Sanzhao Zibao Fang Hukou Beidao [FPS Uncovering Vulnerabilities in E-wallet, Three Ways to Prevent the Account from Being Stolen]," *Mingbao*, 28 October, https://ol.mingpao.com/ldy/cultureleisure/culture/20181028/1540663773788/無定向學堂-轉數快揭電子錢包漏洞-三招自保防戶口被盜 (accessed 1 August 2019).

People's Bank of China (2014) "2013 Nian Zhifu Tixi Yunxing Zongti Qingkuang [Payment System Operations Report in 2013]," http://www.pcac.org.cn/Upload/image/20170519/20170519085324_35095.pdf (accessed 1 August 2019).

People's Bank of China (2019) "2018 Nian Zhifu Tixi Yunxing Zongti Qingkuang [Payment System Operations Report in 2018]," http://www.gov.cn/xinwen/2019–03/20/5375401/files/1e1a87e02453432ab032ae5187b7804a.pdf (accessed 1 August 2019).

Pew Research Centre (2019) "Mobile Fact Sheet," https://www.pewinternet.org/fact-sheet/mobile/ (accessed 1 August 2019).

PwC (2019) "It's Time for a Consumer-Centred Metric: Introducing 'Return on Experience'," https://www.pwc.com/gx/en/consumer-markets/consumer-insights-survey/2019/report.pdf (accessed 1 August 2019).

Simon-Kucher & Partners (2019) "How Behavioral Science Can Unleash Digital Payments Adoption," https://www.simon-kucher.com/sites/default/files/2018–12/SimonKucher_Report_Payment%20Adoption_Final_0.pdf (accessed 1 August 2019).

Statista (2019) "Mobile Payments Worldwide—Statistics & Facts," https://www.statista.com/topics/4872/mobile-payments-worldwide/ (accessed August 2019).

WeChat Pay (2019) "Account Security," https://pay.wechat.com/en_hk/safety.shtml (accessed 1 October 2019).

Wong, Kai-yi, & Guobin Zhu (2016) *Personal Data (Privacy) Law in Hong Kong: A Practical Guide on Compliance*, Hong Kong: City University of Hong Kong Press.

Woodruff, Mandi (2015) "Google Wallet Funds Are Now FDIC-Insured," *Yahoo Finance*, 20 April, https://finance.yahoo.com/news/google-wallet-venmo-paypal-fdic-insurance-215842545.html (accessed 1 August 2019).

Xu, Jialong (2018) "Disanfang Fengxian Yu Heike Kechengzhiji [Third-Party Risk Gives Hackers a Chance]," *Hong Kong Economic Journal*, 5 November, https://www1.hkej.com/features/article?q=%23%E8%BD%89%E6%95%B8%E5%BF%AB%E6%99%82%E4%BB%A3%23&suid=3966743977 (accessed 1 October 2019).

Zhu, Yinling (2018) "Zhifubao Shengji Yanshi Daozhang, Bei Zhapian Ke Yuanlu Tuihui [Alipay Upgraded the Delayed Remittance, Fraudulent Payments Can Be Returned]," *Xinhuanet*, 22 August, http://www.xinhuanet.com/fortune/2018–08/22/c_1123307380.htm (accessed 1 October 2019).