Your World First

C/M/S/
Law.Tax

FinTech 2.0

Transformative trends across Asia

November 2017

Your World First

The financial services sector has been disrupted by the rise of FinTech, to the extent that FinTech innovations have now become part of the business norm.

As a result of this, we are now witnessing a new way of delivering financial services that provides immense value to consumers by delivering financial services that were previously unavailable to them whilst providing financial institutions and FinTech companies alike with greater insight. This has led to structural changes in the market. The vanguards of this new FinTech era have been non-financial institutions that have leveraged on new technologies to gain market share. These new entrants have included not only innovative start-ups, but also established internet giants. The effect is that the dominant position of financial institutions in the provision of financial services are gradually being eroded by FinTech entrants.

As a firm that is focused on both the technology and financial services sector, we are in the privileged position of having advised both established financial institutions and FinTech companies across the world on the innovations and technologies that are creating this FinTech era. In this paper, we explore the following key FinTech trends that are changing the financial services sector across Asia:

Payment Ecosystems

Artificial Intelligence

Internet of Things

Cost of Compliance

Payment Ecosystems

Evolution of financial services

The most popular e-payment platforms in Asia today are operated by non-financial institutions that provide an ecosystem of services to their customers (Payment Ecosystems). Financial institutions are increasingly at risk of being relegated to just the provision of back-end functionality, such as clearing and settlement, and in this process losing the customer relationship.

'Owning' the customer relationship is crucial to the success of Payment Ecosystems. By aggregating all the services required along the customer journey, Payment Ecosystems become the go-to platforms for their customers. Consumers now no longer have to use multiple platforms for each particular transaction type. Instead, when a customer wishes to make an online purchase, he or she can search for items online, chat with merchants, and make payment – all within a single platform.

Financial institutions need to start viewing e-payments as part of a larger customer journey, instead of a discrete activity. Customers typically require e-payment services only as a final step to complete their transactions. Payment Ecosystems recognise this, and have tagged-on e-payment services to their primary services, such as e-commerce or social media. Doing so allows them to control their customers' full range of experience, and removes dependence on third-party products. Even if there are third-party products involved, these products are often relegated to an back-end role or often white labelled.

To stay competitive, financial institutions have to start integrating their services within Payment Ecosystems, as payment services are no longer the unique preserve of financial institutions. Alternatively, they might try to recover their customer relationship through the offering of an equally seamless customer experience. However, financial institutions are typically saddled with legacy systems and processes which make them less nimble in terms of evolving.

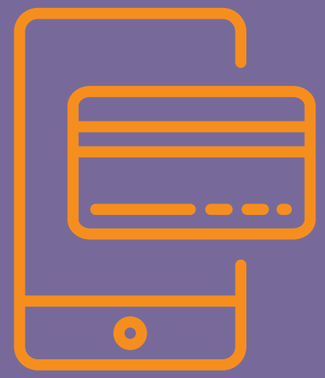
Regulators need to play their part too in enabling financial institutions to take on platform providers. The current regulatory hurdles that restrict financial institutions from participating in non-banking activities should be lowered and the playing field between financial institutions and non-financial institutions levelled. Regulatory obligations and oversight should not be focused on entity type but rather on activity. Most regulators have acknowledged this regulatory asymmetry, and have taken steps to remedy it as further detailed below.

An enabler

E-payments offerings within Payment Ecosystems function as an enabler of the primary services offered to their customers. It enhances the value of those primary services and increases the platform's attractiveness to its customers. This is largely in part due to its ability to make peer-to-peer (P2P) transfers seamless.

A Chinese e-commerce giant's free e-payment offering is arguably one of the main reasons that its websites are amongst those most visited in China today. Its key feature is its escrow service, which allows customers to verify whether they are satisfied with the product purchased from e-commerce websites before money is released to the seller. This was a key enabler in the take-up of its e-commerce business, because it provided value-added services in addition to pure e-payment services.

'Stickiness' to a particular Payment Ecosystem can also be a result of a well-positioned e-payments offering. For example, a transport company incentivizes its customers to store credit in its e-payments offering in order to ensure that they are 'locked-in' and prevent them from utilising other platforms for similar primary services. This company's integration of its e-payments offering into its platform has enabled it to become a Payment Ecosystem, and has created a moat around it, protecting it from competitors.



Nonetheless, the mere incorporation of an e-payments offering into a platform does not mean that customers will be sufficiently 'locked-in'. Adoption of the enabling e-payment offering depends on how seamless its usage is, and whether there are any incentives for customers to use it. For example, another company, which provides transportation and food delivery as its primary services, launched its e-payment offering in order to enable its customers to pay for these services more efficiently. However, since it does not offer a simple cash-to-e-money conversion through its drivers, the adoption of its e-payment offering by its customers has been slower and less successful.

Regulatory asymmetry

Payment Ecosystems, as non-financial institutions, have been able to thrive to date as they have not consistently been subject to the same regulatory requirements as financial institutions. Despite the rise of Payment Ecosystems, regulatory regimes have generally only applied to financial institutions. This asymmetrical regulatory approach allowed Payment Ecosystems to continue innovating at a much faster pace than financial institutions, free of the constraints brought about by regulations. Payment Ecosystems have consequently been able to flourish to the extent that the regulators can no longer ignore them. An example of this would be when the two largest Payment Ecosystems in China recently promoted the concept of a cashless society and distributed significant

Payment Ecosystems, as non-financial institutions, have been able to thrive to date as they have not consistently been subject to the same regulatory requirements as financial institutions.

rewards to customers of their e-payments offering. This led to some merchants rejecting cash as payment, which in turn led to complaints from customers. Eventually, the PRC regulator – the People's Bank of China (PBC) – had to step in to mandate that the refusal of cash was not allowed.

Regulators are now starting to increase their oversight of Payment Ecosystems to ensure consumer protection and protect the overall integrity of the financial system. For example, the PBC recently mandated that financial institutions providing e-payment offerings have to channel their payments through a new clearing house by June 2018. All payment companies in China, both financial institutions and Payment Ecosystems, would have to operate under a standard set of clearing protocols and rules. Payment Ecosystems will no longer be able to operate under a different set of terms with financial institutions that fall outside of the PBC's oversight. Thus, all payment providers, including Payment Ecosystems, will be subject to regulatory scrutiny by the PBC. Prior to this announcement, information on capital flows bypassed the PBC, and were used by Payment Ecosystems to enhance their suite of service offerings, for example targeted marketing and credit scoring. The regulatory playing field between financial institutions and Payment Ecosystems is now becoming more level, and the valuable information generated will now be disclosed to the government and competitors.

Existing regulatory barriers imposed on financial institutions are also in the process of being removed. This would allow financial institutions, previously saddled with restrictions on permissible business activities, to compete on a more even footing with Payment Ecosystems. In June 2017, the Monetary Authority of Singapore (MAS) proposed to relax its position on anti-commingling rules for financial institutions. These rules were originally put in place more than a decade ago to ensure that financial institutions will maintain focus on their core financial services. But with the increasing disintermediation of financial institutions, the relaxing of such rules were necessary for them to compete.

As innovations in the e-payments space continue to develop, it is important for regulations to evolve. Therefore, the recent acknowledgment by PBC and MAS of the changing landscape and their subsequent adjustment of rules is encouraging. Previous distinctions between financial and non-financial businesses are blurring, and new rules and attitudes have to be adopted in our modern age.

Back to basics

In a pre-dominantly cash-based economy, external push factors are necessary to create the foundations for Payment Ecosystems to flourish. The inertia to shift consumer behaviour online is otherwise too significant for any financial service provider to overcome. In China, where Payment Ecosystems are extremely popular, the shift to digital transactions was particularly swift arguably because the adoption of credit cards never quite caught on. Unlike most of the Western world, Chinese consumers did not have to learn and subsequently un-learn the process of using credit cards to pay for goods and services.

Mandatory requirements imposed by the government can go a long way towards shaping consumer behaviour. In November 2016, India's Prime Minister Modi announced the demonetisation of all Rs 500 and Rs 1,000 banknotes to control the use of counterfeit cash to fund illegal activities. The sudden announcement led to endless queues outside financial institutions across India, as millions of people rushed to deposit their banknotes before the deadline. A spike in the usage of debit and credit cards was also reported.

This regulatory imposition accelerated India's migration from being a cash-based economy to a digital one, almost overnight. As a viable alternative to cash, e-payment options witnessed a 400 to 1,000% increase in usage since the beginning of the demonetisation exercise. A month after Modi's announcement an Indian e-payments company added over 20 million new customers and was processing more transactions per day than all credit cards in India combined. Merchants as diverse as shopkeepers, vegetable sellers and petrol pump operators also started offering e-payment options via this company's platform.

To harmonise standards, the National Payments Corporation of India (NPCI)5 launched a new payment system – the Unified Payment Interface (UPI) – which allows payments to be made between any two bank accounts. Consumers can now make e-payments without having to check their counterparty's ability to do so beforehand. Seamless and hassle-free e-payments can now occur.

Since then, Payment Ecosystems are starting to take shape. For example, an Indian payments company has started to integrate its e-payment offering to allow customers to perform other services, such as booking taxis and paying utility bills. Similarly, other platforms in India are also starting to behave more like Payment Ecosystems.

Harmonization of standards

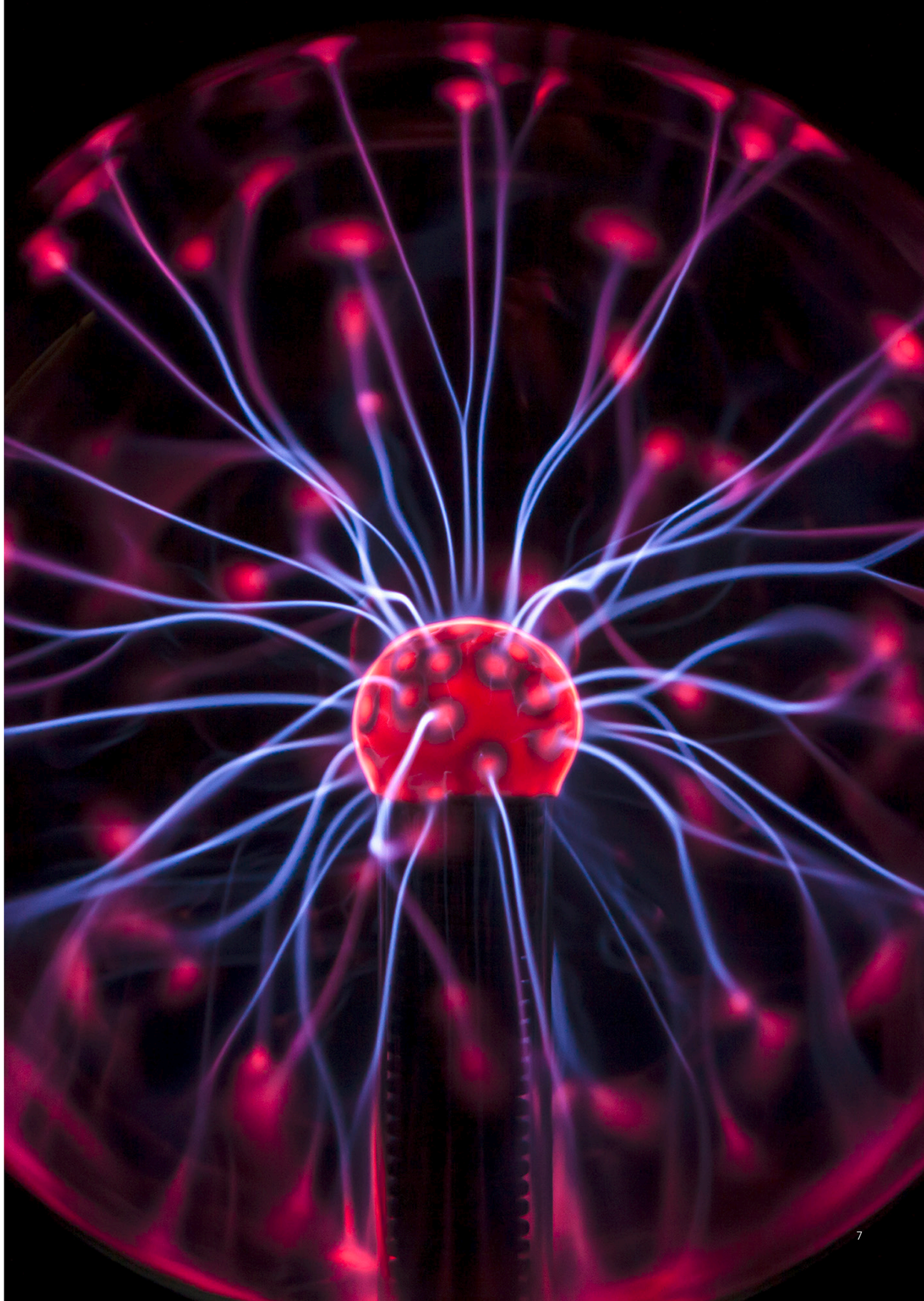
As a pre-condition to widespread adoption of e-payments in an economy, there has to be a harmonisation of standards amongst payment systems within that economy. Without it, electronic transactions between persons with bank accounts from different financial institutions cannot occur. Only then will Payment Ecosystems gain mainstream adoption and flourish.

Digital transactions are unlikely to take off in an economy where there are a variety of payment system standards available. The inconvenience of checking whether the counterparty has a bank account with similar payment system standards as one's own is usually a deal-breaker. To harmonise standards, the National Payments Corporation of India (NPCI) launched a new payment system – the Unified Payment Interface (UPI) – which allows payments to be made between any two bank accounts. Consumers can now make e-payments without having to check their counterparty's ability to do so beforehand. Seamless and hassle-free e-payments can now occur.

Harmonization of payment system standards have directly led to the adoption of digital transactions. Since the adoption of the UPI, e-payment transactions have skyrocketed, both in volume and in value. The alphabet soup of payment system standards is now a thing of the past, and along with the demonetisation exercise, the scene has been set for Payment Ecosystems in India to gain mainstream adoption.

Here to stay

Payment Ecosystems, having been successfully integrated into our daily lives, are here to stay. In order to thrive in modern society, financial institutions should either build Payment Ecosystems that are integral to their customers' lives, or integrate themselves within them. E-payments, being an enhancer to the primary services offered by Payment Ecosystems, are therefore essential in ensuring the 'stickiness' of these platforms.



Artificial Intelligence

A transformative advancement

Artificial intelligence (AI) in financial services is a transformative technology that financial institutions have to embrace. It not only enhances the customer experience but also reduces costs for financial institutions. While disruption is a constant, AI accelerates this by delivering financial services that were previously unavailable or inaccessible. With AI, consumers can receive tailored financial services on demand. The customer value-add makes adopting AI an imperative for financial institutions.

AI enables financial institutions to be proactive, and not simply reactive. Instead of merely providing financial services on demand, financial institutions can anticipate needs and pre-emptively fulfil them. This is done by utilising AI to create behavioural profiles of their customers, and extrapolating their needs. Service offerings can then be tailored to meet these exact needs on a 'just in time' basis.

To exploit AI to its fullest potential, financial institutions need to ensure that they have the right to use relevant data. AI needs to collect data and process it in order to generate usable information for financial institutions. Where machine learning is utilised, financial institutions should also protect the derivative intellectual property rights (IPRs). These IPRs derive from AI's ability to learn and adapt its performance without human intervention to change its own programming or instructions.

Financial services is a regulated industry, and AI can only be utilised within certain boundaries. Compliance risks will exist for specific-use cases, and these have to be identified before AI is implemented. For example, where AI is used in a customer-facing role, there may be consumer protection rules that apply. If a charge of non-compliance occurs, financial institutions may be required to disclose the algorithms and other means by which the AI functions in order to determine the cause of non-compliance.

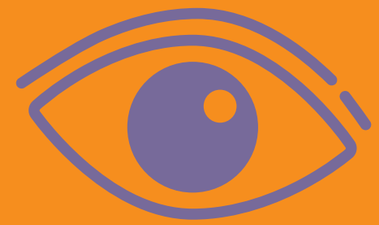
Enhancing customer experience

AI allows financial institutions to break away from traditional product offerings and provide customised ones on a more cost efficient base. An example would be in the insurance industry where insurers price their premiums depending on objective factors such as the demographic of policy-holders or the value of the product to be delivered. With the advent of AI, insurers can introduce dynamic pricing where premiums vary depending on the profile of each policy-holder. A Chinese insurer, which provides customers with insurance for shipping returns costs on e-commerce purchases, varies its premiums for customers depending on various factors, including the individual customer's return ratio. Such a personalised approach benefits consumers, because they only pay for the risk which their profile attracts. It also benefits insurers, because its risk assessment is more targeted to cover the risks incurred by each individual customer.

A Chinese insurer, which provides customers with insurance for shipping returns costs on e-commerce purchases, varies its premiums for customers depending on various factors, including the individual customer's return ratio.

The nature of the interaction between financial institutions and their customers is also shifting because of AI. Human operators no longer need to interact with a customer. Instead, financial institutions are now launching artificial conversational entities such as chatbots as an interface to their customers. This is a paradigm shifting development because consumers' accessibility to financial services is now no longer limited by the availability of human resources.

AI needs to operate within the confines of financial regulation. AI software that delivers chatbots will come with default script libraries. Financial institutions will have to ensure that these libraries are compliant with regulations. Since the chatbots are interacting with customers, potentially to deliver financial services, they will have to comply with consumer protection and financial advisory rules. Although financial institutions can contract for vendors to comply with such rules, financial institutions will be interacting directly with customers and therefore would, *prima facie*, be liable. In any case, financial institutions will be keen to ensure compliance, as any breach would also result in reputational damage. This means that any AI product would have to be carefully scrutinised for regulatory compliance before being launched.



Predictive analysis

By integrating AI into their businesses, financial institutions can anticipate their customers' needs and proactively meet them. As data about their customers is being collected, the AI is gradually building an increasingly complete behavioural profile of them. Such customer data can be collected either through traditional means, or less typical ones like social media. Once these behavioural profiles are created, predictive analysis can occur, and financial institutions should be able to sell their products and services to consumers on a 'just in time' basis.

Before collecting customer data, financial institutions should obtain consent under data protection rules. Such rules usually require that consumers also be informed of the purposes of such collection and use. As such, before utilising AI to collect and analyse customer data, financial institutions need to put internal processes in place to ensure compliance with data protection rules.

A Singapore bank recently partnered with IBM to utilise the Watson platform to provide client-specific portfolio recommendations to the bank's financial advisors.

Predictive analysis by AI can help customers make better decisions. This is because the AI understands the individual customers' needs and is able to tailor their suite of products or services to these needs. For example, there have recently been wealth management AI platforms launched that are able to accurately assess customers' income, expenditure and risk profile, and advise on an appropriate investment strategy to suit that profile. On a more granular level, there have also been AI platforms that track customers' purchases and automatically update them real-time about their spending habits. Such AI platforms provide value-add to customers by informing and advising them on their personal finance habits. A Singapore bank recently partnered with IBM to utilise the Watson platform to provide client-specific portfolio recommendations to the bank's financial advisors. Advisors from the bank trained IBM Watson and worked through scenarios to build a rules base for the platform. The result is a tool that empowers wealth management by dynamically segmenting clients on several parameters, including behaviour, while predicting life and financial events. It also predicts client attrition, identifies product opportunities and delivers tailored news and alerts to clients.

Nonetheless, such predictive analysis services are still at the nascent stage. Although predictive personal finance platforms provide personalised information and advice, it is uncertain as to how effective they will be in changing customers' behaviour. A potential approach may be to automate money-saving activities whenever they become available. For example, AI can be integrated into the financial services sector by automatically changing bank accounts whenever AI identifies better interest rates. But such a development also has hurdles in requiring that customers accept to allow AI to control their lives, as well as various regulatory risks.

Before embedding automated financial services, financial institutions need to consider the degree to which the activities may be regulated. For example, the automation of money-saving activities may trigger financial advisory rules. Regulators would also likely scrutinise it for compliance with consumer protection rules generally. If the algorithm makes an error, and a charge of regulatory non-compliance is made, an investigation may be made into the algorithm by which the automation functions. These, coupled with reputational risks, mean that financial institutions would be cautious in launching such predictive and automated services.

Costs reduction

Financial institutions can reduce costs by streamlining processes through the use of AI. Certain functions such as claims management or customer on-boarding that previously required human operators can be restructured. For example, a Japanese insurer plans to introduce AI to improve operational efficiency in its payment assessment process. Since the AI system will be able to analyse and interpret data, including unstructured images and text, it will be tasked with reading medical certificates written by doctors and other documents to determine pay-outs.

AI systems can also be trained to analyse patterns in claim submissions and factor in individual customer profiles for insurance claims. Recent advances in machine learning have vastly improved the ability of computers to gain insights from data. Claims that meet certain criteria are automatically approved, and those that are suspicious and do not fit pre-determined categories are flagged as fraudulent. Once claims are approved, wiring instructions to the financial institution for the transfer of the claim amount can be automatically sent. This makes the claims management process more efficient, by removing the human element from most of the process. Human intervention is only introduced where there are claims which AI do not understand and are potentially suspicious.

AI system will be able to analyse and interpret data, including unstructured images and text, it will be tasked with reading medical certificates written by doctors and other documents to determine pay-outs.

Where financial institutions have utilised machine learning to analyse patterns in its customer data, the IPRs derived from the process should be protected. There is otherwise a risk that the knowledge developed would be owned by the vendor. Financial institutions can protect this contractually, by preventing the vendor from taking an ownership or implied license to the knowledge acquired by the AI. This is especially important where the AI, with financial institutions instructions and data, has created derivative works. By protecting such IPRs, financial institutions can then build on the knowledge to continue improving operations to service their customers more effectively.

Costs can also be reduced by replacing low level cognitive tasks. Tedious and time-consuming work such as reviewing insurance claims can be automated. This improves the accuracy of the work as the potential for human-error is removed. Financial institutions also save on costs because they do not need to employ human resources to contribute to the work input that has been automated. Consequently, consumers benefit from the quicker pace at which their claims get processed, and the cost savings may eventually get passed on to them. This way, AI allows for the introduction of human element into the process only where human value-add is necessary. More time is made available for strategic thinking and methods to improve work processes as managers will not get bogged down by day-to-day activities. The hope is that such developments in AI would enable financial institutions to maintain their focus on customer satisfaction and improving their product and service offerings to customers.

Democratisation of intelligence

AI will eventually democratise access to intelligence, which will permanently change the landscape of financial services. Even small financial institutions can gain access to AI tools, and along with affordable computing power from the cloud, be able to process large amounts of data and derive unique customer insights. Flexibility provided by the cloud would also allow financial institutions to react quickly to such insights, and change their suite of products and services accordingly.

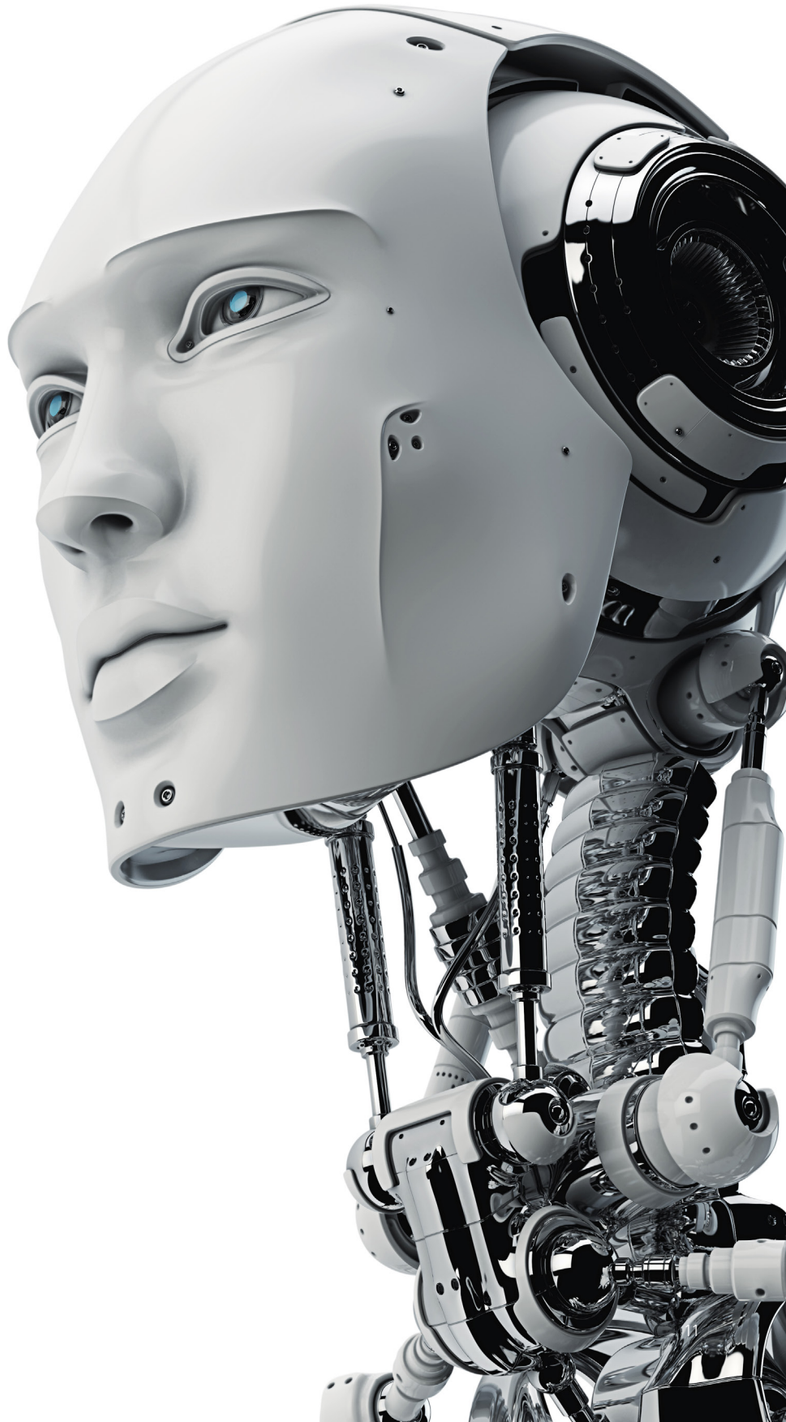
The accessibility that financial institutions have to AI capacity via the cloud means that AI-tools such as predictive analysis and smart assistants would soon be widely available. Financial institutions would be able to utilise these AI-tools and weave them into product and service offerings, enhancing the value proposition to their customers at minimal cost. The financial services landscape would be permanently changed as a result, and the big beneficiaries in the end would be the consumers.

The distinguishing element that separates the value proposition of a financial institution will then be its proprietary data. Since machine learning occurs through ingesting large amounts of data about customers and other business activities, the access that a financial institution has to that data is crucial. AI is only as intelligent as the data which is fed to it. Both the quantity and quality of data are important. There is minimal value in feeding large amounts of data to a machine if that data is homogenous and does not present an opportunity for the machine to learn and identify patterns.

Consequently, it is important for financial institutions to ensure ownership and access – preferably exclusive – to relevant consumer data. Financial institutions can achieve this contractually, by agreeing with their vendors that their rights in customer data will continue to hold. Where AI utilises data from various sources, financial institutions' access to relevant data may be more difficult to obtain. Despite this, financial institutions should still attempt to obtain licenses to use them. Financial institutions can contract with other parties to retain the right to use data for specified purposes. Access to relevant data is key for financial institutions to maintain a competitive edge, and financial institutions should ensure access to them whenever necessary.

A cautionary note

Although AI has taken off, its use by financial institutions should be properly scrutinised. Financial services remains a regulated activity, and the use of AI needs to fit within the regulatory framework. Financial institutions should remain cautious in utilising chatbots to provide financial advice to consumers, as it could jeopardise their banking licence. Insurers should stay vigilant in automating premium pricings as it may contravene competition law. The rise of AI has enabled financial institutions to service their customers better – they should also ensure that this is done in the right manner.



Internet of Things

A deeper understanding

The Internet of Things (IoT) enables financial institutions to understand customers from a holistic perspective. Financial institutions are now able to see their customers as individuals, and not as abstract entities derived from statistical or historical data. IoT utilises sensors in daily objects to collect real-time data from individuals. The data is then transmitted to a system to be analysed. This process allows financial institutions to obtain information on how individuals utilise daily objects, such as the objects' condition and movement.

New value propositions are created for consumers. Financial institutions' new understanding of customers as individuals enable services to be tailored. The application of IoT would mean that financial services created for mass consumption could soon be a thing of the past. Significantly, IoT does not only have application in the banking industry, but also for insurers.

For example, an insurer recently started to utilise IoT to measure an individual driver's driving performance. Factors measured include acceleration, braking, cornering and speed. Drivers who subscribe to this program are able to reduce their motor insurance premiums by improving their driving behaviour. The insurer is also able to make better risk assessments on its customers, thereby ensuring a more accurate pricing of premiums for each customer. The improvement of overall driving behaviour would ensure that there is a lower risk that accidents, and pay-outs, will occur.

... an insurer recently started to utilise IoT to measure an individual driver's driving performance. Factors measured include acceleration, braking, cornering and speed. Drivers who subscribe to this program are able to reduce their motor insurance premiums by improving their driving behaviour.

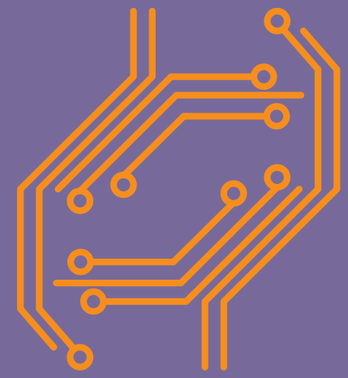
However, the nature of IoT means that financial institutions have to be careful about the way they collect data. Most of the data collected will likely constitute 'personal data', because it will be about identifiable individuals. Such regulated data can generally only be collected with consent from the individuals in question. The speed of which data is collected and the huge quantity of data involved, mean that proper consent may be difficult to obtain in practice. In implementing IoT, financial institutions should be careful about structuring the consent process and ensuring compliance with applicable data privacy regulations.

An enhancer

IoT can be used to enhance investing or lending activities. Sensors are deployed in houses to monitor utility consumption and the occurrence of fire hazards. During the mortgage loan origination process, lenders can understand the condition of houses by analysing data from IoT sensors. Lenders can also understand the condition and activities of individual manufacturing businesses when commercial loans are processed. For example, connected field devices in manufacturing can be used to generate data to support the lending credit assessment process in question.

When financial institutions combine IoT data with AI, the results can be game-changing. Credit assessments will now not only be improved by AI's analysis of factors such as income levels, but can also include IoT data. Such data on the physical condition of objects can be considered real-time. Financial institutions can utilise such data to detect fraud and improve their understanding of their customers' individual credit situation.

Products can be marketed more effectively through targeted advertising. An enhanced understanding of individual customers through IoT data enables financial services providers to develop personalised offerings to meet their specific needs. Data can also be used to segment their customer base and develop targeted advertising for their offerings such as home or car loans.



Finally, availability of real-time data feeds allows financial institutions to also provide other value-added services. Location-based data feeds allow the financial institution to be alerted to traffic scenarios and bad weather reports. When an accident occurs, roadside assistance can be automatically called for, and logistics and case management issues can be streamlined. Investment managers can also utilise IoT data to alert their investors of impending natural disasters that may affect the prices of their investments, such as commodities.

New opportunities

The potential of IoT in financial services opens up new opportunities for FinTech start-ups. Financial institutions will require a large number of sensors to be provided to their customers. They will also likely be keen to license technology that will assist them in aggregating and analysing IoT data. The volume of such data will be significant and FinTech start-ups that identify a user-friendly way to make sense of these will be in high demand.

IoT can also provide new business opportunities for traditional financial institutions. Financial institutions can now underwrite credit for customer segments that lack credit histories. Previously, financial institutions were unable to serve this market because of a lack of data available. However, with IoT, financial institutions can perform pattern-of-life (POC) analyses on individuals to understand their behaviours and habits. The condition of certain businesses can also be extrapolated by analysing data generated from their manufacturing control sensors. Nonetheless, this process is still undergoing testing, and the challenge to develop such an understanding based on IoT data still stands.

An enhanced understanding of individual customers through IoT data enables financial services providers to develop personalised offerings to meet their specific needs.

Unbundling of services

The availability of usage-dependent insurance premiums may lead to an increased request for on-demand coverage. Consumer expectations may evolve to a point where insurance coverage would only be for a certain scope of activities. Premiums would be lower because there would be a more defined set of risks covered.

Prior to the availability of IoT data, different types of risks were bundled together under a single insurance policy cover. However, IoT enables assessments on individual risks to be made, as more granular data on customer behaviour become available. Insurers can fine-tune their coverages to potentially add or eliminate certain risks. This unbundling of insurance coverages would create differentiation from other products in the market. Customer satisfaction should improve due to the lower premiums for effectively the same coverage.

Emerging risks

Financial institutions risk breaching data privacy rules due to the nature of IoT data collection. Instead of active interaction for the collection of personal data, IoT enables passive collection. IoT devices seamlessly collect and transmit data, including personal data, across communication networks. Due to the high velocity of data collection, financial institutions may not be able to seek individuals' consent for every instance of data collection. Financial institutions may also not be able to anticipate and notify individuals of the full range of purposes for collecting their data at the outset.

However, regulators are alive to the challenges that IoT poses to privacy rules. There is an awareness that regulations need to keep up with technological innovations, while continuing to address consumer protection concerns. For example, Singapore's PDPC proposed to

recalibrate the balance between individual autonomy and corporate responsibility in situations where it is unlikely to have adverse impact on individuals. The PDPC proposed that if it is impractical to obtain consent, and where no adverse impact is expected on individuals, mere notification of purpose (instead of obtaining consent) can be sufficient for collection of personal data. In addition, where collection of personal data is for legitimate legal or business purposes, and subject to certain conditions, financial institutions may not need to notify individuals of the collection purposes. Nonetheless, these recommendations are only at the proposal stage, and current data protection rules continue to apply.

The vast amount of data created by IoT will also have to be analysed. Most financial institutions already struggle with the existing data volume that they have to process daily. The additional IoT data that have to be processed would likely overload existing legacy systems and processes. With their current capacities, financial institutions may not be able to fully utilise the benefits of IoT data.

Cybersecurity is a growing concern that financial institutions have to consider when using IoT. The real-time personal data of individuals collected is valuable and will likely attract cyber-attacks. Financial institutions are also a regulated sector and constitute 'critical information infrastructure' in certain jurisdictions. This requires financial institutions to put in place minimum security measures and internal processes to ensure that such IoT data are sufficiently secure. Such measures are challenging to install because of the huge volume of IoT data, but are necessary to ensure compliance.

Cost of Compliance

Playing catch-up

As technological developments continue to change the financial services landscape, regulators have to adapt and update current rules. New technology has changed the way financial services are delivered and the efficiency of various internal processes. These developments have resulted in a shift in market power from financial institutions to Payment Ecosystems that could not have been anticipated ten years ago. Due to emerging risks, regulatory frameworks need to be updated to ensure the integrity of the financial services industry and the protection of consumers.

The evolution of consumer behaviour in utilising Payment Ecosystems as gateways for services has blurred the lines between different categories of financial services. Businesses often do not differentiate between e-payment and online remittance activities. Increasingly, the same platform can allow customers to both fund payments and remittances directly from their bank accounts.

Regulators have acknowledged this shift in consumer behaviour, and have made proposals to update the law. In Singapore, the MAS has proposed to alter the regulatory regime so that it applies on an activity basis rather than on a payment systems basis. This is a more streamlined approach, and would allow the MAS to properly address specific issues such as consumer protection, access and corporate governance. Since it reflects consumers' use of technology in practice, it would also build public confidence and encourage a more significant uptake of e-payments.

As the nature of financial services migrates online, new risks are beginning to emerge. The potential threat of cybersecurity attacks and the consequential impact are becoming greater. Recently, there has been a surge in the number of cybersecurity incidents, including ransomware, cyber theft, banking fraud and disruptions to internet services.

Regulators are starting to put in place regulatory frameworks that proactively counter these emerging threats. The PRC's Cybersecurity law, which came into effect in June 2017, imposes statutory obligations on financial services providers to evaluate their cybersecurity risks at least once a year. Similarly, Singapore also issued a public consultation on its draft Cybersecurity Bill. Under this Bill, financial services providers have certain statutory duties including audit requirements, incident reporting and risk assessments.

More specifically, the emerging risk of cybersecurity attacks will leave financial services providers vulnerable to data leaks of their customers' personal data. In order to protect consumers, regulators have proposed to update the rules to shift the breach notification regime from a voluntary to a mandatory basis. Singapore's Personal Data Protection Commission (PDPC) has issued a public consultation to impose mandatory breach notifications obligations on financial institutions. By doing so, affected individuals who are notified of the breach are able to take steps to protect themselves from the impact of such breaches.

Regulatory attitudes

The attitude of regulators towards technological development in financial services is crucial in the uptake of such developments. Regulators play an important role in shaping the regulations applicable to financial services providers, and hence the regulatory burdens that such providers have to ensure compliance with. In addition, regulators are also responsible for the enforcement of such regulations, and have to ensure that they are applied evenly across the industry.

Development-friendly regulators can enhance a financial services provider's ecosystem by streamlining their regulatory obligations. For example, the MAS has proposed to condense the two current overlapping payment regulatory regimes into one. Platforms which conduct activities under both regimes would in the future only need to ensure compliance with one. Such a decrease in regulatory obligations would allow technology to develop more freely. More resources can also be devoted to actual development instead of ensuring regulatory compliance.

Where there is uncertainty about the compliance of technological developments, some regulators have allowed these to be tested out in regulatory sandboxes. During the sandbox-phase, such developments are exempt from having to comply with the full suite of applicable regulations. However, there is usually a list of criteria that needs to be satisfied before entry into the sandbox is allowed. For example, developments may be required to be innovative and be scalable to a wider audience after the sandbox period. The existence of such sandboxes encourage the development and use of new technology in the financial services space.

Regulators are also starting to acknowledge that technological developments are not bounded by national boundaries, and are cooperating with other countries to foster innovation. For example, the MAS has signed FinTech cooperation agreements with regulators not only from the region, but also from Australia, Japan and the United Kingdom. Such collaborations between regulators should lead to more comprehensive and integrated cross-border collaboration over FinTech developments. Regulators are ultimately concerned with ensuring financial stability and such cooperation would better enable that.

An enhanced understanding of individual customers through IoT data enables financial services providers to develop personalised offerings to meet their specific needs.

RegTech – an enabler

Regulatory technology (RegTech) solutions enable financial services providers to comply with increasingly stringent regulatory burdens more efficiently, at a lower cost. Since the global financial crisis, the amount of new regulatory regimes being introduced have steadily grown. In response, financial services providers have had to hire an ever-growing number of compliance personnel and external IT vendors to ensure compliance. This issue is particularly problematic in Asia, where financial services providers often have to keep up with various regulatory regimes, each with a different set of rules and requirements.

By using RegTech solutions, financial services providers can streamline their internal compliance processes. For example, instead of manually sorting out and monitoring the progress of compliance tasks via spreadsheets, RegTech solutions can be used to automate these tasks. For example, a compliance management software provides its clients with a compliance library that lists the compliance activities required for particular financial services providers. The software also allows clients to assign these responsibilities to specific employees. A system of red, amber and green charts for monitoring compliance activities is also provided.

The uptake of RegTech solutions has been swift, as they seek to empower financial services providers, and not to disrupt them. Financial services providers are incentivized to cooperate with one another since doing so would streamline their compliance processes and bring cost reductions for all of them. For example, there are currently various Know-Your-Customer (KYC) initiatives that are being discussed across Asia, where customers will only need to go through the on-boarding process once. Financial services providers would then allow one another to access customers' information when completing their own KYC process.

Consumers and regulators will also benefit from RegTech solutions. In a competitive landscape, the cost savings experienced by the financial services providers would be passed onto consumers. The streamlined compliance processes would also mean that customer experience would also be enhanced. Regulators would also benefit since the automation of compliance processes would eliminate inevitable human-errors. Financial services providers would also have better oversight of their data, allowing regulators to capture time-sensitive information whenever necessary. The Hong Kong Securities & Futures Commission (HKSFC) recently held a RegTech and FinTech Contact Day, where emerging RegTech innovations that intersected with securities regulation were displayed.

Similar to AI, RegTech can also streamline the compliance process by replacing low level cognitive tasks. Prior to utilising RegTech solutions, compliance teams in financial institutions need to manually monitor conversations between traders and their clients or review flagged email correspondences. Such tasks can be automated and be performed by an AI system, trained in natural language processing (NLP) to identify certain patterns in human communications. Not only will this be quicker and more cost-effective, such tasks will also be performed more accurately. However, human judgment and experience will still be necessary to respond to more complex scenarios, and to oversee the entire compliance process.

Potential game changer

The RegTech solution with potentially the most significant impact is the distributed ledger technology (DLT). The DLT is essentially a database that is decentralised, where each party keeps their own copy of all transactions on the network. Each transaction is encrypted and sent to every party on the network to be verified through consensus, and grouped into timestamped blocks of transactions. The DLT is also irreversible and contains a certain and verifiable record of every transaction ever made.

... a compliance management software provides its clients with a compliance library that lists the compliance activities required for particular financial services providers. The software also allows clients to assign these responsibilities to specific employees. A system of red, amber and green charts for monitoring compliance activities is also provided.

The decentralised nature of the DLT allows for the disintermediation of processes that require centralised third parties, such as clearing houses. Instead of going through a clearing house whenever funds are transferred, funds can move directly from one party to another because they would be validated by all the parties on the network. Disintermediation minimises the time needed to clear transactions, as well as the associated costs. It also makes networks less susceptible to cyber-attacks, as there is no central point of failure to be targeted.

Despite the vast potential of the DLT, the regulator's ability to implement it in practice has not yet been determined. Regulators have been starting to experiment with the DLT to determine its feasibility. The Bank of Canada recently completed an experiment to utilise the DLT to issue its own digital currency, including its transfer, settlement and destruction. More recently, the MAS commissioned a digital cash-on-ledger proof-of-concept (PoC) that utilises the DLT to facilitate inter-bank payments and settlements. The challenges that had to be explored include the interoperability between platforms, selective identification of relevant parties, appropriate levels of privacy, ability to scale and various system upgrades over time.

Other aspects of the DLT, such as its immutability and the encryption of data, enable it to also be utilised as a RegTech solution in the compliance process. For example, in order to streamline KYC customer on-boarding requirements, financial services providers can utilise the DLT to share verified data of that individual customer securely amongst themselves. KYC-Chain, a DLT developer based in Singapore, provides a secure platform for sharing verifiable identity data without compromising the privacy of the individuals involved.

CMS key contacts

Andrew Stott
Managing Partner, CMS Singapore
T +65 9232 5326
E andrew.stott@cms-cmno.com

Jeremy Tan
Director, CMS Holborn Asia
T +65 9730 1190
E jeremy.tan@holbornlaw.sg

Pern Yi Quah
Associate, CMS Singapore
T +65 9770 0337
E pernyi.quah@cms-cmno.com

CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

1710-0031560-4