

The Payment Services Act -

A unique risk-based approach to regulation or an overly complicated set of standards?

June 2020



FINTRAIL

trdc
Smarter Screening

In January 2020 the anticipated Payment Services Act ('PSA') came into force in Singapore. According to the Monetary Authority of Singapore ('MAS') the act is:

'A forward looking and flexible framework for the regulation of payment systems and payment service providers in Singapore. It provides for regulatory certainty and consumer safeguards, while encouraging innovation and growth of payment services and FinTech.'

In this paper we look to understand the genesis of the PSA, what approach has been taken to licensing new payment methods, what are the differences to the approach taken in Europe, and whether the implementation of the PSA in Singapore will succeed in promoting innovation.

“An Electronic Payments Society.”

MAS' desire to revise the regulatory landscape has been ongoing for a number of years. In August 2016 the regulator published a paper suggesting modernising the regulatory framework, making it flexible enough to cater for disruptive technologies emerging in the payments and remittance fields. The move followed MAS Managing Director Ravi Menon's announcement of the agency's plans to push for “an Electronic Payments Society.”

Just one year later in November 2017, MAS released another paper on the proposed Payment Services Act. It specifically outlined that it was working toward regulating cross-border money transfers, e-money issuance and digital currency services, among other things. The regulator stressed that it aimed to improve user and merchant protection, create space for the growth of the fintech-friendly ecosystem, and bolster cybersecurity.

In November 2018, MAS published the finalised edition of the PSA.





The new licensing regime

Prior to the roll out of the PSA, those entities operating in the payments space in Singapore were largely regulated under the Money-Changing and Remittance Businesses Act (Cap. 187) and the Payment Systems (Oversight) Act (Cap. 222A). With the payment services landscape continuing to evolve over the years, new risks and payment methods have also emerged which were not adequately accounted for under the previous regulatory framework.


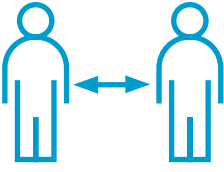





The PSA seeks to replace these previous frameworks and widen the scope of regulation by:

- providing a regulatory structure that recognises the growing convergence across payment activities;
- expanding the scope of MAS to include more types of payment services such as digital payment tokens and merchant acquisition; and
- adopting a modular and risk-focused regulatory structure, allowing rules to be tailored to the scope of the services being offered.

Four key risks will be targeted by the new legislation:

①	②	③	④
			
Loss of customer money	Money laundering & Terrorist financing	Lack of interoperability	Technology and cyber risks

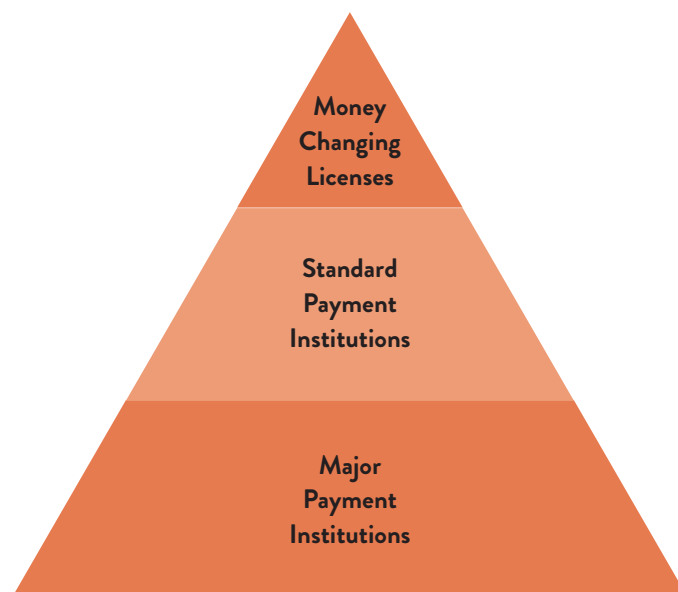
The following is a high level overview of the licensable activities under the PSA:

①	②	③	④
			
Account issuance (e.g. e-wallet)	Domestic transfer (e.g. payment gateway)	Cross-Border Transfer (e.g. remittance)	Merchant Acquisition (e.g. acquiring bank)
⑤	⑥	⑦	
			
E-money issuance (e.g. stored value cards / tokens)	Digital Payment Token (e.g. Bitcoin)	Money Changing (e.g. currency exchange)	

Certain payment services are removed from the scope of the PSA's regulatory regime. Examples include:

①	②	③
		
Limited purpose e-money (e.g. loyalty cards / gift cards)	Limited purpose virtual currency (e.g. in game assets)	Exempt entities under the Securities and Futures Act and the Financial Advisers Act

MAS will issue three types of licenses. The requirements for obtaining each of them are different and depend on the risks associated with the scope and scale of the services:



The narrowest regulation will apply to “money-changing licensees”, typically small businesses offering OTC services with limited risks.

“Standard payment institutions”, the second group, may provide a combination of payment services below certain thresholds and the regime for them will be relatively light to encourage innovation.

“Major payment institutions”, which are the third class of licensees, will be subject to wider and stricter regulations, given the greater risks due to the scale of their operations.

Four key risks will be targeted by the new legislation:

1. Loss of customers’ money,
2. Money laundering or terrorist financing risks,
3. Fragmentation and lack of interoperability across payment solutions, and
4. Technology risks, including cyber risks.

The case for crypto

The PSA puts Singapore in line with Japan, Malta, Switzerland and a few other countries that have enacted regulations on cryptocurrency. The Act comes into force in line with a global push to comply with the requirements on crypto assets mandated by the Financial Action Task Force (FATF). In a bid to promote Singapore as an attractive hub for crypto players, the PSA seeks to both clarify and tighten regulatory requirements. In particular, all providers of digital payment token services in Singapore will have to meet the country’s anti-money laundering (AML) and counter-terrorism financing (CTF) requirements. These are

documented in supplementary guidance note PSN02 and cover everything from know your customer (KYC), sanctions screening, ongoing monitoring and well drafted policies and procedures.

For those entities who have baked a robust financial crime programme into their crypto model, the PSA requirements are likely to re-emphasise what is already being done. However, those companies that have chosen to take advantage of the lack of regulatory oversight to date may struggle to put in place proportionate controls to satisfy the heightened barrier to entry.

“According to a recent report by Chainalysis¹, in 2019 criminal entities moved \$2.8 billion in Bitcoin to exchanges, up from around \$1 billion in 2018. We have seen a similar trend in the number of reported cybercrime offences from our global adverse media monitoring – up 55% over the same period² – with a significant portion of this linked to cryptocurrency.

Legislation such as the PSA and 5AMLD (5th EU Anti-Money Laundering Directive) will help relevant firms clamp down on these illicit flows by establishing appropriate AML controls, including robust KYC practices. Screening entities for sanctions, PEPs (Politically Exposed Persons) and adverse media is an effective way to identify bad actors and we have been encouraged by the number of cryptocurrency businesses we’ve seen proactively implementing such measures.”

Hugo Veazey, Director of Anti-Financial Crime Solutions, RDC

The categorisation challenge

Whilst the PSA has sought to take a nuanced approach to licensing and regulating the payments space based on activity, it is clear that not all activity will fit neatly into the defined parameters. It could also be the case that some parts of the process can be defined as ‘A’ and others as ‘B.’ As such really navigating what license and supplementary controls are the right ones may be challenging. For example the PSA will regulate tokens that fulfil the definition of a “digital payment token”. Concepts or labels that are commonly used to describe and distinguish tokens such as “security token”, “payment token” or “utility token” are not recognised by the PSA and are inconclusive in determining whether a token would be regulated by the PSA.

The key to navigating the requirements will be to have a thorough breakdown of your product portfolio and controls and to conduct a comprehensive mapping exercise. If there is any uncertainty, early and transparent dialogue with the regulator will potentially avoid costly mistakes in the future.

1 <https://blog.chainalysis.com/reports/money-laundering-cryptocurrency-2019>

2 <https://rdc.com/cybercrime/blog/cybercrime-in-recession/>

Too much too soon

The PSA afforded a n a ttractive ‘grandfathering’ p eriod f or t hose c ompanies t hat r egistered a head o f t he regulatory roll out. Such companies were given a 6-12 months grace period to operate during which time they need to meet the new standards. Undeniably beneficial, it has also proved challenging for those companies who have had very little, if anything, in terms of controls.

For those companies applying for licenses today, the bar has been set intentionally high. There is an extremely important cost vs commercial value discussion to be had ahead of any application. This includes an understanding of in-country resourcing requirements in addition to any process builds.

Singapore vs Europe - same same but different?

How unique is the approach taken by Singapore when considered against Europe? This is an interesting question, where context is key. Unlike Singapore, EU regulations look to provide a framework for a number of countries. Singapore, in comparison, is a small geography and those organisations looking to build a presence in the region do not benefit from ‘passporting’ as those based in the EU do. Instead each market within the APAC region needs to be tackled independently and has its own set of licensing requirements.

With that in mind, it is difficult to compare the approach taken in Europe and that in Singapore. However, there are some interesting parallels. The EU Anti-Money Laundering Directive (‘AML’) does not provide a tiered approach - entities are either obliged or not. In this regard the risk rating of services and commensurate requirements to mitigate those specific risks is a novel and nuanced approach taken by the MAS. However, under the EU Payment Services Directive 1 (‘PSD1’), entities with an average volume of monthly payment transactions below €3 million can benefit from a lighter authorisation regime if their Member State of establishment makes use of that option. This so-called “waiver” regime is maintained under PSD2 as an option for Member States, albeit with the difference that Member States making use of the option can decide to define a lower threshold under which such “waivers” can be granted.

In terms of approach to crypto, AMLD added as “obliged entities”:

- providers engaged in exchange services between virtual currencies and fiat currencies
- custodian wallet providers

This means that registered entities must comply with AML/CTF regulations, which is aligned to the approach taken in Singapore by the MAS. However, the directive does not determine their regulatory status, which is decided by local regulators.

In the US regulation of payment systems is dispersed across multiple state and federal regulators. This interplay means if something is regulated at a state level, this can result in up to 50 different sets of requirements and subsequently many inconsistencies between states.

Another challenge with the US financial services sector is its scale and the diversity of US financial institutions: unlike the UK which has a more concentrated market, the US has a range of financial institutions from large global banks through to community banks.

Some observers have argued that certain payment companies would be more effectively regulated through the federal banking regulatory framework, whereas opponents of this idea assert it would result in the preemption of important state-level consumer protections and in an inappropriate combination of banking and commercial activities. The US Treasury's drafted a report entitled 'A financial system that creates economic opportunities - nonbank financials, fintech and innovation', which included recommendations to modernise the US financial services sector. The report is interesting because the key areas it identifies for development closely align with those areas of focus elsewhere in the world. The US has been observing trends in Europe and Singapore around issues such as open banking, cloud and regulatory sandboxes. Although there are aspects of the US financial market that mean that examples from other jurisdictions cannot just be 'lifted and shifted', it is clear that the US is keen to learn lessons from other markets.

Conclusion

PSA provides a good framework which mandates high standards for controls which should not only protect consumers and instill a sense of trust in the FinTech space, but will also allow legitimate players to operate in a competitive environment.

Companies that have planned and built their business with a strong compliance framework at its core are likely to be best placed to succeed in the long term. To those applying now: get your ducks in line, break down the requirements and really understand how they apply to your organisation, and stress test the adequacy of the systems, controls and processes you have in place. It's also important to note that meeting regulatory requirements is the minimum requirement. All entities should have a framework in place that addresses the specific risk exposure they / their customers face - this may in some cases mean going over and above minimum regulatory requirements.

Thank You

www.fintrail.co.uk

www.rdc.com



FINTRAIL

rdc
Smarter Screening