Image: d3sign / Moment / Getty Images

Stored value facilities: licensing and privacy in Hong Kong

Privacy Commissioner issues statement as first SVF licences are granted.

On 25 August 2016, the Hong Kong Monetary Authority ('HKMA') announced that it had granted five stored value facility ('SVF') licences[1], the first licences granted by the HKMA under the Payment Systems and Stored Value Facilities Ordinance (Cap. 584) ('PSSVFO'). On the same date, the Hong Kong Privacy Commissioner ('PC') issued a statement setting out advice on the collection of personal data by SVF operators in light of the sensitive data that may be involved[2].

SVFs and retail payment systems

On 13 November 2015, the new regulatory regime for SVFs and retail payment systems ('RPS') came into operation under the PSSVFO. Under the PSSVFO: (a) issuers of both device and non-device based multi-purpose SVFs must obtain a licence from the HKMA (note that licensed banks will already be deemed to have the necessary licence to carry on an SVF business, and single-purpose SVFs are not subject to the licensing requirements[3]); and (b) the HKMA has the power to designate RPSs that will be subject to its oversight[4]. For further details on the PSSVFO, please see our previous articles published in this publication in October 2013[5] and November 2014[6] respectively, alongside another on our firm website[7].

The provisions concerning the application and processing of SVF licences and the designation of RPSs came into operation on 13 November 2015. SVF operators were provided with a 12 month grace period in order to obtain the required SVF licence. The grace period comes to an end on 13 November 2016. From 13 November 2016 onwards, it will be an offence to operate a multi-purpose SVF without a licence in Hong Kong.

Personal data protection

SVF operators' collection of personal data from consumers should be no more than necessary to provide services. The more an operator collects, the greater the risk of being in breach of the Personal Data (Privacy) Ordinance (Cap. 486) ('PDPO') or being vulnerable in the event of a cyber attack.

SVF operators are reminded to fully comply with the PDPO requirements (e.g. on notifications, direct marketing, security and data access/correction requests, etc). The PC also recommends:

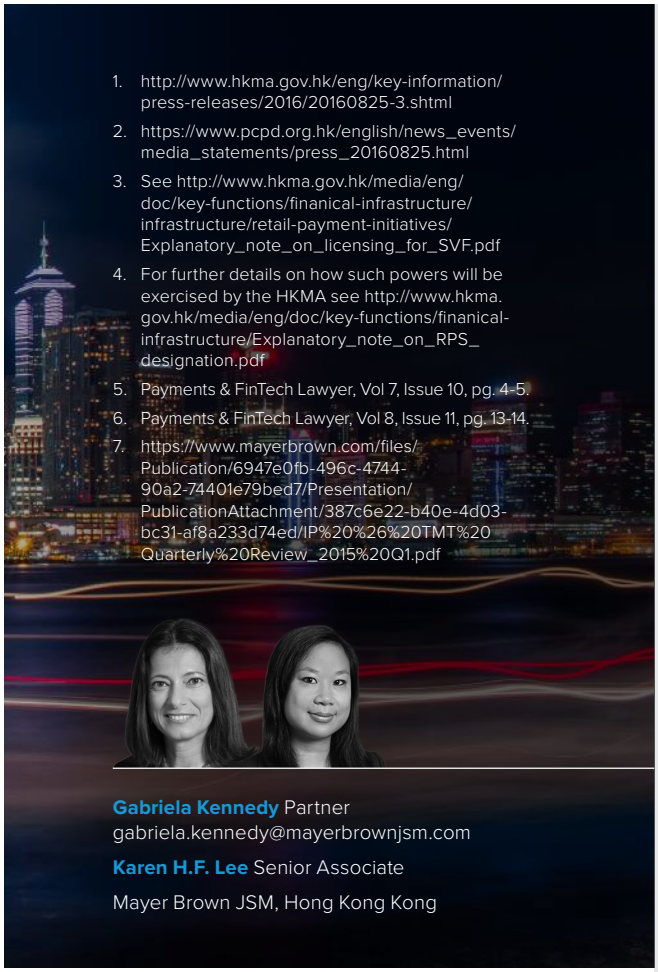
(a) Privacy should be the default starting position of SVFs, and users should be given the option to decide what personal data can be accessed or collected by the operator. Users should be allowed to withdraw their consent at any time, without prejudicing their right to use the SVF, to the extent possible. This obligation to minimise the amount of personal data collected is of course subject to the licensee's AML obligations under the PSSVFO.

(b) SVF operators are advised to be transparent about the data collected, how it will be used and to whom it will be transferred. Such information must be presented to customers in compliance with the PDPO, and in a simple, user-friendly manner.

(c) If an SVF operator intends to use the personal data of a customer for any purpose not directly related to the payment service, then it should obtain the explicit consent from the relevant customers. This recommendation goes beyond simply obtaining the customers' express consent for use of their personal data in direct marketing, and could apply to any purpose outside of the payment service.

(d) SVF operators should carry out formal risk assessments on a regular basis to ensure the level of security used to safeguard the personal data they hold is commensurate with the types of data held, i.e. the more sensitive the personal data, the greater the security measures.

(e) SVF operators that engage third party agents to process personal data on their behalf, must utilise either contractual or other means to ensure that the personal data transferred to the third party agent are not kept longer than necessary,



1. http://www.hkma.gov.hk/eng/key-information/press-releases/2016/20160825-3.shtml
2. https://www.pcpd.org.hk/english/news_events/media_statements/press_20160825.html
3. See http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/retail-payment-initiatives/Explanatory_note_on_licensing_for_SVF.pdf
4. For further details on how such powers will be exercised by the HKMA see http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Explanatory_note_on_RPS_designation.pdf
5. Payments & FinTech Lawyer, Vol 7, Issue 10, pg. 4-5.
6. Payments & FinTech Lawyer, Vol 8, Issue 11, pg. 13-14.
7. https://www.mayerbrown.com/files/Publication/6947e0fb-496c-4744-90a2-74401e79bed7/Presentation/PublicationAttachment/387c6e22-b40e-4d03-bc31-af8a233d74ed/IP%20%26%20TMT%20Quarterly%20Review_2015%20Q1.pdf

Gabriela Kennedy Partner
gabriela.kennedy@mayerbrownjsm.com
Karen H.F. Lee Senior Associate
Mayer Brown JSM, Hong Kong Kong

and safeguarding measures are implemented by the third party agent to prevent unauthorised or accidental access, processing, erasure, loss or use of the data.

Conclusion

The expiry of the grace period for operating a multi-purpose SVF without a licence is fast approaching. Such operators must commence the process of obtaining a SVF licence as soon as possible. If a licence is not issued by 13 November 2016, then the relevant SVF business will need to consider contingency plans. The operation of a multi-purpose SVF business after 13 November 2016, without a licence, could give rise to a maximum fine of HKD $1,000,000 and five years imprisonment upon conviction on indictment.

SVF operators should also carry out a privacy due diligence exercise to ensure that their internal procedures are in-line with the PDPO and their security measures are sufficient. Headlines regarding PC investigations, customer complaints or cyber attacks could not only cause irreparable damage to a company's reputation, but could also weaken public confidence in m-payments and e-wallets, and hinder the general public uptake of new payment methods.

FCA identifies concerns with insurance sector use of big data but decides against full market study

The UK's Financial Conduct Authority ('FCA') published on 21 September 2016 its feedback statement on its Call for Input on the use of big data in the retail insurance sector; in its feedback statement the FCA highlights both positive consumer outcomes and concerns about insurers' use of big data, though ultimately the FCA has decided not to launch a full market study into the area at the present time.

The FCA describes positive outcomes for consumers from insurers' use of big data as including the development of new products and streamlining processes. However, the FCA expresses concern that the use of big data could alter insurance firms' pricing practices, leading to increased prices for certain consumers as firms identify ways in which to charge more, and that firms may as a result of big data change how they assess risks and thus certain categories of consumers will find it harder to obtain insurance. "These concerns can be mitigated by firms complying with data protection, consumer and competition law," believes Simon Stokes, Partner at Blake Morgan. "The FCA can also intervene itself through its powers under FSMA (e.g. its rule-making powers and powers over firms' permissions) and as a concurrent competition regulator."

Despite deciding not to launch a full market study, the FCA intends to remain alert to developments and is carrying out some measures in this area; for example it will conduct a separate examination of the pricing practices of a limited number of firms in the retail general insurance sector.

"I'm pleased the approach is currently light touch - there have been a lot of alarmist statements about how big data could be used to unlawfully price differentiate between customers and be used to deny insurance coverage, for example," said Stokes. "There clearly isn't enough evidence to persuade the FCA to act at present and in any event consumers have strong redress under both data privacy law, which will become stronger once the EU General Data Protection Regulation applies in 2018, and, if anti-competitive conduct occurs, through competition law."

"Insurance companies, which are increasingly using big data - gleaned from social media, loyalty cards, aggregator sites and other sources - to determine risk profiles and set premiums, can rest a little easier given that the FCA has decided not to undertake a full market study or make a reference to the Competition and Markets Authority," adds Tim Wright, Partner at Pillsbury LLP. "However the European Commission is still expected to press on with a call for information on big data this year, as part of its digital single market consultations, and both the French and German competition authorities are expected to launch investigations into the impacts of big data for competition in the next few months."