Where disruption meets regulation

Jake Robson, Gordon Milner and Nick Davies from Morrison & Foerster
discuss cross-border regulatory challenges and how fintechs can plot a path of compliance

In southeast Asia, a wide range of businesses from retailers to ride hailing companies, as well as traditional financial institutions, are poised to harness technology to launch, or collaborate with fintech companies to offer, payments, lending, wealth management or insurtech products regionally.

Yet regulatory compliance is often an afterthought. A failure to plan for, and adapt to, rapid changes in financial services regulation and the resulting financial and reputational implications of breaches of such regulation can all have disastrous consequences. These are critical considerations for all fintechs planning cross-border rollouts, as well as for other businesses considering commercial partnerships with fintechs in this region.

MORRISON FOERSTER

www.mofo.com

Regulators welcome innovation but regulatory requirements remain high

There is little doubt that the financial services industry in southeast Asia is in the process of being "disrupted" by new business models, new market participants and new products, but this is only part of the story. Financial services regulators are tasked with the dual role of ensuring that customers are adequately protected whilst at the same time encouraging financial inclusion, especially through innovation. Until relatively recently, many regulators in the region have been playing catch up with technological developments in the financial services sector and the regulatory infrastructure has not kept pace with innovation, which, in certain jurisdictions, has led to a certain amount of paralysis and uncertainty. This is, however, beginning to change.

Many financial services regulators in ASEAN countries are engaging with innovators in regulatory sandboxes as part of a broader remit to increase financial inclusion and move to a cashless economy, and a new wave of regulation is being implemented in many countries in southeast Asia to respond to innovation in the payments, lending and crowdfunding sectors in particular.

Jake Robson
Partner, Morrison & Foerster
Singapore
T: +65 69222026
E: jrobson@mofo.com
W: www.mofo.com

About the author

Jake Robson heads Morrison & Foerster's Asia fintech and financial institutions practices and the TMT practice in Singapore. He has extensive experience in cross-border acquisitions, disposals and joint-venture arrangements, as well as venture capital investments and fundraisings.

Jake has a particular focus on the financial institutions, insurance, technology and telecommunications sectors, which locates him at the nexus of the fintech and insurtech sectors. He regularly advises on cross-border regulatory matters and product roll-outs in the financial institutions and fintech sectors. Jake is highly ranked as a leading individual for corporate/M&A by Chambers Global, Chambers Asia Pacific, IFLR1000 and the Legal 500 Asia Pacific.

Gordon Milner
Partner, Morrison & Foerster
Hong Kong
T: +852 25850808
E: gmilner@mofo.com
W: www.mofo.com

About the author

Gordon Milner heads Morrison & Foerster's Asia technology practice. He specialises in advising on data privacy, technology regulation, intellectual property, licensing, outsourcing and cross-border technology transactions in Asia.

With nearly two decades experience providing specialist intellectual property, regulatory and operational technology law advice to clients in Asia, Gordon advises clients on projects ranging from traditional technology roll-outs in the financial services sector to state-of-the-art, data-driven collaborative development projects in the AI and deep-learning space. He also specialises in open source software.

Gordon is ranked in Tier 1 for TMT in China by Chamber Asia-Pacific 2019; as a leading individual in Hong Kong for TMT; and recommended for Hong Kong Intellectual Property and China Fintech, Healthcare, Life Sciences and TMT by Legal 500 Asia-Pacific 2019.

Nick Davies
Senior associate, Morrison & Foerster
Singapore
T: +65 69222029
E: ndavies@mofo.com
W: www.mofo.com

About the author

Nick Davies is a senior associate in Morrison & Foerster's Asia fintech team and a member of the firm's blockchain group. He represents multinational corporations, financial institutions and investors on their Asia-Pacific cross-border M&A, joint-ventures and other commercial matters.

Nick also has an active venture capital practice, advising both investee companies and investors on capital raising, strategic joint ventures and partnerships involving fintech ventures. Nick is frequently involved in fintech matters involving blockchain technologies. He advises venture capital investors and institutional investors on appraising blockchain investments, including how to reconcile equity investments with holdings of tokens issued by investee companies.

In addition, fintechs and those partnering with them must also comply with a host of other regulations that impact on their businesses; from licensing restrictions tied to foreign ownership caps to data privacy and localisation laws as well as general anti-money laundering reporting requirements.

The real challenge for fintech innovators is therefore not only to innovate and seek commercial partnerships for the distribution of their financial services offerings – a theme that we covered in our 2018 IFLR fintech special report, but also to create a holistic approach to compliance that will grow and respond positively to the changes in regulation in their target markets.

In this article, we outline some critical areas in which fintech innovators, and businesses that may seek to partner with them, potentially expose themselves to future regulatory risk. These areas should be considered as early as possible when planning a fintech product or distribution joint-venture.

Monetising customer data in a data privacy minefield

Customer data plays a key role in the fintech economy. In addition to its immediate use in individual transactions, the collection, processing and analysis of sets of customer data can provide invaluable market insights to help a business develop new products, identify third party synergies and focus marketing efforts.

Lending platforms in particular have benefitted from the acquisition of detailed customer databases. By applying deep learning techniques to these datasets, platforms are able to generate accurate, highly-granular individual risk profiles and credit scores that enable accurate and rapid risk pricing for individuals, thus opening up previously underserved markets in countries like the Philippines and Indonesia.

Indeed, customer databases are often the most valuable asset on a fintech's balance sheet and the size, quality and transferability of data assets are increasingly the focus of interest (and careful diligence) by investors and potential acquirers.

However, data can be a double-edged sword – the collection, processing, retention, protection and sharing of personal data are heavily regulated. Recent years have seen a proliferation of cyber security and data protection laws – with China, Singapore, South Korea, Japan, Australia, Malaysia, Indonesia and the Philippines all introducing or updating compliance rules and Indonesia and India taking important steps toward statutory regulation.

The net effect is a patchwork of different regulatory regimes across southeast Asia. This is compounded by the extra-territorial reach of the EU's General Data Privacy Regulation (GDPR), which can apply to southeast Asia fintechs catering to local customers who are European nationals.

The infrastructure and manpower costs of achieving regulatory compliance when operating a platform across multiple jurisdictions can be substantial. Given the relatively light policing and minor penalties imposed by many southeast Asian jurisdictions, some early-stage fintechs have taken the view that it is cheaper to ask for forgiveness than to foot the costs of compliance. However, this is a false economy. It merely stores up the problem for the future, where the costs and difficulty of rectification might even outstrip the value growth of the business. A platform's hard-earned goodwill and reputation might easily be destroyed by a single data breach – particularly as more jurisdictions (such as the Philippines, China, Indonesia and Singapore) impose mandatory breach notifications.

A more advisable approach is for fintechs to work with privacy and data security specialists to build compliance into the platform from the ground up.

In particular, fintechs should:

- obtain adequate consents from customers when data is collected;
- conduct adequate diligence on the provenance of third-party data sources;
- develop a privacy policy tailored to the platform and ensure that any sharing of data from the platform complies with that policy;
- avoid collecting and retaining personal data for which the business has no legitimate need and wherever practical, anonymise and/or tokenise datasets; and
- be particularly wary of incorporating unverified scripts and other elements into the platform when collaborating with third parties.

Customer loyalty and digital wallets in the context of payments systems regulation

In the payments sector in southeast Asia, there is a trend towards creating consumer-orientated end-to-end payment systems that remove many steps and actors from the traditional payment and settlement process.

The flip-side to greater reach and customer conversion is increased regulatory risk

Payment for goods and services using e-money by scanning a QR code at the point of sale has spread from China to much of southeast Asia. This in turn is helping to promote the wider use of e-wallets and e-money and also fits with financial regulators' desire to promote cashless transactions.

Blockchain technology is already available that can facilitate the interoperability of e-wallet providers, while also potentially allowing consumers to carry out frictionless peer-to-peer payments or remittances. Adding elements of convertibility or exchange with points-based customer loyalty systems can also help businesses achieve customer engagement and obtain access to deeper customer data.

However, regulation in this area remains segmented along national lines and tends to view with suspicion payments and settlement systems that run independently of the traditional banking system. For instance, in Indonesia, the 2018 Electronic Money Regulation imposes foreign ownership limits on system operators and requires operators to either choose between providing "front end" or "back end" elements of the system, but not both. In Singapore, the new Payment Services Act has a narrow safe-harbour in which "limited purpose e-money" (or digital tokens carrying out a similar function) is allowed to operate before requiring full licensing as a payments system provider.

The regulatory uncertainty becomes even more pronounced if blockchain technology is brought into the equation, with countries like Malaysia now stipulating that all digital tokens must be regulated as investment securities, and others such as Singapore, regulating so-called "stablecoins" potentially as both debt securities and as payment instruments.

Businesses focused on this sector should therefore recognise that expansion of products and services in southeast Asia must be done incrementally, and that due to greater regulatory requirements, commercial partnerships or strategic joint-ventures with incumbents may be a key component of a disruptive business model.

Friction-less customer acquisition and the dangers of mis-selling

Financial services have been sold online for a number of years. However, the ability to pro-actively market financial services to consumers, though smartphone apps based on customer data and behavioural analytics, is set to transform the way in which financial services are marketed and sold.

Similar to how many supermarkets or retailers in the UK developed financial services joint-ventures with retail banks in the late 1990s, in a number of southeast Asia countries we are seeing banks and insurers actively partnering with online retailers or platforms to extend their reach and customer base. However, the flip-side to greater reach and customer conversion is increased regulatory risk, which in the absence of self-regulation by the fintech industry is likely to result in stricter regulatory standards being imposed by regulators and legislators.

- *Compliant product distribution*: Putting in place a network of licensed distribution partners in multiple countries in southeast Asia is challenging. The regulatory framework in many countries in this region for certain types of products such as life insurance, is still largely based on face to face sign-ups using licensed agents. Financial institutions looking to extend their reach through digital platforms to new customer segments need to demonstrate that due attention has been applied to respecting the spirit of these regulations when designing the customer sign up and onboarding process. This should also be reflected in the minimum

compliance standards set out in distribution arrangements.

- *Disclosure of commission*: The ease and convenience of offering and selling financial services such as lending or wealth management through, for example, an online shopping app, does not necessarily mean that these products ought to be sold in the same manner as other products on the platform. For instance, in EU countries there is a trend to require clearer disclosure of all referral fees, commissions and other fees earned by intermediaries. This has consequently required changes to many distribution models. Fintech businesses in southeast Asia may wish to consider carefully how any future implementation of stricter rules on disclosing fees and commissions may adversely affect the fee models for their services.
- *Product description and eligibility*: Targeting and soliciting potential customers for financial services based on individual customer data can sometimes lead to a blurring of the lines between education about the type of product and selling a product that is suitable for the customer's circumstances.

  In some Asian markets, fintech products such as peer to peer lending or robo-advisory services are the first time that consumers may have been given access to such financial services. For instance, if a potential customer is presented with a maximum borrowing amount on a lending platform, should the platform operator also be obliged to check that the customer understands whether or not they can afford to service the loan?

  In Indonesia, the peer-to-peer lending sector has already been tainted by reports of irresponsible lending, with the country's regulator, the OJK, taking action to restrict the issue of new licences and remove licences from blacklisted operators.

If large numbers of customers in a particular market later complain that the product does not deliver on the benefits presented to them during the sign-up process, or that the potential negative aspects of the product were not made clear, the regulatory response could be catastrophic and could lead to whole categories of products becoming outlawed across multiple markets.

This has already occurred in the US with sub-prime mortgages and in the UK with payment protection insurance. The balance between sensible self-regulation and deterring customer sign-up is difficult, but one which all fintechs must achieve.

Outsourced system providers – the dangers of a data breach

Most fintech businesses require an extensive IT infrastructure to operate. The capital cost and management time involved in purchasing, installing and maintaining the necessary hardware can be substantial – particularly for an early-stage fintech. Moreover, self-owned systems can impede agility – it can be difficult to rapidly scale such systems up or down in response to business needs.

Fintechs often look to address these issues by entering into outsourcing arrangements with cloud providers and other outsourced service providers (OSPs). OSPs offer a wide variety of services that may be of interest to a fintech, including virtual servers, storage, compute, backup and payment gateways. Typically, these services can be rapidly implemented and subsequently scaled as necessary to speedily bring the fintech's product to market.

However, outsourcing functions to an OSP often necessitates the transfer of personal data, transaction information and other sensitive data to the OSP. This, coupled with the inevitable reduced visibility of and control over the outsourced systems by the fintech, leads to an increased risk that the transferred data might be subject to unauthorised access, processing or transfer. As a consequence, such arrangements can lead to increased regulatory risk.

In addition to general privacy laws (mentioned above), many jurisdictions have imposed sector-specific rules on regulated entities in the insurance, banking and securities sectors. Sector-specific regulations vary widely from jurisdiction to jurisdiction. Some are rather detailed and prescriptive (for example, the outsourcing rules issued by MAS in Singapore and the HKMA in Hong Kong), whereas others simply set out high-level principles.

The lack of harmonisation in both privacy laws and sector-specific regulations can be a challenge for fintechs operating across multiple jurisdictions. In the interests of efficiency and consistency, many fintechs try to identify the operating jurisdiction with the strictest regulations and apply that high water mark across all of their local operations. However, this approach is becoming increasingly complicated by recent regulatory trends requiring data users to localise, store and process personal data in-country (for example in Indonesia, Malaysia, India and China).

One particularly important regulatory requirement is the obligation to report data breaches to the regulator. This is becoming increasingly common in the region – many jurisdictions (including the Philippines, China, Indonesia and Singapore) now impose mandatory breach notifications on data users. A business with operations in more than one jurisdiction may find itself required to report a breach to multiple regulators. The lack of harmonisation between jurisdictions on key matters such as materiality thresholds, process and form of report can make it difficult for a fintech to ensure compliance, particularly in the light of the very short prescribed statutory notification deadlines.

The lack of harmonisation in both privacy laws and sector-specific regulations can be a challenge

Attempting to pass through regulatory risk to the OSP is not a viable solution. Many regulations impose strict liability on the fintech as a data user and, historically, many OSPs (particularly in the cloud and virtual server space) have operated using non-negotiable standard terms with extensive liability disclaimers. That said, some OSPs are now actively targeting potential banking and fintech companies with less one-sided agreements backed up by service level agreements and meeting minimum standards imposed by regulators. A better approach is to plan ahead and choose carefully. Fintechs should:

- work with privacy and data security specialists to develop detailed data security policies;
- conduct appropriate diligence before

engaging OSPs;
- conduct regular testing after engaging OSPs;
- develop breach policies and procedures; and
- wherever practical, encrypt and/or tokenize datasets at rest and in flight.

The long-arm of the law: extra-territoriality in financial services regulation

In southeast Asia, an increasingly geographically mobile population together with the cross-border nature of many fintech products results in a significant risk to fintech businesses of falling foul of financial regulation in countries in which they had not anticipated launching.

When compared with the EU, the level of mutual recognition of licensing requirements in ASEAN countries is very low. Furthermore, in many countries, there are restrictions on foreign entities offering financial services products to their citizens – for example, all e-money operators in Indonesia must not be more than 49% foreign-owned. Other fintech focused legislation, such as Singapore's 2018 Payment Services Act, or Thailand's 2018 decree on Digital Assets Businesses, has introduced specific offences aimed at entities that solicit customers in their respective countries without having the requisite licences.

The issue for fintechs therefore becomes whether it is sufficient to rely on terms and conditions that list the jurisdictions in which users are permitted to access their services and rely on users to comply with those restrictions, or whether clearer monitoring and active exclusion of customers from all non-licensed jurisdictions is required. The latter approach is likely to be preferable for three reasons:

- *Maintaining an unblemished record with a future regulator*: asking for forgiveness from a regulator once a product has gained traction in a market is an extremely risky strategy, especially when domestic operators are also trying to demonstrate regulatory compliance and may enjoy strong relationships with their domestic regulator.
- *Avoiding issues with home regulator*: in our experience, even in a common market such as the EU, home regulators may be concerned where a financial services company is predominantly serving customers based outside its jurisdiction. Regulatory complaints made in other jurisdictions are likely to find their way back to the home regulator, which may result in closer scrutiny over a business's overseas expansion plans.
- *Anti-money laundering*: the Financial Action Task Force (FATF) has published a number of recommendations on the level of know-your-customer checks that countries should apply to their financial technology sectors. Most recently, in their February 2019 statement on mitigating risks from virtual assets, the FATF recommended a $/€1,000 limit above which full client due diligence should be conducted. In this context, it is becoming largely unsustainable for a fintech to argue that it does not hold full and up to date information on a client's identity, since a fintech should have verified the client's address and therefore country of residence and citizenship as part of its due diligence.

The most sustainable fintech businesses will be those that adopt a holistic approach to compliance

Overall, in southeast Asia, we are rapidly seeing that grey areas of regulation are giving way to clear principles on how financial services regulation is responding to fintech innovation. The most sustainable fintech businesses will be those that adopt a holistic approach to compliance with all aspects of regulation that touch upon their businesses, and also which develop their products, back-end systems, strategies and commercial partnerships in a way that can respond to likely future regulatory changes.