ASEAN Plus Group's Guide to the Regulation of Payment Services in Asia-Pacific

The Member Firms:

HOLDING REDLICH

RHTLaw Cambodia

國浩律師事務所 GRANDALL LAW FIRM

F. ZIMMERN & CO. 施文律師行

AMA ANANT MERATHIA & ASSOCIATES

N&A NASOETION & ATYANTO

PCA Law Paul Cheah Associates

V&A VILLARAZA & ANGANGCO THE FIRM · EST. 1980

RHTLaw Asia

DR & AJU DAERYOOK & AJU

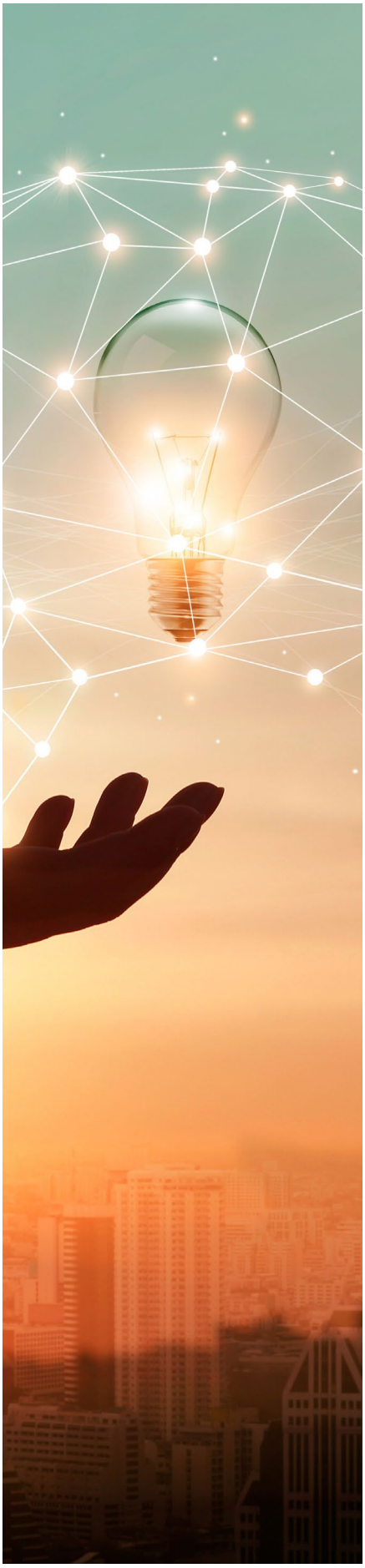
理律法律事務所 LEE AND LI ATTORNEYS-AT-LAW

BGL

RHTLaw Vietnam International Capabilities Delivered Locally

ASEAN+ We know ASIA.

Content



Foreword

This year, Southeast Asia continues to lead the world in adoption of digital practices like social media and messaging. With a young, tech-savvy population and the widespread use of mobile phones, the region is seeing a sharp increase in connectivity and quick payments for daily transactions.

The Association of Southeast Asian Nations (ASEAN) has championed the digital economy strongly in the past few years, and a majority of ASEAN countries have pioneered real-time domestic payments systems (some examples are Thailand - PromptPay, Indonesia - ATM Prima, and Philippines - Instapay), while enhancing their respective core payment infrastructure. ASEAN publicly stated its ambition to develop an instant cross-border payments system, to drive e-commerce and trade finance in the region with a population of 650 million.

The globalisation trend continues unabated, and the Covid-19 pandemic that appeared in the first half of 2020 has only strengthened the resolve of ASEAN to accelerate the adoption of e-payments in a seamless and convenient way.

However, the significant gaps in ASEAN's policy and regulatory infrastructure identified in the 2019 World Bank report "The Digital Economy in Southeast Asia" must be addressed decisively, so as to unlock further growth in the digital economy and an environment of mutuality and integration in the region.

This inaugural issue of the ASEAN Plus Group (APG)'s "Regulatory Guide to Payments" maps the latest state-of-play in the payments space in some of the regional group's jurisdictions: Cambodia, Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam. In addition, Australia, Bangladesh, China, India, South Korea and Taiwan (each significant economies with key relationships to ASEAN), are also represented in this Guide. All country chapters are written by leading regulatory lawyers from their respective jurisdictions, providing valuable insights into the respective supervisory regimes and key licensing and regulatory requirements in the area of payments including the related issues around technology, data privacy, financial crime and intellectual property.

It is noteworthy that while the supervisory frameworks for payment services in the region often share common principles, the specific laws and regulatory mechanisms may differ significantly between countries. Licensing of payments and associated services like banking, money transfer and even crypto assets, as well as compliance requirements are addressed in different ways across countries. In some cases regulatory exemptions and exceptions are available or permitted. This Guide aims to shine a light in this area of regulatory law where there are complexities and uncertainties in the different countries.

We hope that you will find this Guide practical and helpful. The APG law firms listed in this Guide would be pleased to render expert assistance to you in navigating the challenges and opportunities in the exciting and evolving payments space.

About Us

Economic and demographic indicators show ASEAN as a region on the verge of robust growth and change. Home to nearly 600 million people, it is one of the most populous regions in the world and boasts more than 10 percent of the emerging world's 2,000 largest companies. Asia's other economic heavyweights, China, Japan, South Korea and Taiwan, are virtually located in the backyard of ASEAN and are already strong engines of growth for Asia. Given their proximity and economic performance, ASEAN and North Asia are becoming increasingly unified as the region moves towards a more cooperative and integrated community.

Buoyed by this development, the ASEAN Plus Group was formed to support our clients throughout the ASEAN region and beyond.

ASEAN Plus Group (APG) is a group of full-service and well-established law firms in Asia, with strong local knowledge and international expertise. The group functions as a bridge for our clients to venture regionally with confidence. APG provides clients direct access to 14 lucrative markets in the region, including Singapore, Australia, Bangladesh, Cambodia, China, Hong Kong, India, Indonesia, Malaysia, Philippines, South Korea, Taiwan, Thailand and Vietnam. Together our APG team is not only attuned to the nuances of working in Asia, but also possesses the added perspective and expertise of an international firm.

What sets us apart is that we operate as a single unit while delivering multi-jurisdictional and multidisciplinary representation on some of the most complex transactions.

Australia

1. What is the payments landscape in Australia:
The types of activities, state of development of the market and new trends eg FinTech if any?

According to the Reserve Bank of Australia (**RBA**), most of the value of payments in the Australian economy come from non-cash payments. In 2019, on average, non-cash payments of around A$255 billion were made each business day. This equates to around 13 per cent of annual GDP. However, the use of cash as a method of payment remains common.

A small number of high-value payments where most of the value relates to the settlement of foreign exchange and securities market transactions is made through Australia's real-time gross settlement (**RTGS**) system. These payments make up about 82 per cent of the value of non-cash transactions. As large business payments have moved to the RTGS system, the importance of cheques have declined.

At the retail level, the use of electronic payment instruments has been rapidly increasing. Businesses and the government usually use direct entry credits for salary and social security payments, and consumers often pay bills this way. Direct entry payments account for most of the value of non-cash retail payments.

The Australian Payments Network is a self-regulatory body for Australia's payments industry. It coordinates the clearing of most payment instruments in Australia, including direct entry payments, cheques, debit cards, ATMs and high-value payments. Other payment clearing systems in Australia include MasterCard and Visa, eftpos Payments Australia Limited, BPAY and the New Payments Platform (**NPP**).

The final settlement of obligations occurs by entries to the payment providers' Exchange Settlement Accounts at the RBA. High-value payments are settled individually on an RTGS basis, and retail payments are settled on a net settlement basis.

Payments is one of the two largest FinTech sectors in Australia by number and amounts invested. Over the past few years, new technology has significantly impacted the payments market in Australia. For example, the launch of digital wallets such as Apple Pay, a surge in the use of "buy now, pay later" services and major Australian banks teaming together to develop a new app called "Beem" to enable the instant transfer of cash for free.

2. Which official agency regulates payments in Australia?

The Payments System Board (**PSB**) of Australia's central bank, the RBA, is responsible for overseeing the payments system and purchased payment facilities (**PPF**) (a facility where the holder of stored value makes a payment to another person on behalf of the user of the facility, for example, smart cards and electronic cash).

The Australian Securities and Investments Commission (**ASIC**) regulates non-cash payment facilities (**NCP**), for example, stored value cards, electronic cash and direct debit services. NCPs are a broader class of facilities which include PPFs.

Payment services may also be regulated by the Australian Prudential Regulation Authority (**APRA**).

The Australian Competition and Consumer Commission (**ACCC**) regulates competition and consumer law and so may also have a role to play, as may the Australian Transaction Reports and Analysis Centre (**AUSTRAC**) which collects and analyses financial reports and information to detect, deter and disrupt criminal abuse of the financial system.
Payment services may also be subject to regulation by State and Territory bodies.

Australia 

3. What are the main sources of laws regulating payments services in Australia?

The main source of law regulating payment services in Australia is federal legislation. Some examples of relevant legislation are as follows:

- The *Corporations Act 2001* (Cth);
- The *Payment Systems (Regulation) Act 1998* (**PSRA**)(Cth);
- The *Payment Systems and Netting Act 1998* (**PSNA**) (Cth);
- The *Reserve Bank Act 1959* (Cth);
- The *Banking Act 1959* (Cth);
- The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth); and
- The *Privacy Act* (1998) (Cth)

In addition to federal legislation, there is also the E-Payments Code, rules and regulations from the Australian Payments Network, and publications and guidance from regulators, for example, ASIC regulatory guides.

4. Describe the regulatory framework(s) for payment services operating in Australia, and the type of payment services that are regulated.

As outlined in Question 2, payment services are regulated by a variety of agencies in Australia. Australia has a complicated framework for payment regulation, and so it is important to seek advice to obtain a comprehensive understanding of the regulatory framework when considering entry into the Australian payments market. An overview of the regulatory framework is as follows:

RBA:

The PBS of the RBA is responsible for promoting safety, efficiency and competition in the payments system through the PSRA and the PSNA and has one of the most powerful mandates in the world regarding payment systems. However, the RBA has adopted a presumption in favour of self-regulation by industry such that it only regulates where it considers it necessary in the public interest, meaning that in practice, the scope of the RBA's regulation is fairly narrow.

Under the PSRA, the RBA is able to designate a payment system if it considers it in the public interest, and can then impose standards or an access regime on that designated system. For example, in 2008 the RBA designated the ATM system and determined an access regime to facilitate new entrants and prohibit the charging of interchange fees except in certain circumstances. Examples of other designated systems include MasterCard and Visa, and examples of standards include those relating to surcharging and interchange fees.

The RBA is currently undertaking a review into the regulation of retail payments.

With regards to PPFs, the RBA is also able to declare that the PSRA does not apply to a specific PPF or class of facilities, and may exempt corporations from the PSRA. Facilities that are exempted are loyalty schemes, gift card facilities, electronic road toll devices, pre-paid mobile phone accounts, as well as PPFs under which the total amount of obligations to make payments does not exceed A$10 million, and PPFs where the number of people to whom payments may be made using the PPF does not exceed 50 people. Corporations whose obligations are guaranteed by an Authorised Deposit-taking Institution (**ADI**) or by a Commonwealth, State or local government authority may also be exempt.

The *Corporations Act 2001* also provides the RBA with a formal regulatory role which involves ensuring that the infrastructure facilitating the clearing and settlement of transactions in financial markets promotes financial stability. The RBA has made financial stability standards for licensed clearing and settlement facilities; however these only apply to facilities that settle obligations of more than A$200 million per financial year.

The PSRA does not impose any licensing requirements.

ASIC:

Non-cash payment facilities (e.g. stored value cards, electronic cash and direct debit services) are regulated by ASIC. An entity that provides services relating to a non-cash payment facility will generally be required to hold an Australian Financial Services License (**AFSL**) and comply with the standard financial services disclosure and consumer protection requirements. These requirements include the obligation to comply with restrictions on handling client money and providing the necessary disclosure documents to customers.

However, there is a regulatory sandbox which allows eligible fintech companies to test some products and services for up to one year without holding an AFSL.

E-Payments Code

The E-Payments code is a voluntary code of practice which regulates consumer electronic payment transactions. This includes ATM, EFTPOS and credit card transactions, internet and mobile banking, online payments and BPAY. The code is administered by ASIC. Most banks, credit unions and building societies subscribe to it, as well as various non-banking businesses.

APRA:

Entities that carry on a banking business in Australia require an ADI license from APRA. APRA licenses PPF providers that have PPFs that hold customer funds above A$10 million, are redeemable on demand in Australian currency and are widely available (more than 50 users). PPF providers form a special class of ADIs which are given authorisation to undertake a limited range of banking activities. If an entity is already an ADI, it does not require further authorisation in the special class of PPF provider. Entities provided with PPF authorisation, as well as other ADIs that are also provide PPFs will be subject to prudential regulation by APRA.

Note that APRA's licensing framework has a limited application, as PayPal is currently the only PPF provider authorised by APRA.

5. How does Australia's payments licensing laws apply to cross-border business into your jurisdiction?

Generally, an entity that provides a non-cash payment facility that is not subject to an exemption will be required to hold an AFSL if it is 'carrying on a financial services business in Australia'. If an entity has a place of business in Australia, establishes or uses a share transfer office or share registration office in Australia, or deals with property in Australia, it will be deemed to carry on a business in Australia. Other facts that indicate an entity may be carrying on a business in Australia include continuous, systematic and repetitious activity connected with Australia, or a substantial one-off transaction.

An entity will need to hold an AFSL if it engages in conduct that is intended, or likely to induce people in Australia to use the financial services it provides.

However, it is important to consider that there are various exemptions that may apply *(please see Question 8)*.

Regarding APRA authorisation, APRA has stated that it will ordinarily impose as a condition of authorisation that PPF providers be incorporated in Australia. However, as discussed at question 4, the requirement to be licensed as an ADI by APRA has limited application.

Australia 

6. What are the main requirements to be licensed for payments in Australia?

As discussed above, the RBA does not impose any licensing requirements.

Entities who provide a facility for non-cash payments and do not fall within an exemption must apply for an AFSL. However, recognising that the definition of non-cash payment is broad, and compliance with the financial services regulatory regime may be disproportionately burdensome where there is minimal likelihood or extent of potential consumer detriment, ASIC has provided relief from some of the licensing and disclosure requirements to a number of non-cash payment facilities. These include

- Low-value non-cash payments (up to A$1,000 and no more than A$10M available for non-cash payments at any one time)
- Gift vouchers or cards
- Prepaid mobile phone accounts
- Loyalty schemes; and
- Road toll services

Further, non-cash payment facilities that only allow payments to be made to one person, or that only allow payments that are debited to a credit facility, or that are an incidental component of another facility where the main purpose of the other facility is not a financial product purpose, or that provide certain one-off electronic fund transfers may be eligible for an exemption.

As discussed at *Question 4*, entities that carry on a banking business must be licensed by APRA.

7. What is the process to become licensed for payments in Australia?

ASIC is responsible for issuing AFSLs and supervising those who hold an AFSL. ASIC has an "eLicensing system" in place that allows applicants to apply online. When assessing an entity's application, ASIC will consider

- The entity's competence to carry on the proposed financial services business;
- Whether the entity has sufficient resources to carry on the proposed business; and
- Whether the entity can meet the other obligations required of a licensee, including training, compliance, insurance and dispute resolution.

If ADI authorisation is required, prospective PPF provider applicants are encouraged to contact APRA at an early stage for a preliminary consultation, before submitting a final application. Amongst other things, an entity must demonstrate to APRA that its proposed or existing risk management and internal control systems are adequate and appropriate for monitoring and limiting risk exposure, that their accounting systems are suitable and that adequate arrangements have been established with external auditors.

Australia

8. What payment services "passporting" arrangements does Australia have with other countries, if any?

ASIC recently introduced a new regime whereby an entity may apply for foreign AFSL if it is authorised to provide financial services under a sufficiently equivalent overseas regulatory regime, but this only applies to entities wishing to provide the services to wholesale clients or professional investors in Australia. Each jurisdiction has different wholesale financial services permitted under a foreign AFSL. The jurisdictions are:

- Denmark
- France
- Germany
- Hong Kong
- Luxembourg
- Ontario, Canada
- Singapore
- Sweden
- United Kingdom; and
- United States

A foreign Australian Financial Services (**AFS**) licensee is exempt from certain obligations imposed upon regular AFS licensees on the basis that it is subject to sufficiently equivalent overseas regulatory requirements. The application process is also less burdensome.

Previously, foreign financial service providers providing services to wholesale clients were able to rely on either sufficient equivalence (the passport exemption) or limited connection relief, allowing them to operate without an AFSL. There is currently a two year transitional period, meaning that foreign financial service providers that have already obtained this relief can rely on it until 31 March 2022.

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Australia.

The main piece of legislation in Australia relating to AML and financial crime requirements is the *Anti-Money Laundering* and *Counter-Terrorism Financing Act 2006* (Cth).

Designated services under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* are regulated by AUSTRAC. Entities that provide designated services and have a geographical link to Australia are known as reporting entities and must enrol and/or register with AUSTRAC. Most providers of financial and credit services are providing designated services.

Reporting entities are subject to obligations such as reporting business activities and transactions to AUSTRAC, as well as record-keeping obligations and having an AML and counter-terrorism financing program in place.

There is also the *Financial Transaction Reports Act 1988* (Cth) which operates alongside the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, however most of the obligations have been replaced by obligations by the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

Australia

10. Describe the technology risk requirements that apply to payment services in Australia.

There are various technology risk requirements that an entity providing payment services in Australia must consider. ADIs must meet APRA's prudential requirements, one of which aims to ensure that the entity takes measures to be resilient against information security incidents.

Entities that fail to manage technology risk requirements may be in breach of provisions of the *Corporations Act 2001* (Cth), such as the duty imposed on directors to act with a reasonable degree of care and diligence. ASIC provides guidance on cyber resilience good practices, which include recommendations relating to board engagement such as periodic review by the board of cyber strategy, responsive governance, the use of third party experts to assess threats, detection systems, response and recovery planning, protective measures and training. In addition, there is an obligation for an AFS licensee to have adequate technology resources and risk management systems in place.

Companies may also be subject to the data privacy requirements described below at *Question 11*.

11. Describe the data privacy requirements that apply to payment services in Australia.

In Australia, the *Privacy Act 1998* (Cth) and the Australian Privacy Principles apply to entities with annual turnovers of more than A$3 million. The *Privacy Act 1998* and Australian Privacy Principles promote and protect the privacy of individuals and cover the collection, use, storage and disclosure of personal information in both government agencies and the private sector.

Entities covered the *Privacy Act 1998* and the Australian Privacy Principles are subject to a notifiable data breaches scheme, whereby they are required to notify the Office of the Australian Information Commissioner and affected individuals where a data breach is likely to result in serious harm to an individual whose personal information is involved.

The Australian government is currently conducting an inquiry into future directions for the Consumer Data Right, which gives consumers the right to safely access certain data about them held by businesses and share this with certain third parties. Open Banking is the application of the Consumer Data Right in the banking sector, which is set to be introduced in July this year. The government is considering adding a "write power" to the consumer data right which would allow recipient to make changes to information, for example, to make a payment from a customer's account on behalf of a customer without engaging a bank, rather than just read information. This may be advantageous for new payment services.

12. Describe how innovations and inventions are protected by law in Australia.

The *Patents Act 1990* (Cth) is administered by IP Australia. IP Australia can grant a standard patent for up to 20 years from the filing date of the application if an invention is new, involves and inventive step and is able to be made or used in an industry. An inventive step means that the invention is not an obvious thing to do for someone with knowledge and experience in the technological field of the invention.

Alternatively, an innovation patent may be granted for up to 8 years and is designed to protect inventions that do not meet the inventive threshold required for standard patents. However, innovation patents will be phased out in Australia, with the last day to file being 25 August 2021.

Entities can also trademark business logos and names.

Australia

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

The trading of cryptocurrencies is permissible in Australia, and people involved in cryptocurrencies are subject to a range of regulations.

People involved in cryptocurrencies are required to comply with Australian competition and consumer laws, such as ensuring that they do not engage in misleading or deceptive conduct. Digital currency exchange providers must register with AUSTRAC and comply with AML/CTF obligations.

Further, people who issue, give advice, deal in, or provide other intermediary services for cryptocurrencies that are considered a "financial product" (for example, an interest in a managed investment scheme or a security) will be subject to obligations under the Corporations Act 2001 and the Australian Securities and Investments Commission Act 2001. In particular, they will be required to hold an Australian financial services licence. Other considerations may include complying with the capital raising provisions of the Corporations Act 2001 for initial coin offerings, and for platforms enabling customers to buy cryptocurrencies, whether they are required to hold an Australian market licence.

It is also important to consider tax consequences of acquiring and disposing of cryptocurrency. A capital gains tax event may occur when someone disposes of cryptocurrency, and if that person makes a capital gain, some or all of the gain may be taxed. However if the disposal is part of a business, the profits made may be assessable as ordinary income rather than a capital gain.

Bangladesh

1. What is the payments landscape in Bangladesh:

The types of activities, state of development of the market and new trends eg FinTech if any?

Electronic payment landscape in Bangladesh constitutes of BEFTN (Bangladesh Electronic Fund Transfer Network), NPSB (National Payment Switch Bangladesh), RTGS (Real Time Gross Settlement) and MFS (Mobile Financial Services).

2. Which official agency regulates payments in Bangladesh?

The Central Bank of Bangladesh – Bangladesh Bank.

3. What are the main sources of laws regulating payments services in Bangladesh?

Primary Legislation- Bangladesh Bank Order-1972. Secondary Legislation:

- Bangladesh Payment and Settlement Systems Regulations-2014 ("**BPSSR-2014**") and
- Bangladesh Mobile Financial Services (MFS) Regulations – 2018 ("**MFSR-2018**").

4. Describe the regulatory framework(s) for payment services operating in Bangladesh, and the type of payment services that are regulated.

Regulatory framework: Same as response to query *Question 3*.

Types of payment services that are licenses/regulated:

- Payment Service Provided (**PSP**);
- Payment Systems Operator (**PSO**); and
- Mobile Financial Services (**MFS**).

5. How does Bangladesh's payments licensing laws apply to cross-border business into your jurisdiction?

Not applicable. Bangladesh has strict laws monitoring the outflow of currency to abroad as such the payment licensing laws apply to only transactions within Bangladesh.

Bangladesh

6. What are the main requirements to be licensed for payments in Bangladesh?

Applicants are required to exhibit, *inter alia*,

- Satisfactory financial background of sponsors;
- Robust governance arrangements in respect of proposed payment service business;
- Clear rules to solve disputes associated with payment services; and
- Safe, accessible and secured IT systems. (Other requirements listed under Section 5.1 of BPSSR-2014 and Section 7.2 of BMFSR-2018).

7. What is the process to become licensed for payments in Bangladesh?

After submission of relevant papers and documents before Bangladesh Bank, the PSP, PSO and MFS applicants are required to satisfactorily address any queries, information or shortcomings identified by Central Bank. In respect of MFS, if satisfied, Bangladesh Bank initially provides NOC based on which the applicant is expected to set up the business platform and apply for final license/approval for commencement of business within 1 (one) year from the date of NOC.

8. What payment services "passporting" arrangements does Bangladesh have with other countries, if any?

No passporting arrangement exists with other countries in the context of Bangladesh. MFS are allowed to with deal inward remittance only if the relevant transaction is carried out by way of money being credited into the Nostro Account of any scheduled banks. Outward remittance of any kind can only be carried out scheduled banks.

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Bangladesh.

The primary AML mechanism is various ceiling imposed on monthly and daily transactions carried out by MFS clients. Additionally, by dint of Section 5 (9) of BPSSR-2014 and Section 11 of BMFSR-2018, operators are required to comply with all relevant AML/CFT provisions and required to report suspicious transactions to the Bangladesh Financial Intelligence Unit (BFIU) of Bangladesh Bank periodically.

Bangladesh

10. Describe the technology risk requirements that apply to payment services in Bangladesh.

PSP and PSO are required to implement a safe and secured IT System with disaster recovery plan. MFS are additionally required to comply with ICT Security Guidelines for Scheduled Banks and Financial Institutions-2010 issued by Bangladesh Bank.

11. Describe the data privacy requirements that apply to payment services in Bangladesh.

Section 17 of BPSSR-2014 and Section 12.2 of BMFSR-2018 requires all operators to main privacy and confidentiality of information relating to their clients and the transactions. In addition, any breach of confidentiality by an operator may also lead to be convicted of an offence under the Digital Security Act-2018.

12. Describe how innovations and inventions are protected by law in Bangladesh.

"Computer Programmes" are eligible for copyright registration and protection under the Copyright Act-2000. Other innovations/ inventions which meet the definition of "patents" can be registered under the Patents Act-1911.

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

The position of cryptocurrency in Bangladesh has been clarified by Bangladesh Bank through various circulars and public notices over the years. As per Bangladesh Bank, cryptocurrencies are NOT a legal tender and there is NO recognized financial claim against a cryptocurrency as they are not authorized or regulated by any official body of any country in the world. Consequently, buying/trading of cryptocurrency by way of outward remittance from Bangladesh may tantamount to one or more offences under the Foreign Exchange Regulations and relevant Anti-Money Laundering laws.

Cambodia

1. What is the payments landscape in Cambodia:
The types of activities, state of development of the market and new trends eg FinTech if any?

Main Regulators: The National Bank of Cambodia ("NBC") and Ministry of Economy and Finance ("MEF")

Types of payment services in Cambodia:

- Service enabling cash to be paid into or withdrawn from a payment account, and any operations required for operating payment account;
- Execution of payment transactions including the transfer of funds on a payment account (such as direct debits, credit transfers, and car payments);
- Execution of payment transaction where funds are covered by a credit line for a payment service user;
- Issuing of payment instructions including issuing of electronic money and/or acquiring payment transaction;
- Money remittance;
- Payment initiation service; and
- Other payment services as defined by NBC.

Financial Technology (FinTech) is both relatively new and under-estimated terms in the Cambodian financial service industry.

2. Which official agency regulates payments in Cambodia?

The National Bank of Cambodia ("NBC") and Ministry of Economy and Finance ("MEF").

3. What are the main sources of laws regulating payments services in Cambodia?

A. **Primary Legislation:**
- Law on Banking and Financial Institution 1999

B. **Secondary Legislation:**
- Anti-Money Laundering and Combating the Financing of Terrorism 2007;
- Law on E-Commerce 2019;
- PRAKAS on the Management of Payment Service Provider 2017;
- PRAKAS on Third-Party Processors 2010;
- Technology Risk Management Guidelines

Cambodia

4. Describe the regulatory framework(s) for payment services operating in Cambodia, and the type of payment services that are regulated.

There are two types of payment services allowed to operate in Cambodia under the above-mentioned legislation;

A. Payment Service Provider ("PSP")

- **Applicant:** Existing BFIs intend to provide such service must seek prior approval from NBC while other external legal entities must apply for a license from NBC.
- **Regulator:** National Bank of Cambodia.
- **Regulation:** National Bank of Cambodia PRAKAS on the Management of Payment Service Provider date June 2017
- **Type of Payments:** See above response No.1.
- **Licensing Procedure:** *Please See Question 7*

B. Third-Party Processor ("TPP")

- **Applicant:** Legal entity who intends to be the TTP must be entrusted by an existing Bank and Financial Institutions ("BFIs") to act on behalf of the BFIs
- **Regulator:** National Bank of Cambodia
- **Regulation:** PRAKAS on Third-Party Processors dated August 2010
- **Type of Service:**
  i. A communication facility;
  ii. An inter-bank clearing facility;
  iii. Managing or operating of Bank's customers' accounts;
  iv. A service provider of money remittance by mobile phone or other means;
  v. A service provider of clearing and settlement of debit and credit card payment.
- **Licensing Procedure:** *Please See Question 7*

5. How does Cambodia's payments licensing laws apply to cross-border business into your jurisdiction?

N/A

Cambodia

6. What are the main requirements to be licensed for payments in Cambodia?

As per Article of the PRAKAS on the Management of Payment Service Provider, the main requirements for the applicant to acquire to PSP license are:

- Minimum Capital 8,000,000.00 KHR (USD 2 Million- with 5% to be deposited with NBC;
- A description of the type of payment services envisaged;
- A business plan including a forecast budget calculation for the first 3 (three) financial years which demonstrates that the applicant is able to employ the appropriate and proportionate systems, resources and procedures to operate soundly;
- Evidence that the payment service institution holds adequate capital;
- A description of the safeguarding-of-fund procedure
- A description of the applicant's governance arrangements and internal control mechanisms, including administrative, risk management, and accounting procedures, which are appropriate, sound and adequate;
- A description of the procedure in place to handle and follow up customer complaints, including monitor and incidents reporting mechanisms;
- A description of the process in place to file, monitor, track and restrict access to sensitive payment data;
- A description of business continuity arrangement including clear identification of the critical operations, effective contingency plans, and a procedure to regularly test and review the adequacy and efficiency of such plans;
- A description of the principles and definitions applied for the collection of statistical data on performance, transactions, and frauds;
- A security policy document, including a detailed risk assessment in relation to its payment services and a description of security control and mitigation measures taken to adequately protect payment service user against the risks identified;
- A description of the mechanism and the obligation in relation to AML/CFT;
- A description of the applicant's structural organization, including the intended use of agent and branches, agent control, outsourcing arrangements, and of its participation in a payment and settlement system;
- A description of the identity of the shareholder, the size of their shareholdings and evidence of their suitability taking into account the need to ensure the sound and prudent management;
- A description of the identity of directors and persons responsible for the management as well as evidence that they are of good repute and possess appropriate knowledge and experience to perform payment services;
- Information pertaining to the identity of statutory auditors and audit firms;
- Relevant legal documents and Articles of Association; and
- Identifying of the address of the applicant's head office.

Cambodia

7. What is the process to become licensed for payments in Cambodia?

A. **Payment Service Provider (PSP):**

Applicant other than the existing BFI shall complete the application form and submit to NBC. 6 (six) months upon the submission of application, NBC shall notify the applicant of its decision and issue its provisional approval with terms and conditions for the application to undertake, if all terms and conditions are satisfied then the NBC shall issue License to the applicant.

- **License validity:** 6 years – renewable upon 3 months prior notice to NBC.
- **Annual License Fees:** KHR 20 million (Est. USD 5000).
- **Enquiry Fees:** KHR 500,000 (Est. USD 120).
- **Application Fees:** KHR 2 million (Est. USD 500).

B. **Third Party Processor (TPP):**

TPP's applicant shall be first entrusted by a registered bank or a financial institution to be eligible to apply for a TPP licence with NBC. The application for license shall be approve or deny by NBC within 30 days after submission of the complete application date.

- **License validity:** 3 (three) years- renewable
- **Annual license fee** which is paid by the Bank on behalf of TPP every 15 January of each year is KHR 10 millions (Est. USD 2500)
- **Application Fee:** KHR 2 million(Est. USD 500)

8. What payment services "passporting" arrangements does Cambodia have with other countries, if any?

N/A

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Cambodia.

All financial institutions are required to report to Financial Intelligence Unit ("FIU") for any suspected transaction or any transaction has reasonable grounds to suspect of cash transaction which involves several connected cash transactions exceeding the amount of USD 10,000 is the proceeds of the offense, or are related to the financing of terrorism within 24 hours. Failing such might result in disciplinary sanctions and penal sanctions.

Cambodia 

10. Describe the technology risk requirements that apply to payment services in Cambodia.

NBC's Technology Risk Management Guidelines set out compliance requirements for the licensed PSP and TTP:

- Set daily transaction and amount limits for usage in case of payments, and allowed based on approved requests at respective branches only;
- Implement two-factor authentication for fund transfers and payments initiated for high-value transactions wherever possible;
- Provide an effective authentication method which should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and interoperability with other systems;
- Provide an authenticated session, together with its encryption protocol, which should remain intact throughout the interaction with the customer. In case of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means;
- Inform the customers through email or SMS as and when a new payee is added to the wallet (each new payee should be authorized by the customer based on a One Time Password from a second channel which also shows the payee details);
- Set up a risk-based transaction monitoring or surveillance process needs to be considered to monitor fraudulent use of wallets; and
- Implement appropriate measures to minimize exposure to a man-in-the-middle attack (MITM), man-in-the-browser (MITB) attack or man-in-the-application attack.

11. Describe the data privacy requirements that apply to payment services in Cambodia.

Cambodia has not enacted any comprehensive data protection legislation. However, as per Article 32 of Law on E-Commerce provides that all personal data that are electronically stored online must maintain privacy and confidentiality.

Cambodia

12. Describe how innovations and inventions are protected by law in Cambodia.

Innovations and inventions are protected through the registration under the Intellectual Property Rights (IPR) Protection such as:

Copyrights

The registration shall be done with Department of Copyright and Related Rights of Ministry of Culture and Fine Art. The duration of the protection is owner life-time plus 50 years.

Requirements Attachment[1]

- The confirmation letters
- Author or Creator List
- ID Card/passport
- Original work
- Transfer right letter (if any)
- A Business Registered Letter
- Other related to business laws
- License from owner (if concerning)
- Other contracts

Patent

The Patent application shall be filed with the Ministry of Industry, Science, Technology and Innovation which lasted for a period of 20 years from the date of filing. The patent applicant must pay an annual fee in advance to the Registrar for each year after the filing date of application of the patent. Moreover, the inventor must note that the invention need to disclose to public.

Requirements Attachment[2]

- A request: indicate each applicant's name, address, nationality and residence and shall be signed by each applicant
  Note*: Where applicant is the inventor, the request shall contain a statement to that effect, and, where he is not, it shall indicate each inventor's name and address and be accompanied by the statement justifying the applicant's right to the Patents. If the applicant is represented by an agent, the request shall so indicate and state the agent's name and address.
- A description
- One or more claims
- One or more drawings (where required), and
- An abstract.

Industrial Design

The registration shall be done with Ministry of Industry, Science, Technology and Innovation which lasted for a period of 5 years from the date of filing and shall be renewed for two further consecutive periods of 5 years.

Requirements Attachment[3]

- A request: indicate each applicant's name, address, nationality and residence and shall be signed by each applicant
  Note*: Where applicant is the creator, the request shall contain a statement to that effect, and, where he is not, it shall indicate each creator's name and address and be accompanied by the statement justifying the applicant's right to the registration of the industrial design. If the applicant is represented by an agent, the request shall so indicate and state the agent's name and address.
- Drawings, photographs or other adequate graphic representations of the article embodying the industrial design and
- An indication of the kind of products for which the industrial design is to be used.

[1] Based on the application forms of Patent. https://drive.google.com/file/d/1S3bSC3xjOQ0XyZPnlmNH7Yxlj0iuOIXF/view?usp=sharing
[2] Prakas (Declaration) on the Procedure for the Grant of Patents and Utility Model Certificates (2006)
[3] Prakas (Declaration) on the Procedure for Registration of Industrial Design (2006)

Cambodia 

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

On October 5th 2017, the National Bank of Cambodia ("NBC") issued a restriction to all domestic financial institutions to prohibit the purchase and trade of cryptocurrency- namely Bitcoin. However, with the formidable growth of the trading of Bitcoin and other cryptocurrencies in Cambodia, on May 11th 2018 the National Bank of Cambodia and the Securities and Exchange Commission of Cambodia along with the General-Commissariat of National Police issued a Joint Statement to the public that the propagation, circulation, buying, selling, trading, and settlement of Cryptocurrency without obtaining licenses from competent authorities are illegal activities and shall be penalized in accordance with applicable laws. However, as to date, there is no specific legal framework that regulates cryptocurrency. It is not clear as to what licenses are needed and what are the requirements to obtain such. This has actually created a gray-area and remained unclear to the cryptocurrency investors that whether such trading is legal or illegal ("permissible") but that has not stopped the circulation of trading and acceptance of cryptocurrencies in Cambodia. In June 2020, as a means to promote financial inclusion and the use of Khmer Riel (Cambodian national currency), the National Bank of Cambodia launched a interbank payment system called "Bakong" – an online application that enables users access to centralized digital payments platform and the use of digital currency- Central Bank Digital Currency ("CBDC"). This Bakong project allows NBC to play crucial roles of being a catalyst, an operator and an overseer of payment system in Cambodia.

China

1. What is the payments landscape in China:
The types of activities, state of development of the market and new trends eg FinTech if any?

China is leading the mobile payment revolution of which the unique landscape is reinforced by China's dedication to its tech giants. The story of China transitioning to a cashless society is about Alipay versus WeChat Pay. Collectively, these two technology giants hold roughly 90% of the mobile payment market in China.

Alipay was initially created in 2004 as a payment tool for Alibaba's e-commerce platform, the Ant Financial Services, which is the China's largest e-commerce network. Now, Alipay serves a record-breaking number of uses all around the world. However, Tencent's WeChat Pay entered into this market almost 10 years later, in 2013. It was expanded from its social networking and instant messaging app, WeChat. With billions of monthly active uses, WeChat is one of the most popular social media platforms in China, which helps its mobile payment system becomes one of the most widely used among Chinese consumers.

Other payment service providers, regardless of banks or those engaging in third party payment ("**TPP**") service, such as Union Mobile Pay, JD Bank Mobile Wallet share the rest 10% of the market share.

However, we cannot see those new payment trends as they are standing at the opposite side of traditional banking payment system. Actually, faced with rapidly evolving technology and potential growth in digital payment, traditional banks are frequently collaborating with those large internet companies, such as launching joint fintech labs, sharing systems, technologies and resource, etc.

2. Which official agency regulates payments in China?

Two main governmental authorities responsible for regulating payments in China are the People's Bank of China ("**PBOC**"), the central bank of China, and the China Banking and Insurance Regulatory Commission ("**CBIRC**"). There is also one important self-regulatory organization engaging in payment service regulation called the Payment and Clearance Association of China.

3. What are the main sources of laws regulating payments services in China?

For regulation of traditional banking related payment and clearance business, main sources of laws are:

- Law of the People's Republic of China on the People's Bank of China (2003);
- Payment and Settlement Measures (1997);
- Measures on the Settlement of Domestic Letters of Credit (2016);
- Notice of the People's Bank of China on Improving Personal Payment and Settlement Services (2007);
- Administrative Measures on Bank Card Acquiring Business (2013); and
- Notice by the People's Bank of China of Enhancing the Administration of Bankcard Acquiring Outsourcing (2015).

China

For non-banking payment business, including online and offline, main source of laws are:

- Administrative Measures on Payment Services Provided by Non-financial Institutions (2010) ("**2010 Payment Service Measure**");
- Administrative Measure on Online Payment Services Provided by Non-Bank Payment Institutions (2015)
- Measures on Management of Classification and Rating of Non-Bank Payment Institutions (2016);
- Notice on Non-Bank Payment Organization Network Payment Operations Shifting from the Direct Model to China NetsUnioun Platform Handling (2017);
- Bar Code Payment Service Specification (2017);
- Notice on the Relevant Requirements for Reporting of Large Amount Transactions by Non-Bank Payment Organizations (2018); and
- Measures on Management of Customer Provisions on Payment Platforms (2020 Revision).

4. Describe the regulatory framework(s) for payment services operating in China, and the type of payment services that are regulated.

Overall, payment services under regulation mainly include online payment, issuance and acceptance of prepaid card, bank card acceptance and other payment services specified by PBOC or CBIRC.

Under the whole regulatory framework, PBOC supervises the interbank lending market, interbank bond market, interbank foreign exchange market, and financial payment and clearance market. Most of the participants in these markets are financial institutions that are monitored by the regulators of their respective sectors. In addition to the regulatory requirements from their respective regulators, PBOC imposes regulatory requirements in connection with market entry, transactional activities, deposits and settlements in these markets. Meanwhile, CBIRC imposes requirements on banking institutions and non-banking financial institutions within its jurisdiction in connection with establishment and changes of institutions, business operations, corporate governance, finance and accounting, risk management and internal control, although such requirements may vary depending on the specific type of institution.

5. How does China's payments licensing laws apply to cross-border business into your jurisdiction?

Payment licensing is irrelevant with cross-border business.

For issue regarding cross-border business conducted in China, except for very limited scenarios under the *Administrative Measures on the Registration of Enterprises of Foreign Countries (Regions) Engaging in Production and Operational Activities within the Territory of China*, where a foreign company can conduct business operations directly in China upon approval, laws in China require that all foreign investors obtain a business license prior to carry out business in China.

With aspect to payment business particularly, since 2018, PBOC opened the market for online payment business to foreign investors. *(See Answer To Question 8)* Except for online payment business, no specific regulations in China have specially stated that whether foreign investors were allowed to engage in fintech related business, such as P2P lending, crowd-funding, etc. in China.

China

6. What are the main requirements to be licensed for payments in China?

Generally, PBOC regulates non-financial institutions providing payment services quite strictly, as payment business is seen as a sensitive area. Any TPP service provider in China must hold a Payment Business License issued by PBOC.

The applicant for a Payment Business License shall satisfy the following conditions:

- Being a limited liability company or limited share company established in China in accordance with law and a non-financial institution with legal person status;
- Having the minimum registered capital (see below);
- Having capital contributors as required (see below);
- Having more than five senior management personnel familiar with payment business;
- Having anti-money laundering measures that meet requirements;
- Having payment business facilities that meet the requirements;
- Having a sound organisational structure, internal control system and risk management measures;
- Having business offices and safety precautions; and
- The applicant and senior management personnel thereof is free of indictment for committing any illegal criminal activities by abusing payment business or handling payment business for illegal criminal activities for the last three years.

The minimum registered capital

Where an applicant intends to engage in payment business on a national scale, its minimum registered capital shall be RMB100,000,000; where it intends to engage in payment business within a province (autonomous region, centrally-administered municipality), its minimum registered capital shall be RMB30,000,000. The minimum registered capital shall be paid-in monetary capital.

Engagement in business on a national scale as mentioned includes the circumstances where the applicant establishes branches across provinces (autonomous regions and centrally-administered municipalities) or where a paying institution provide client with payment business service across provinces (autonomous regions and centrally-administered municipalities). Besides, PBOC may adjust the minimum registered capital of the applicant in accordance with relevant laws and regulations and policies of the State.

The major capital contributor

The major capital contributors of an applicant shall satisfy the following conditions:

- Being a limited liability company or limited share company established in accordance with law;
- As at the application date, having provided information processing support service for financial institutions for more than two years consecutively or have provided information processing support service for e-business activities for more than two years consecutively;
- As at the application date, having made profits for more than two years consecutively; and
- Free of any punishment for committing any illegal criminal activities by abusing the payment business or handling payment business for illegal criminal activities for the latest three years.

The major capital contributors as mentioned herein include the capital contributors that have the de-facto control of the applicant or that hold more than 10% of the equities of the applicant.

China

7. What is the process to become licensed for payments in China?

Below are major steps of application for the Payment Business License:

A. Submission of application

The applicant shall submit the following documents and materials to the branch of PBOC in charge of the region where it is located:

- Written application, specifying the name, domicile, registered capital and setup of organizational structure of the applicant, payment business to be applied for, etc.;
- A copy of the company's business license (duplicate);
- The articles of association;
- Verification certification;
- Financial and accounting reports audited by an accounting firm;
- Feasibility study report on payment business;
- Acceptance materials on anti-laundering measures;
- Certification on technical safety testing and authentication;
- Resume materials of senior management personnel;
- Certification that the applicant and the senior management personnel thereof are free of any criminal records;
- Relevant materials of major capital contributors; and
- Authenticity statement of application materials.

B. Public announcement after acceptance

The applicant shall make public announcement of the following items after receiving the acceptance notice:

- The registered capital and equity structure of the applicant;
- The name list, shareholding proportion and financial situation of major capital contributors;
- The payment business to be applied for;
- The business license of the applicant; and
- Certification on technical safety testing and authentication of payment business facilities.

C. Branch's preliminary examination and PBOC's issuance of licence

The branch of PBOC shall, in accordance with law, accept all applications that meet requirements, and report the preliminary examination opinion and application materials to PBOC. Where PBOC approves the application upon examination, it shall issue the Payment Business License in accordance with law and make a public announcement.

The Payment Business License shall be valid for five years as of the date of issuance. If a paying institution intends to continue engaging in the payment business after the expiration of the Payment Business License, it shall file an extension application to the branch of PBOC in charge of the region where it is located within six months before the expiration. The extension shall be valid for five years if the same is approved by PBOC.

China

8. What payment services "passporting" arrangements does China have with other countries, if any?

Foreign investors in online payments are particularly limited by regulatory restrictions. However, on 19 March 2018, PBOC issued the *Announcement No. 7* of 2018 ("**No. 7 Announcement**"), which allows qualified foreign-invested enterprises ("**FIEs**") to apply for Payment Business Licences under the existing legal regime applicable to domestically-owned entities. This is viewed by the market as a significant step towards opening up the payment industry to foreign investors, who were not permitted to enter prior to this No. 7 Announcement.

Therefore, to provide third-party electronic payment services in China, qualified foreign investors must establish a foreign-invested payment institution and obtain a Payment Business License in accordance with the 2010 Payment Services Measures. In addition, the No. 7 Announcement requires foreign-invested payment institutions to:

- Have secure operating and disaster recovery systems that meet the requisite standards and can independently process payment transactions in China;
- Store, process and analyze in Chinese territory all personal information and financial data collected and generated in China. Where international transfers of such information are necessary to process cross-border transactions, the consent of the data subject must be obtained, the overseas data recipients must be required to perform equivalent confidentiality obligations, and the transfer must comply with applicable laws and regulations; and
- Meet the requirements of PBOC on non-banking payment institutions in relation to corporate governance, daily operation, risk management, fund processing, reserve deposit, contingency plans, etc.

In November 2018, American Express became the first foreign card network to gain approval to establish a network to clear card payments in China.

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in China.

In China, financial institutions are statutorily required to establish the AML mechanisms and procedures to fully identify, evaluate and safeguard against risks of money laundering. AML obligations are imposed by analogy to other quasi-financial institutions or non-financial institutions.

A notable law that directly regulates fintech businesses, including payment services is the *Administrative Measures for Anti-Money Laundering and Counter-Terrorism Financing by Internet Financial Service Agencies (for Trial Implementation)* (the "**Implementation Measures**") promulgated by PBOC, CBIRC and the China Securities Regulatory Commission jointly in October 2018. The Implementation Measures basically imposed AML obligations applicable to traditional financial institutions, mutatis mutandis, to internet financial institutions. AML obligations mainly include establishing a sound system for monitoring large-value or suspicious transactions, conducting monitoring and analysis of fund transactions with each customer as a basic unit, monitoring and analysing customers and their businesses, transactions and processes. Service agencies shall also perform their duties diligently, implement the customer identification system, follow the principle of "know your customers", and take reasonable measures for customers, business relationships or transactions with different characteristics of money laundering or terrorist financing. They shall also understand the purposes and intentions of establishing business relationships, learn about the information of the beneficial owners of non-natural person customers and get to know whether the transaction of a natural person customer is operated by himself as well as the actual beneficiary of the transaction.

Another frequently happens crime related to payment service is crime of property violation, such as steal other people's property by monitoring calls and emails and using intercepted information (e.g. Alipay password).

China

10. Describe the technology risk requirements that apply to payment services in China.

As online transactions are "card-not-present" ones, possibilities of fraudulent payment, money laundering and tax avoidance develop alongside. While automated software detection systems are designed to interface with various payment systems and detect above accidents, payment that span multiple payment channels are still difficult to catch.

Meanwhile, online payment allows consumers in every corner of the world to proceed with the payment any time. Considering of the complexity, quantity and frequency of transactions around the world which could happen every second, the speed, stability and flexibility of interconnections between systems and vendors are central to the value proposition of digital payment. Should any system failure happen, the whole payment process might be crashed. Therefore, system availability and sustainability have grown in importance.

Further, a technological risk inherent in the internet is the threat to cyber security as electronic payment channels offer more opportunities for hackers and virus to access, which resulting to customer data theft, misuse and misappropriation. Therefore, how to collect, store, process, compass, classify, delete and prevent leakage of personal information, especially sensitive personal information which contains specific biological characteristics, is of great importance.

11. Describe the data privacy requirements that apply to payment services in China.

Lacking an overarching law on the protection of data privacy in China, there are many diverse and scattered laws, regulations and local ordinances in civil, criminal, and administrative branches. After years of legislation work, the *Cyber Security Law* has been the most principal reference regarding data privacy. As an supplement to the *Cyber Security Law*, the national standard *GB/T 35273-2020* provide a more detailed suggestive rules. *The Guidelines for Data Management of Banking Financial Institutions* promulgated by CBIRC in 2018 May is the most relevant departmental regulatory document. Thereby, basically all data privacy protection laws and regulations may be applicable to the payment services.

The main obligations espoused in these general laws and regulations on data controllers is to ensure that data is processed properly, and for companies and other legal entities to collect and use personal information with regards to:

- Principles of legitimacy, rightfulness and necessity when collecting and using personal information;
- Policies regarding the purpose, manner and scope of collecting and using personal information;
- Obtaining consent from any individual that has information collected;
- Refraining from collecting or using personal information in breach of any laws or regulations and with the agreement of any individual that has information collected; and
- Confidentiality and legality of the handling of the personal information.

Although the qualification requirements resulting from the domestic legal regime are numerous, potentially the largest stumbling block will be the data localization requirement under the current regulatory framework. For example, subject to the Cyber Security Law, any FIEs involved in payment services may be classified as Critical Information Infrastructures ("**CIIs**"), and made subject to the requirements that all personal information and financial data generated or collected in China must be stored, processed and analysed in China as a general principle and that cross-border data transfer is only allowed if that is necessary for business needs and the FIEs have passed a security assessment.

China

12. Describe how innovations and inventions are protected by law in China.

Innovations and inventions in China are protected as copyrightable works under the Copyright Law, as patentable creations under the Patent Law, and as trade secrets under the Anti-Unfair Competition Law.

Recently, China has been improving its intellectual property systems and the protection level in China has been brought onto an international level. Despite the fact that there are still rampant infringements, especially in some online e-commerce platforms, IP awareness has been improved, protections have been strengthened and the government has been making huge efforts to create an IP-friendly environment. Specialist intellectual property courts have been formed in Shanghai, Beijing and Guangzhou. And the Intellectual Property Tribunal, a new subdivision in the Supreme People's Court was formed at the end of 2018 which is responsible for all appeal cases concerning invention patents, utility model patents, technical secret, computer software, etc. The first internet court was also established in Hangzhou in August 2018 which is in charge of trying internet based disputes and online intellectual property infringements. Later, the second and the third internet Court were established in Beijing and Guangzhou respectively.

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

A. Government Attitude

The Chinese government does NOT recognize any cryptocurrency as legal currency. The court also holds a negative attitude toward this problem. Any banking system cannot accept or provide related services for cryptocurrencies. To protect investors and prevent financial risks, the Chinese government has taken a series of regulatory measures to crack down on activities related to cryptocurrency.

B. Legal Regime

However, current laws are silent as to whether the transaction of cryptocurrencies or cryptoassets is legally permissible. At present, there are two documents published by the People's Bank of China ("PBOC") guiding these issues.

In December 2013, PBOC, together with the Ministry of Industry and Information Technology, China Banking Regulatory Commission, China Securities Regulatory Commission and China Insurance Regulatory Commission, promulgated the Notice on Guarding Against Bitcoin Risks (Yin Fa [2013] No.289). It states that despite being called a "currency", bitcoin is not a currency in real sense given the fact that it is not issued by currency authorities and does not possess the legal status of being compulsorily used and accepted. Judging from its nature, bitcoin should be regarded as a specific virtual commodity: it does not possess the status a legal currency has, and cannot and should not be circulated in market as a currency. No financial institution or payment institution may offer bitcoin-related services.

In September 2017, PBOC, together with the Ministry of Industry and Information Technology, State Administration for Industry and Commerce, China Banking Regulatory Commission, China Securities Regulatory Commission and China Insurance Regulatory Commission, published the Announcement on Preventing Token Fundraising Risks. It defines that token fundraising shall be referred to a process where fundraisers distribute so-called "cryptocurrencies" to investors who make financial contributions in form of cryptocurrencies such as bitcoin and ether. By nature, it is an unapproved and illegal public financing activity, which involves financial crimes such as the illegal distribution of financial tokens, the illegal issuance of securities and illegal fundraising, financial fraud and pyramid sales. The token or cryptocurrencies that are distributed during token fundraising are not issued by the monetary authority, which have no legal properties like legally repayable and mandatory, have no equal legal standing as flat currency, and cannot circulate in the monetary market. All organizations and individuals are banned from starting illegal token fundraising activity. All financial institutions and non-banking payment institutions should not do any business related to token trading.

India

1. What is the payments landscape in India:
The types of activities, state of development of the market and new trends eg FinTech if any?

For a long time now, liquid cash transaction has been the dominant payment landscape in India. Cashless transactions via credit/debit cards have also gained immense popularity after the demonetization of 2016 in India. However, given the wide use of the internet and the increase in usage of smart phones, digital payment methods such as internet banking, e-wallets, payment banks and the like are a rising trend.

Types of Activities in India include:

A. Pre-paid Payment Instruments (PPI)

This is essentially the purchase of goods and services against its value as stored. Three types of PPI are:

- Closed system PPI which does not permit cash withdrawal, such as gift cards;
- Semi-closed system PPI which is used to purchase goods from a group of identified merchants such as e- wallets and;
- Open system PPI which can permit cash withdrawal such as ATM cards.

B. Unified Payment Interface (UPI) Payment

This enables real time payments from one bank to another via instant mobile transfers by use of QR codes, phone numbers and the like.

C. Peer-peer lending

In this type of activity, lenders and borrowers register to avail benefits and borrowing which is based on peer to peer transfer.

D. Payment Aggregators and Intermediaries

E-commerce platforms accept payments electronically and transfer the payment to respective merchants etc.

E. Digital Lenders

Online based lending/credit facility to SMEs and retail clients. Here the loan disbursement is online based.

F. Payment Banks

These are licensed platforms based through online medium, similar to the functions of a bank for a limited deposit threshold.

FinTech investments in India nearly doubled to USD 3.7 billion in 2019 from USD 1.9 billion in previous year according to a survey conducted by one of the popular MNCs, which shows that India is attracting a good number of investments and the FinTech market is booming.

India

2. Which official agency regulates payments in India?

A. There is no single regulatory agency for FinTech in India. The primary regulation is through the
- Reserve Bank of India (RBI) and
- Securities and Exchange Board of India (SEBI).

B. The various other aspects of FinTech are governed by the
- Telecom Regulatory Authority of India (TRAI) and
- Insurance Regulatory and Development Authority of India (IRDAI).

C. The FinTech Regulation is primarily under:
- The Ministry of Electronics and Information Technology (MEITY),
- Ministry of Corporate Affairs and
- Ministry of Finance.

3. What are the main sources of laws regulating payments services in India?

The main source of law regulating payments in India is the Payment and Settlement Systems Act, 2007, also the National Payments Corporation of India (NPCI), is an umbrella organisation for operating retail payments and settlement systems in India, which is an initiative of Reserve Bank of India (RBI) and Indian Banks' Association (IBA) and are deemed to be the main sources among many other which aid in specific areas such are InsurTech, RegTech, Data Privacy and the like.

4. Describe the regulatory framework(s) for payment services operating in India, and the type of payment services that are regulated.

The Payment and Settlement Systems Act, 2007 ('PSS Act, 2007'), governs and regulates all the modes of payment systems used in India. Under the PSS Act, 2007, two Regulations have been made by the RBI, namely,

- The Board for Regulation and Supervision of Payment and Settlement Systems Regulations, 2008 (BPSS Regulations) and
- The Payment and Settlement Systems Regulations, 2008 ('PPS Regulations, 2008').
- There is also 'Policy Guidelines on Issuance and Operation of PPIs' (Master Direction DPSS.CO.PD. No.1164/02.14.006/2017-18).

India

5. How does India's payments licensing laws apply to cross-border business into your jurisdiction?

Foreign transactions are governed by the Foreign Exchange Management Act, 1999 ("FEMA") and subsequent rules and regulations under it. This along with RBI and the Foreign Direct Investment (FDI) Policy together ensure that cross border transactions are done efficiently. Payment Banks are regulated to allow remittance from various countries. The PPIs are also issues in various semi- closed and open systems to ensure secure transactions across borders. The PSS Act 2007 does not prohibit foreign entities from operating a payment system in India and the Act does not discriminate/differentiate between foreign entities and domestic entities.

6. What are the main requirements to be licensed for payments in India?

A payments license is preliminary given to Banks and Non-banking Financial Companies (NBFC). The company must be registered under the Companies Act, 2013 and a requisite amount of capital/ net worth must be present. Fintech Companies are licensed under the NBFC category in India. In case of foreign banks, they must be set up in India on basis of public interest and the incorporated country(home country) does not discriminate a company registered in India.

7. What is the process to become licensed for payments in India?

Banks are to register with the RBI under the Banking Regulation Act, 1949 and NBFCs under the RBI Act, 1934. An application is to be submitted to the RBI, either in online or physical mode and along with relevant documents to the respective regional office of the RBI. A company application reference number would be given and upon the verification of documents the company is added to the list of licensed payment companies and a licence is given to the company.

8. What payment services "passporting" arrangements does India have with other countries, if any?

India does not allow for any "passporting arrangements" and FinTech companies are required to register separately in the Indian jurisdiction.

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in India.

Anti-money laundering in India is regulated through Prevention of Money Laundering Act, 2002 (PMLA) along with its rules and RBIs Master Directions on Know Your Customer Guidelines. This ensures that each customer verifies their identity before registering with the payment services. E-KYC facilities are also made available to ensure far outreach of the Guidelines. In lieu of privacy of customers, the identity is verified without access to the files of the customer, though QR scanning, masked identity verification and so on. PMLA also requires banking companies and Financial Institutions to maintain record of all transactions and furnish such information to the authority within the prescribed time limit. This is applicable for single transactions or a series of transactions interconnected with each other.

India

10. Describe the technology risk requirements that apply to payment services in India.

A strong risk management system is necessary to meet the challenges of fraud and ensure customer protection. E-commerce entities and merchants are required to put in place adequate information and data security infrastructure and systems for prevention and detection of frauds. They are to adopt the technology related recommendations as stated in the Guidelines on Regulation of Payment Aggregators and Payment Gateways, which are as below:

- The entities shall carry a comprehensive risk assessment of their people to ensure security.
- Data security standards and best practices like PCI-DSS, PA-DSS, latest encryption standards, transport channel security, etc., are to be implemented.
- The entities are required to report any sort of breach to the regulator (RBI) within the prescribed time limit.
- Entities are required to comply with majority of the security assessment during the merchant on-boarding procedure itself.
- Entities are required to carry out cyber security audit and reports internally on quarterly basis and externally on annual basis.
- An IT policy will be framed for regular management of IT functions and ensure that detailed documentation in terms of procedures and guidelines exists and are implemented. The strategic plan and policy are to be reviewed annually.
- The entities are to maintain an "enterprise data dictionary" incorporating the organisation's data syntax rules. This shall enable sharing of data across applications and systems, promote a common understanding of data across IT and business users and prevent creation of incompatible data elements.
- The risk assessment shall identify each threat or vulnerability.
- There are to be documented standards or procedures for administering an application system, which are approved by the application owner and kept up-to-date.
- Trained staff are required to perform based on the specific skillset adhered to the entities functions.
- The entities shall consider assessing their IT maturity level and shall select encryption algorithms, based on well-known international standards.
- The entities shall take preventive measures to ensure storing data in infrastructure that do not belong to external jurisdictions
- Payment applications shall be developed as per PA-DSS guidelines and complied with as required. The entities shall review PCI-DSS compliance status as part of merchant on-boarding process.

Entities are required to submit the System Audit Report, including cyber security audit conducted by CERT-In empanelled auditors, within two months of the close of their financial year to the respective Regional Office of Department of Payment and Settlement Systems (DPSS), RBI.

It must be noted that India is a developing country with vast population, it is certainly a challenge to keep up with the fast pace of technology. Technology over the past decade has been prevalent and is consistently developing and the Cyber Security Laws in India are still developing to meet these challenges.

India

11. Describe the data privacy requirements that apply to payment services in India.

Data privacy is quite important in the Indian jurisdiction, E-KYC earlier was considered a breach of the personal data associated with the Aadhaar (unique identification), however through a judgement given in the Supreme Court, access to such data was barred and later on developments towards e-KYC in masked/ QR forms were encouraged. The Information Technology Act, 2000 and the rules there under govern the protection of personal data. In August 2017, the Union Ministry of Electronics & Information Technology (MEITY) constituted an Expert Committee to study and identify key data protection issues headed by Supreme Court Judge (retired) Justice B N Srikrishna and included members from government, academia, and industries.
The requirements for data protection as per RBI guidelines are as follows:

- Data localization for payment services- All payment system providers and their intermediaries, third party vendors, service providers etc. must store all their data in India (certain exceptions are available to foreign transactions)
- The compliance report of such storage of data must be report to the RBI
- This enable monitoring of supervision of such data

12. Describe how innovations and inventions are protected by law in India.

Innovations and Inventions are protected under the Patent Act 1970. Software is not protected under Indian laws under the ambit of patent hence copyright is sought for software, however if the said software is part of an invention then it may be protected under Patent Act. Essentially, copyright for software is employed by software companies to reduce and prevent unauthorized copying of the software.

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

Blockchain and Cryptocurrency are new areas in India, and the regulation is lacking. Cryptocurrency transactions and trading have not been permitted, and the same has been legalized only on 4th March 2020 vide a Supreme Court Judgment, wherein the Court quashed an RBI circular which prevented banks from providing services in support of cryptocurrencies. By virtue of this Judgement, the ban on cryptocurrencies were deemed to be lifted, however the Government is considering to enforce the Draft Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019 to ensure that there is a ban on cryptocurrency transactions. However the Draft bill leaves scope for the RBI to introduce digital rupee as legal tender and may notify foreign digital currency (recognized in the foreign jurisdiction) as foreign currency.

Indonesia

1. What is the payments landscape in Indonesia:

The types of activities, state of development of the market and new trends eg FinTech if any?

The rise of innovative technology start-ups in the financial sector ("**Fintech**") for the past five years has changed the landscape of payment services in Indonesia. The involvement of a new party in providing the payment transaction process affects the payment infrastructure as well as the payment mechanism in Indonesia. Bank Indonesia ("**BI**"), as the central bank of Indonesia, has the authority regulating activities related to payment activities and payment devices in Indonesia, has passed several regulations facilitating financial technology arrangements, financial regulatory sandbox and payment services, to respond to the Fintech development. In general, the payment activities in Indonesia classified into the following activities:[4]

- Pre-transaction;
- Authorization;
- Clearing;
- Settlement; and
- Post-transaction.

Any party who intends to engage in payment activities as the payment services providers shall be categorized into the one of above classifications and required to obtain a license from BI.

2. Which official agency regulates payments in Indonesia?

Bank Indonesia holds the main regulator with regard to the payments system and Fintech that engage payment systems in Indonesia. For Fintech that is classified as fund-lending services and any other forms of Fintech except payment system shall be supervised by the Financial Services Authorities or Otoritas Jasa Keuangan ("**OJK**").

3. What are the main sources of laws regulating payments services in Indonesia?

The primary regulations are as follows:

- Law No. 11 of 2008 on the Electronic Information and Transactions as lastly amended by Law No. 19 of 2016;
- Bank Indonesia Regulation No. 18/40/PBI/2016 of 2016 on the Operation of Payment Transaction Process ("**BI Rule 18/2016**");
- Bank Indonesia Regulation No. 19/12/PBI/2017 of 2017 on the Implementation of Financial Technology ("**BI Rule 19/2017**");
- OJK Regulation No. 77/POJK.01/2016 of 2016 on the Technology-Based Fund-Lending Services; and
- OJK Regulation No. 13/POJK.02/2018 of 2018 on the Digital Financial Innovations in the Financial Services Sector.

[4] Article 2 BI Reg 18/2016

Indonesia

4. Describe the regulatory framework(s) for payment services operating in Indonesia, and the type of payment services that are regulated.

Under the BI Rule 18/2016, Payment Services provider is further detailed and breakdown into the following activities:

- Principal;
- Switching provider;
- Issuer;
- Acquirer;
- Payment gateway provider;
- Payment clearing provider;
- Final settlement provider;
- Fund transfer provider;
- E-wallet; and
- Other payment services providers.

5. How does Indonesia's payments licensing laws apply to cross-border business into your jurisdiction?

Cross border business licensing is not applicable in Indonesia. Foreign payment services providers are required to established an Indonesian entity and apply for Foreign Payment Services license to BI in order to perform payment services activities in Indonesia.

6. What are the main requirements to be licensed for payments in Indonesia?

Each payment system service provider must first obtain a license from Bank Indonesia with the following requirements:

A. Business entity and shares ownership[5]

In order to meet general requirements, to become a principal, a switching provider, a payment clearing provider, and/or final settlement provider must be in the form of limited liability company with at least 80% of its shares owned by Indonesian citizens and/or Indonesian legal entities. In this case, if there is any foreign ownership, then the calculation of foreign ownership includes direct and indirect ownership.

B. Business fields[6]

To become a switching provider or a payment gateway provider as well as an electronic wallet provider, the business actor must be in the form of a bank or a non-bank financial institution as a limited liability company. Specifically, for switching providers or payment gateway providers, institutions other than banks must conduct business activities in the field of information technology and/or payment systems.

C. Feasibility aspects[7]

Switching provider and/or payment gateway provider and/or electronic wallet provider must meet the following eligibility requirements:

- Legality and company profile;
- Law compliance;
- Operational readiness;
- System security and reliability;
- Business feasibility;
- Adequacy of risk management; and
- Consumer protection.

[5] Article 5 paragraph (2) and (3) BI Rule18/2016
[6] Article 6 and 7 BI Rule18/2016
[7] Article 9 BI Rule18/2016

Indonesia

After obtaining the license as referred, the provider is also required to obtain prior approval from Bank Indonesia in the event that it will carry out activities as follows:

- Development of payment system service activities;
- Product development and payment system service activities; and / or
- Cooperation with other parties.[8]

7. What is the process to become licensed for payments in Indonesia?

In applying for a license as a Payment System Service Provider, the provider must submit an application to BI accompanied by supporting documents. In processing the application, BI will perform the following actions[9]:

- Administrative research;
- Business feasibility analysis; and
- Examination of banks or institutions other than banks (e.g., site visit);

The process will take six months and may be extended for another six months. Bank Indonesia will then determine the decision on whether to approve or reject the proposed license application.

8. What payment services "passporting" arrangements does Indonesia have with other countries, if any?

"Passporting" arrangement for Payment Services does not exist under Indonesian regulation. Payment Services companies are required to obtain a license from BI in order to perform payment services activities in Indonesia.

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Indonesia.

A. Enforcement of anti-money laundering ("AML") in general

The application of AML in Indonesia is regulated through Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering ("Law 8/2020") and all related implementing regulations. Law 8/2020 explains that money laundering is any act that fulfills the elements of a criminal offense as specified in the regulation. This regulation is the legal basis of all AML regulations in Indonesia.

[8] Article 4 BI Rule 18/2016
[9] Article 15 BI Rule 18/2016

Indonesia

B. AML requirements based on Bank Indonesia regulations and Prevention of Terrorism Funding

Bank Indonesia also issued specific regulations for payment system service providers other than banks through Bank Indonesia Regulation No. 19/10/PBI/2017 concerning the Application of Anti-Money Laundering and Prevention of Terrorism Funding for Non-Bank Payment System Service Providers and Non-Bank Currency Exchange Business Providers. Pursuant to this regulation, the provider must implement the followings:

- Duties and responsibilities of the board of directors and active supervision of the board of commissioners;
- Written policies and procedures;
- Risk management process;
- Resource management; and
- Internal control system.

10. Describe the technology risk requirements that apply to payment services in Indonesia.

Under the BI Rule19/2017, BI requires every registered Payment Services Providers / Fintech to implement the application of risk management and prudential principles. In implementing risk management, Payment Services Providers / Fintech need to implement risk identification, measurement, monitoring, and risk forecasting for its business activities. The regulation also allows Payment Service Providers to cooperate with supporting services for the Payment Services e.g., the data centre and/or disaster recovery centre security features for the payment instrument and/or payment transactions[10].

11. Describe the data privacy requirements that apply to payment services in Indonesia.

Protection of personal data in electronic systems provided under Minister of Communication and Information Technology Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems. Based on such regulation, personal data protection in an electronic system is carried out in the following process:

- Acquisition and collection;
- Processing and analyzing;
- Storage;
- Display, announcement, delivery, dissemination, and/or opening of access; and
- Erasure.

[10] Article 3 paragraph (3) BI Rule18/2016

Indonesia

12. Describe how innovations and inventions are protected by law in Indonesia.

In general, the protection of innovation and invention in Indonesia for the financial technology sector, provided under the following regulations:

A. **Law No.13 of2016 on Patent ("Patent Law"):**

Patent Law protects an invention, in this case, is interpreted as an inventor's idea that is drawn into a specific problem-solving activity in the field of technology in the form of a product or process, or improvement and development of a product or process.

An invention will be considered new if it is not the same as the existing technology when the application for registration that meets the Patent Law has been received[11]. Patents are generally granted for a period of 20 years and cannot be extended[12]. However, in Patent Law, also known as the term simple patent, which is a new invention in the form of the development of an existing product or process, and can be applied in an industry that is valid for a period of 10 years[13].

B. **Law No. 28 of 2014 on Copyrights ("Copyrights Law"):**

Indonesian Copyrights Law protects several creations, on which, when seeking something related to the Fintech industry, this could be in the form of a computer program. The computer program here is defined as a set of instructions expressed in the form of language, code, scheme, or in any form intended for the computer to work to perform certain functions or to achieve certain results[14]. The validity period of economic rights granted for computer programs is 50 years since the announcement was first made[15].

C. **Law No. 30 of 2000 on Trade Secret ("Trade Secret Law"):**

Trade secret is defined as information that is not known by the public in the field of technology and/or business, has economic value as it is useful in business activities, and is kept confidential by the owner of trade secrets. The scope of protection based on Trade Secret Law covers production methods, processing methods, sales methods, or other information in the field of technology and/or business that has economic value and is not known by the general public[16]. The holder of trade secret rights based on this law is to use its right of his own as well as to give licenses to or prohibit other parties from using it. However, the holder may also disclose to other parties for commercial purposes[17].

[11] Article 5 of Patent Law
[12] Article 22 of Patent Law
[13] Article 3 and 23 of Patent Law
[14] Article 1 number 9 of Copyrights Law
[15] Article 50 of Copyrights Law
[16] Article 2 of Trade Secret Law
[17] Article 4 of Trade Secret Law

Indonesia

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

Bank Indonesia prohibits the use of cryptocurrency for payment. Rupiah remains the sole official currency as mandated by Law No. 7 of 2011 on Currency.

Even though cryptocurrency could not be used as a tool payment, cryptoassets can be traded through the supervision of the Indonesian Commodity Futures Trading Regulatory Agency ("Bappebti"). In 2019, Bappebti issued a regulatory framework for the trading of cryptocurrency with Bappebti Regulation No. 5 of 2019 on Technical Provisions for the Implementation of the Crypto Asset Physical Market on the Futures Exchange as lastly amended by Bappebti Regulation No. 3 of 2020 ("Bappebti Reg 5/2019").

Under the Bappebti Reg 5/2019, cryptoassets may only be traded after being registered in the cryptoasset list at the Bappebti. The crypto assets must satisfy the following with requirement:

- Created based on distributed ledger technology;
- In the form of utility crypto assets or crypto-backed asset;
- Market capitalization value ranked in the 500 (five hundred) large market capitalization of crypto assets for utility crypto assets;
- Included in the largest crypto assets exchange transaction in the world;
- Has economic benefits, such as taxation, growing the informatics industry and the competence of experts in the field of informatics (digital talent); and;
- Risks have been assessed, including threats of money-laundering and terrorism funding and the proliferation of weapons of mass destruction.

  In transacting the crypto assets, the crypto assets trading system will include following parties clearing agencies, cryptoassets traders, customers of crypto assets customers, and crypto assets storage providers. The futures exchange may appoint physical traders of crypto assets to facilitate the physical market transactions of the crypto assets, with prior approval from the Head of Bappebti.

Malaysia

1. What is the payments landscape in Malaysia:
The types of activities, state of development of the market and new trends eg FinTech if any?

A. Malaysia's fintech industry has been dubbed the "emerging fintech hub in Asia" by Ernst & Young in a recent ASEAN FinTech Census with some 166 financial technology (Fintech) companies operating in Malaysia as of July 2019.

B. It has been estimated that the biggest fintech product is digital payment, which comprises 25% of the fintech ecosystem. In the first half of 2019 alone, digital payment globally has reached US$4.1 trillion. Mobile payments, a subset of digital payments, is on track to break the US$1 trillion mark in 2020.

C. The above trend is expected to influence the payments landscape in Malaysia in the context of its own digital penetration landscape.

D. The following is a snapshot of Malaysia's digital landscape in 2018.

Malaysia: At a glance	
Population	31.6 million
Average age	28.7 years
Gross domestic product	$314.7 billion
E-commerce market value	$4 billion
Mobile commerce market size	$1.9 billion
Mobile commerce as a percentage of e-commerce market size	47%
Internet penetration	80.1%
Smartphone penetration	63.9%
Bank account penetration	85%
Card penetration per capita	1.74

E. Driven by a relatively high internet penetration rate, the e-commerce market in Malaysia is going from strength to strength and is forecast to grow at a compound annual growth rate of 24 percent a year. A 63.9 % smart phone penetration in Malaysia provide a solid foundation for mobile wallets to thrive. Indeed, internet penetration in Malaysia is high (80%) as more and more providers enter the space. Existing mobile wallet users cite convenience as the biggest driver of usage, and adoption will continue to rise driven by the increasing popularity of app-based online shops, ride hailing services, online gaming, cinema ticket booking etc.

F. The traditional financial institutions have always prioritized to serve the first-tier customers, preventing much of society to be part of the main financial stream and accessing the most basic financial services such as savings account and credit lines. These financial institutions have a certain cost structure to keep up with, thus understandably impose higher financial fees unaffordable to the many less affluent.

Malaysia

G. Thus, the emergence of Fintech makes it the most exciting development of today and will very well be the solution to broaden the financial inclusion. Fintech stands at an advantage with their appealing combo; low cost high tech financial services and strong grasp of consumer habits to tap into the unbanked segment. Financial institutions see this development as a possible threat to the existing formal -financial ecosystem, thus their businesses. Despite that, regulators continue to push for Fintech to be an indispensable part of the ecosystem, in order to generate a competitive landscape. The regulatory sandboxes conceived for example, is aspired to catalyze innovative Fintech developments, involving all players of the industry. Platforms such as this should be connected to create more of a symbiotic relationship rather than of a competitive one, between financial institutions and Fintech companies, to co-exist and complement each other.

H. At the end of the day, inadvertently this reassuring development will no doubt benefit consumers the most. This ecosystem should bring to the table a strong value proposition for product offerings to cater for all, especially to the ¬financially underserved, the main problems faced by SMEs and the unbanked households, that is to bridge the payment and credit gap.

I. In April 2019, the Ministry of Communications and Multimedia launched its five-year National Fiberisation and Connectivity Plan (NFCP) under which the Malaysian Communications and Multimedia Commission (MCMC) has been tasked with developing Malaysia's broadband network to improve on the three key areas of affordability, coverage and speed.

J. Payments Network Malaysia launched Malaysia's first real-time retail payments platform in January 2019, which is expected to boost electronic payments by modernizing Malaysia's payments infrastructure. Features include instant credit transfer via mobile number and national security number to both citizens and businesses. Further features are set be rolled out in the coming years, including real-time debit transfers and e-mandates.

K. Malaysia's e-commerce fraud rates appear positive: digital payment provider iPay88 reported fraud occurring in just 0.02 percent of transactions in 2018, a drop from 0.03 percent in 2017. The introduction of the Consumer Protection (Electronic Trade Transactions) Regulations in 2012 is thought to have assisted in cutting down on incidences of e-commerce fraud.

L. In February 2020 BNM issued guidelines for Licensed banks and licensed Islamic banks to apply for a digital bank license separate from their current licensed entity should they wish to carry on digital banking business or Islamic digital banking business in a joint venture with other parties. However, this does not preclude licensed banks and licensed Islamic banks from digitalising their current business operations, which remains within the scope of their existing banking license and does not require the application of a separate digital bank license.

M. Malaysia's preferred payment method.

Payment Method	Payment Split (%)
Bank transfer	46%
Card	29%
Other	11%
Digital wallet	7%
Cash	7%

Malaysia

N. Today, there are 44 banks and digital payment start-ups that have obtained approval to issue e-money via the different mobile apps. Despite the e-commerce potential and high number of players in the digital payments space has resulted in a highly fragmented landscape. As illustration Malaysia has 44 e-wallet players operating in a market of 31 million people as compared to Indonesia with its 37 e-wallet providers operating in a market of 264 million population It is expected that the market will consolidate to a few players in the coming years who provide the best features with the best use cases to the demanding consumer.

O. Expansion of e-wallet providers going beyond payment solutions is expected to dethrone cards and cash in all consumer segments e.g utility bill payments, transport services, loans, wealth management, insurance, SME working capital etc.

P. Citing BNM data for value of transactions in 2017 was staggering with online banking recorded with Rm6.5trillion, credit card transactions at Rm15. Billion, mobile transactions at Rm30 billion and e-money at Rm9.1 billion.

Q. Digital payment players have begun putting in the fundamentals and infrastructure to meet the consumer demand for convenience to transact goods and services via e money.

The following list some of the e wallet players in Malaysia in 2018.

Payments (40)

Wallets (38)

2. Which official agency regulates payments in Malaysia?

- Ministry of Finance oversees economic and fiscal policy of the government and implemented by the politically independent Central Bank of Malaysia (Bank Negara Malaysia). The regulation of payment system falls under the purview of Bank Negara Malaysia (BNM) which deals with financial matters of the country.

- Ministry of Domestic Trade and Consumer Affairs is responsible for domestic trade, companies, competition, price control amongst other matters.

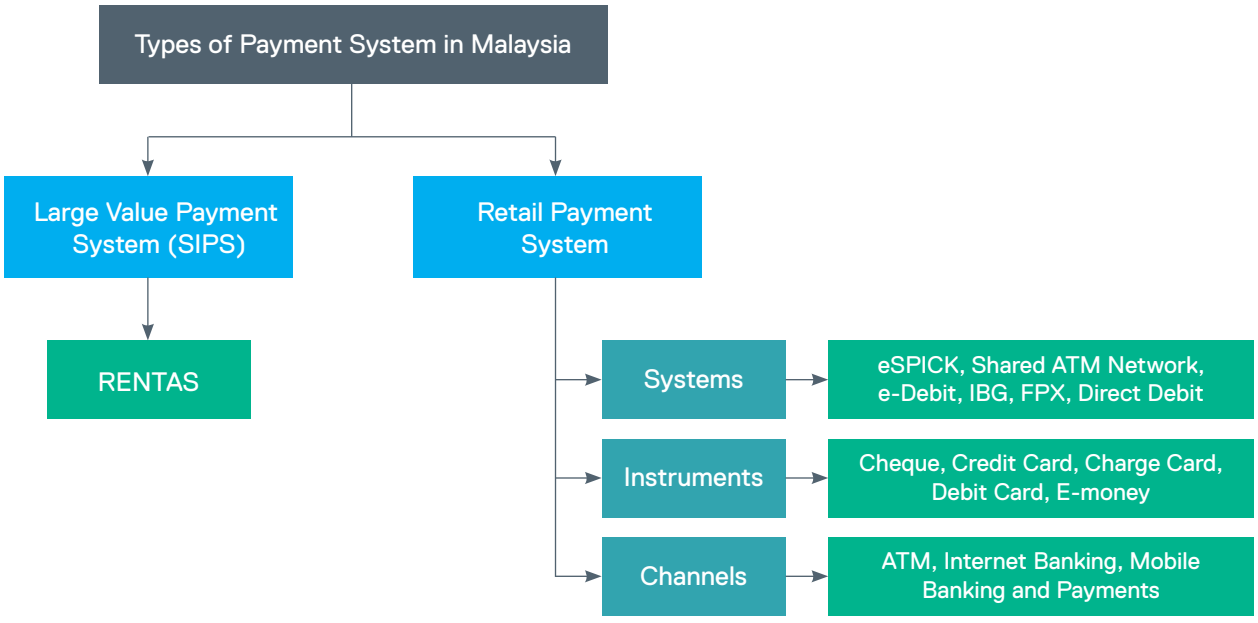
Malaysia

3. What are the main sources of laws regulating payments services in Malaysia?

- Central Bank of Malaysia Act 2009
- Financial Services Act ("FSA" 2013;
- Islamic Financial Services Act ("IFSA") 2013;
- Labuan Financial Services and Securities Act 2010;
- Development Financial Institutions Act ("DFIA") 2002;
- Money Services Business Act ("MSBA") 2011.
- Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001;
- Electronic Commerce Act 2006;
- Consumer Protection Act 1999;
- Consumer Protection (Electronic Trade Transactions) Regulations 2012; and
- Guidelines issued by the BNM.

4. Describe the regulatory framework(s) for payment services operating in Malaysia, and the type of payment services that are regulated.

Malaysia's Payment System



Malaysia

A. Systemically Important Payment System (SIPS)

A systemically important payment system or large value payment system (LVPS) typically processes high-value and time-critical payments. It is an essential payment system to ensure the smooth functioning of the economy, financial system and financial markets, and its failure could trigger disruptions or transmit shocks within the economy and the financial market, both at the domestic and potentially at the cross-border level. RENTAS is the only LVPS for Malaysia and it is operated under Real Time Gross Settlement (RTGS) basis.

B. Real Time Electronics Transfer of Funds and Securities (RENTAS)

RENTAS was implemented in July 1999 with the objective to improve the overall efficiency of the large value payment system, particularly in respect of reducing interbank settlement risk. It enables the transfer and settlement of high value interbank funds and scripless securities transactions. There are two types of transactions handled by RENTAS namely Interbank Funds Transfer System (IFTS) and Scripless Securities Transfer System (SSTS). The following transactions can be performed by RENTAS members via the system:

- Interbank funds transfer;
- Cash withdrawals from Bank Negara Malaysia;
- Statutory reserve adjustment;
- Money market settlement;
- Ringgit leg of foreign exchange; and
- Scripless securities transfer.

C. Retail Payment System

In general, the retail payments in Malaysia can be divided into three:

- Retail Payment Systems
  i. Bank Negara Malaysia had in 2008 implemented the **National Electronic Cheque Information Clearing System (eSPICK)** to replace the previous Sistem Penjelasan Imej Cek Kebangsaan (SPICK) cheque clearing system. eSPICK was fully rolled out nationwide in July 2009. Under the eSPICK, customers will receive funds from the cheques deposited during business hours on the next business day, compared to between 2 to 8 business days previously;
  ii. **Shared ATM Network (SAN)** enables bank customers to access their funds from any of the participating banks' automated teller machine (ATMs);
  iii. House;
  iv. Interbank Giro;
  v. Direct Debit;
  vi. Financial Process Exchange.

- Retail Payment Systems
  i. Cheque, credit Cards, Charge Cards, Debit Cards and E-money.

- Retail Payment Channels.
  i. Internet Banking;
  ii. Mobile Banking;
  iii. Mobile Payment.

Regulatory framework for the payment system are described in *Question 6* and 7 below.

Malaysia

5. How does Malaysia's payments licensing laws apply to cross-border business into your jurisdiction?

A. The payments licensing laws promulgated by BNM has not hindered cross-border business activities. Indeed, Malaysia has had the international credit card system for many decades but primarily run under the auspices and monopoly of the licensed banks in Malaysia and only available to a small part of the wealthier population who could afford the high transaction costs.

B. As pointed out in Paragraph 8, BNM's Guideline on Electronic Money (E-Money) to all e-money issuers in relation to the operation of their E-Money schemes issued pursuant to the Payment Systems Act 2003 had provided the adequate licensing foundation for payment and ecommerce business to flourish.

C. Further in 2013 BNM issued guidelines for the easing of licensing submission requirements pursuant to Financial Services Act 2013 (FSA).

D. Growth and advancement of the internet and mobile devices technology has heralded a tremendous acceleration in ecommerce globally where on line connection payments can be made instantaneously, securely to anyone in any part of the world with reduced costs.

E. Advancement of internet and mobile technology continues to reduce much friction and costs and has removed the boundary between domestic and international business transaction.

F. In terms of regulatory compliance there were was no major amendments to the regulations relating to operational aspects of the payment systems business and that of issuing payment instruments following the modernizing Financial services Act 2013.

G. Further developments in the cross border payments systems are expected as follows:-

- In April 2019 Eight ASEAN countries agreed on ASEAN Payment Connectivity, which aims to cut transaction fees for migrants, tourists and businesses, during the meeting of ASEAN Finance Ministers and Central Bank Governors;
- ASEAN has laid out important policy measures and frameworks, including the AEC Blueprint 2025, Masterplan on ASEAN Connectivity 2025, and the e-ASEAN Framework Agreement, to address roadblocks;
- Extensive collaboration among banks, non-banks and card companies to develop cross-border payment services using modern technologies, ranging from interoperable QR Code, Blockchain technology, Application Programming Interface [API], and card networks. These new services can serve the needs of different customer segments; improve efficiency of the regional financial system; facilitate business transactions and international trade; reduce the cost of service providers and customers; and enhance financial inclusion for a broad range of ASEAN population.

Malaysia 

6. What are the main requirements to be licensed for payments in Malaysia?

In addition to the local banks being licensed via conventional requirements, issuers of e-money are required to obtain approval from BNM pursuant to Section 25 and 70 of the Payment Systems Act 2003 and comply with BNM Guideline on E-Money issued in 2003.

BNM Guideline on Electronic Money (E-Money)

A. This Guideline stipulates the operational requirements for all e-money issuers and specific requirements for large e-money issuers;

B. An issuer of e-money shall be a company incorporated under the Companies Act 1965;

C. This Guideline is applicable to all e-money issuers in Malaysia, including licensed institutions;

D. E-money issuers are required to adopt the principles and the minimum standards in this Guideline, taking into consideration the nature, size and complexity of their e-money schemes;

E. The main regulatory objective in overseeing e-money operations is to promote the safety and soundness of e-money schemes, and therefore enhance users' confidence in the usage of e-money. The E-Money Guidelines sets out principles to be adhered;

F. The following terms were defined as follows:

- E-money is defined in the Payment Systems (Designated Payment Instruments) Order 2003 as a payment instrument, whether tangible or intangible that: i. stores funds electronically in exchange of funds paid to the issuer; and ii. is able to be used as a means of making payment to any person other than the issuer;
- Issuer of e-money refers to any person that is responsible for the payment obligation and assumes the liabilities for the e-money being issued;
- User refers to any person to whom the e-money has been issued or any person who uses the e-money to make payments for purchases of goods and services;
- Merchant refers to any person that accepts the e-money as payment for their goods and services;
- Reload agent refers to any person that accepts payment on behalf of the issuer for the purpose of adding monetary value to the e-money;
- Purse limit means the maximum monetary value that can be stored in an e-money instrument;
- Licensed institution refers to any person licensed under the Banking and Financial Institutions Act 1989 (BAFIA), Islamic Banking Act 1983 (IBA) and Development Financial Institutions Act 2002 (DFIA);
- Outstanding e-money liabilities refer to the unutilised amount of e-money which has been issued and the utilised amount of e-money which is pending payment to merchants;
- Large e-money scheme refers to e-money scheme with: i. Purse limit exceeding RM200 The maximum purse limit for large scheme is capped at RM1,500 or any amount as approved by the Bank; or ii. Outstanding e-money liabilities 1 for 6 consecutive months amounting to RM1 million or more;
- Small e-money scheme refers to e-money scheme with: i. Purse limit not exceeding RM200; and ii. Outstanding e-money liabilities of less than RM1 million.

G. Operational requirements:-

- Establish Adequate Governance And Operational Arrangements;
- Ensure Proper Risk Management Is In Place;
- Ensure That The Risks Of Using E-Money, And Rights And Responsibilities Of All Stakeholders Are Clearly Defined And Disclosed;
- Ensure Prudent Management Of Funds;
- Ensure Timely Refund Of Stored Value In The E-Money;
- Implement Adequate Measures To Prevent The Use Of E-Money For Money Laundering, And Ensure Compliance With Other Requirements;
- Sets out criteria of an individual to be "fit and proper to hold position of director or senior management and stipulates the responsibilities of the board.
- Conditions and safeguards for outsourcing of e-money operations.

7. What is the process to become licensed for payments in Malaysia?

BNM Submission Requirements

With the enactment of the Financial Services Act 2013 (FSA) and the Islamic Financial Services Act 2013 (IFSA), which came into force on 30 June 2013, any person who intends to operate a payment system or issue a designated payment instrument is required to obtain prior approval of BNM pursuant to section 11 of the FSA or section 11 of the IFSA and comply with BNM guidelines for the following:-

- For Approval to Operate a Payment System; or
- To Issue a Designated Payment Instrument; or
- To be Registered to Provide Merchant Acquiring Services.

A. Any person who intends to operate a payment system or issue a designated payment instrument is required to obtain prior approval of BNM, as the case may be, while any person who intends to provide merchant acquiring services is required to register with BNM;

B. Merchant Acquiring Services Pursuant to section 17 of the FSA states that a person who intends to provide merchant acquiring services shall fulfil the requirements and submit documents or information as may be prescribed by BNM;

C. The payment system:

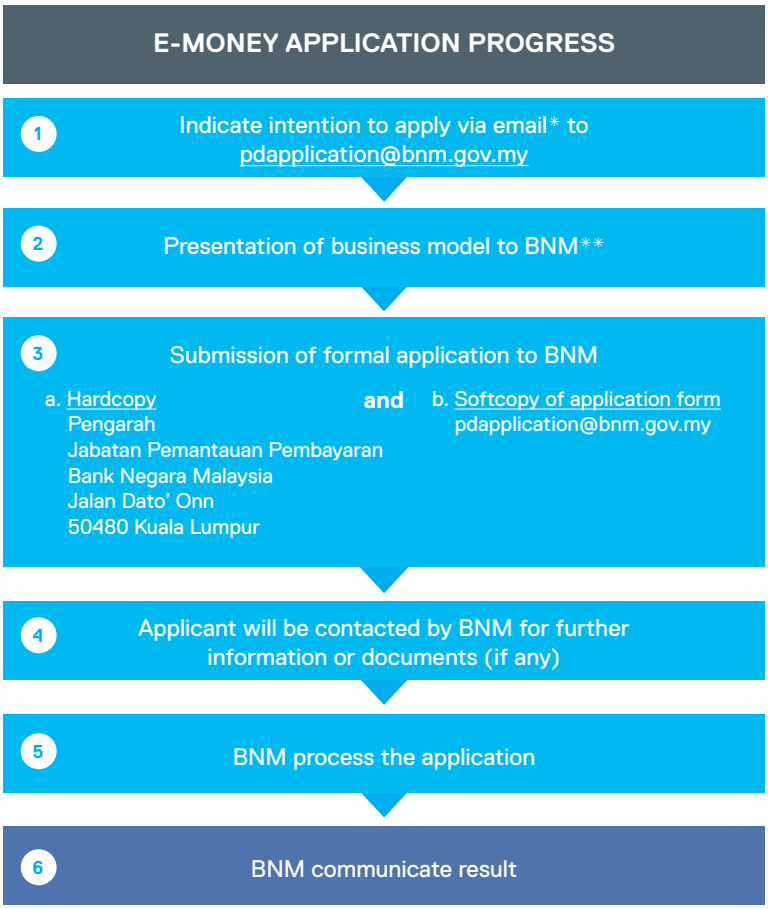
- Enables the transfer of funds from one banking account to another, which includes any debit transfer, credit transfer or standing instructions, but does not include the operation of a remittance system approved under section 40 of the Money Services Business Act 2011; and

- Provides payment instrument network operation which enables payments to be made through the use of a payment instrument.

Malaysia

D. The following payment instruments have been prescribed as designated payment instruments or designated Islamic payment instruments which are:

- Charge card;
- Credit Card;
- Debit Card;
- Electronic money;
- Any combination of 1-4 above.



Note:

Please include the following in the email:

i. Clarification whether you have conducted an assesment that your business model fulfils the definition of e-money; and

ii. A summary or brief explanation of your business model

** Only if your business fits the denifition of e-money

Malaysia

8. What payment services "passporting" arrangements does Malaysia have with other countries, if any?

A. Passporting allows a firm registered for example in the ASEAN Region to do business in any other ASEAN state without the need for further authorization from each country. Companies based outside of ASEAN will get authorized in one ASEAN state. The company will then use the passporting rights it receives from that country to either open an establishment elsewhere in an ASEAN state or provide cross-border services.

B. Whilst it is the one of the objectives of the ASEAN Economic Community Blueprint, there is no specific passport arrangements currently in Malaysia.

C. However as highlighted in the item 5 above in the space of payments, existing licensing laws and regulation in Malaysia do not overtly restrict e commerce and cross-border business which allows many domestic and international players to collaborate and do business in each state whether in ASEAN or globally.

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Malaysia.

A. **Anti-Money Laundering and Anti-Terrorism Financing Act 2001**, otherwise known as AMLA is the primary legislation dealing with anti-money laundering and anti-terrorism financing.

Section 4 of AMLA states as follows 4. (1) Any person who (a) engages, directly or indirectly, in a transaction that involves proceeds of an unlawful activity or instrumentalities of an offence; (b) acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes of or uses proceeds of an unlawful activity or instrumentalities of an offence; (c) removes from or brings into Malaysia, proceeds of an unlawful activity or instrumentalities of an offence; or (d) conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of an unlawful activity or instrumentalities of an offence, commits a money laundering offence.

B. **The Financial Intelligence Unit** ("FIU") in the enforcement department of BNM manages and gives analysis of the financial intelligence received relating to money laundering and terrorism financing. All reporting institutions which are defined in AMLA are subject to the review by the FIU reporting institutions include: commercial banks, merchant banks, finance companies, Islamic banks, money changers etc. They also must file suspicious transaction reports under the AMLA.

C. The AMLA provides wide-ranging investigation powers including powers for law enforcement agencies and Public Prosecutor to freeze and seize properties that are involved or suspected to be involved in money laundering or terrorism financing offences, and the power of the court to forfeit properties derived from the proceeds of serious crimes.

The AMLA is enforced by various agencies depending on the nature of the crime under their respective purviews. Bank Negara Malaysia is only empowered to investigate money laundering cases relating to laws administered by Bank Negara Malaysia:

- Financial Services Act 2013
- Islamic Financial Services Act 2013
- Money Services Business Act 2011
- Development Financial Institutions Act 2002 (Act 618)

D. Guidelines issued by BNM

- The AML/CFT and TFS for FIs (**Policy Document for Financial Institutions**) is a revision of the existing AML/CFT policy documents. This policy document sets out the responsibilities and obligations of reporting institutions imposed under the AMLA. This policy document applies to financial institutions such as banks, insurers, money services businesses and issuers of designated payments instruments. Reporting institutions are expected to fulfil the requirement of implementing risk-based approach in managing ML/TF risks and to comply with the targeted financial sanctions requirements.
- **Policy Document for Non Financial Businesses**, Institutions and Professions applicable to businesses and professionals.
- The Anti-Money Laundering and Courter Financing of Terrorism (AML/CFT) - Digital Currencies (Sector 6) (Policy Document for Digital Currencies

E. The Labuan Financial Services Authority and the Securities Commission have issued their own guidelines on prevention of money laundering and terrorism financing for capital market intermediaries under its purview.

F. The Financial Action Task Force (FATF)is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard. A FAFT report in October 18 analysed Malaysia's progress in addressing the technical compliance deficiencies identified in the FATF assessment of their measures to combat money laundering and terrorist financing and concluded that it was largely compliant.

10. Describe the technology risk requirements that apply to payment services in Malaysia.

A. Bank Negara Malaysia in looking to address identified gaps in technology risk management practices within the financial sector and having conducted a comprehensive review of existing technology risk guidelines have issued the **Risk Management in Technology (RMIT)** guideline which came into effect on 1 January 2020.

This policy document sets out the Bank's requirements with regard to financial institutions' management of technology risk. In complying with these requirements, a financial institution shall have regard to the size and complexity of its operations. Accordingly, larger and more complex financial institutions are expected to demonstrate risk management practices and controls that are commensurate with the increased technology risk exposure of the institution. In addition, all financial institutions shall observe minimum prescribed standards in this document to prevent the exploitation of weak links in interconnected networks and systems that may cause detriment to other financial institutions and the wider financial system. The control measures set out in Appendices 1 to 5 serve as a guide for sound practices in defined areas. Financial institutions should be prepared to explain alternative risk management practices that depart from the control measures outlined in the Appendices and demonstrate their effectiveness in addressing the financial institution's technology risk exposure.

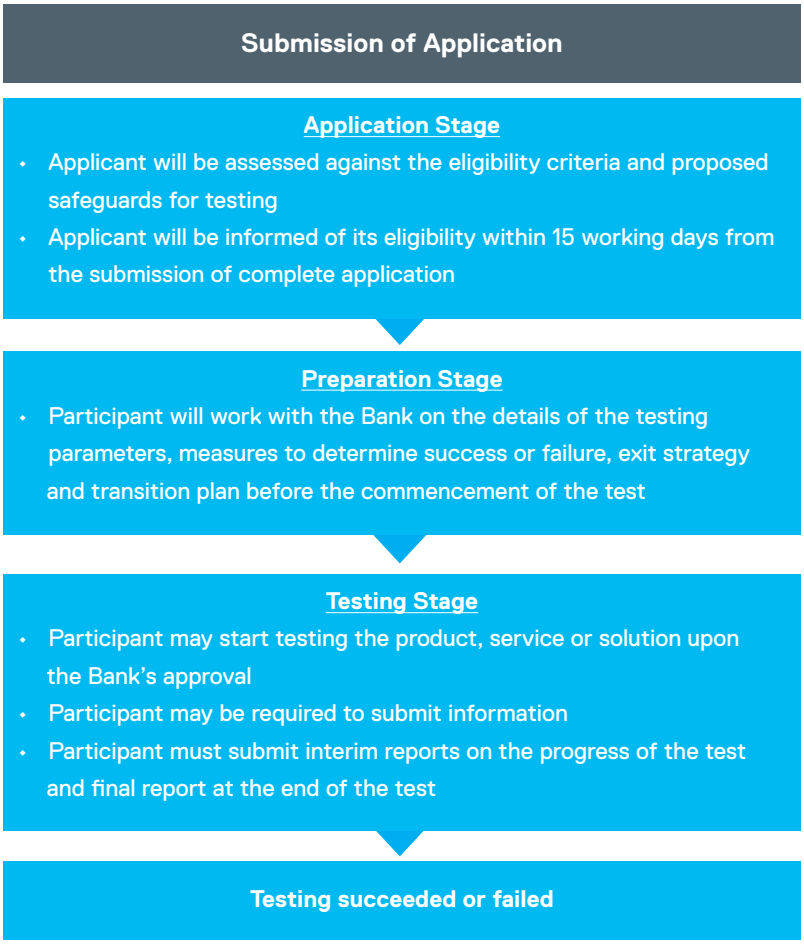
Malaysia

B. The Financial Technology Regulatory Sandbox Framework (Framework) is introduced in 18 October 2016 to enable innovation of fintech to be deployed and tested in a live environment, within specified parameters and timeframes. Risk and failure are an integral part of innovation. Given that a regulatory sandbox (sandbox) operates in a live environment, failure may result in financial loss or other risks to the sandbox participants and their customers. It is therefore imperative for the sandbox to incorporate appropriate safeguards to manage the risks and contain the consequences of failure.

C. See Application process for Sandbox below.

Application Process

- The flowchart below illustrates the application process upon submitting the application for sandbox.



- For a rejected application, a cooling off period of six (6) months shall be observed before the applicant is allowed to resubmit the application.

Malaysia

11. Describe the data privacy requirements that apply to payment services in Malaysia.

A. **Personal Data Protection Act 2010 (PDPA)**

Personal Data Protection Department (PDPD) is an agency under the Ministry of Communications and Multimedia Commission (MCMC) oversees the processing of personal data of individuals involved in commercial transactions by user data that is not misused and misapplied by the parties concerned.

The PDPA purports to safeguard personal data by requiring the data user to comply with certain obligations and conferring certain rights to the data subject in relation to his personal data. The Personal Data Protection Commissioner is responsible for implementing and enforcing the PDPA.

Subsidiary legislation that has been passed to date include:

- The Personal Data Protection Regulations 2013;
- The Personal Data Protection (Class of Data Users) Order;
- The Personal Data Protection (Registration of Data User) Regulations 2013;
- The Personal Data Protection (Compounding of Offences) Regulations 2016; and
- The Personal Data Protection (Class of Data Users) (Amendment) Order 2016.

B. **The Personal Protection Code of Practice for Banking and Financial** sector was approved and registered by the Commissioner on 19 Jan 2017, which regulates the personal data processing activities carried out by members of the banking and financial sector.

Banking secrecy provisions are provided in the Financial Services Act 2013 (Islamic Financial Services Act 2013). Bank Negara Malaysia has issued a number of guidelines and policy documents which address the obligation of financial institutions in respect of management of customer information.

C. **The Personal Protection Code of Practice for the Communication Sector** was approved and registered by the Commissioner on 23 November 2017 which regulates the personal data processing activities carried out by members of the communication sector.

The Communication and Multimedia Consumer Forum of Malaysia ("**Consumer Forum**") has issued the General Consumer Code of Practice for the Communications and Multimedia Industry Malaysia ("**Consumer Code**"). The Consumer Code applies to all licensed service providers and members of the Consumer Forum requires code subject to maintain the privacy of identifiable information of a subscriber of telecommunications services.

D. The Personal Data Protection Commissioner has issued the Personal Data Protection Standard 2015 ('**the 2015 Standards**') which came into force on 23 December 2015. The 2015 Standards include; security standards, retention standards, and data integrity standards, which have application to personal data that are processed electronically and non-electronically. The 2015 Standards are stated to be 'a minimum requirement' and will apply to all data users, meaning any person who processes, has control of or allows the processing of, any personal data in connection with a commercial transaction.

E. PDPA does not provide any provisions on notification of breach of personal data. The implementation of Data Breach Notification ("DBN") is aimed at plugging such gap in the PDPA and at assisting data users in personal data breach management. The DBN is supposed to provide a mechanism where data users will need to provide notification to the relevant authorities and the affected parties when a breach of personal data occurs. However, the DBN Public Consultation Paper has yet to come into force as yet.

Malaysia

12. Describe how innovations and inventions are protected by law in Malaysia.

A. **TradeMarks Act2019 and TradeMarks Regulations 2019 and the common law of passing off**

A trade mark is an important asset for all businesses. It consists of a device, brand, heading, label, ticket, name, signature, word, letter, numeral or any combination thereof. It provides their owners with the legal right to prevent others from using an identical or confusingly similar mark.

B. **Copyright Act 1987**

Copyright protects various type of works such as literacy works which covers novel, lyrics, articles, computer program and so on; dramatic works such as dance choreography; artistic works such as paintings, photographs or any logos, drawings; musical works; recordings; broadcasts and finally, layouts. Regulations pertaining to the voluntary notification of copyright came into force in Malaysia on June 1, 2012. There was no formal copyright registration process prior to the Regulations. Being a party to the Berne Convention, copyrighted works are protected immediately upon creation and fulfilment of certain conditions in the Copyright Act (original or derivative work). Copyright provides protection for a term equivalent to the lifetime of the author plus 50 years.

C. **Industrial Designs Act 1996 and Industrial Designs Regulations 1999**

Industrial designs right is an intangible right to the features of shape, configuration, pattern or ornament applied to an article by any industrial process or means, being features which in the finished article appeal to and are judged by the eye. A registered industrial design is given an initial protection period of 5 years from the date of filing and is renewable for a further two consecutive terms of 5 years each.

D. **Patents Act 1983 with subsequent amendments up to Patents (Amendment) Act 2006, Patents Regulations 1986 and Patents (Amendment) Regulations 1993)**

Patents are grants given to owners by the government which give the owner an exclusive right over the invention that they have created. Invention can cover product or processes. The protection also gives the owner the exclusive right to stop others from manufacturing, using and/or selling the owner's invention in Malaysia without the owner's consent or permission. A patent is protected twenty (20) years from the date of filing and a utility innovation is protected with an initial period of ten (10) years and is renewable for a two consecutive terms of five (5) years each.

Malaysia

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

Under The Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 (effective 15 January 2019) outlawed trading in cryptocurrencies by defining them as securities which hitherto operated and traded unregulated. The 2nd Revision of the Guidelines on Recognised Markets issued on 25 January 2019 by the Securities Commission of Malaysia (SC) paved the way for trading of crypto currencies to be conducted via a SC licensed Digital Asset Exchange. The Guidelines provided the framework and the requirements for Digital Asset Exchanges to be set up. Today Malaysia, has 3 Digital Asset Exchanges namely Luno, Sinegy and Tokenize which are authorised to conduct trading of cryptocurrencies albeit currently limited to 3 crypto currencies namely Bitcoin, Ethereum and XRP.

On 15 Jan 2020, the SC issued its 1st Guidelines on Digital Asset which defined Digital Assets, Digital Currency and Digital Token (Digital Assets Guidelines). The Digital Assets Guidelines introduced the framework to regulate fundraising activities via initial coin offerings ("ICO") by providing the requirements for Digital Token Offering and registration of a platform operator to operate an Initial Exchange Offering (IEO) platform. Hence any ICO can only be carried via a SC licensed IEO platform operator. Applications for registration of an IEO platform is expected in the 2nd half of 2020.

On 16 April 2020, the SC issued updated Guidelines on Recognised Markets (4th Revision) covering Market Operators, Equity Crowdfunding Platform, Peer-to Peer funding platform, Property Crowdfunding Platform and Digital Asset Exchange.

Trading in crypto currencies and digital assets has been permissible in Labuan since 2018 which is a Federal Territory of Malaysia. The Labuan Financial Services Authority Act 1996 (Labuan FSA) and the Labuan International Business and Financial Centre (Labuan IBFC) under the Labuan Financial Services and Securities Act 2010 govern regulation, supervision, and development of Labuan financial services.

Philippines

1. What is the payments landscape in Philippines:
The types of activities, state of development of the market and new trends eg FinTech if any?

With the efficiency and growing stability of e-commerce, the transition to electronic payment is steadily rising in the Philippines. According to the Department of Trade and Industry, as much as one hundred thirty-six (136) fintech companies are operating in the Philippines, with 29% engaged in alternative finances, 22% in payments and 19% in blockchain.[18] Others are involved in remittances, investment and crowdfunding activities.[19] The *Bangko Sentral ng Pilipinas* ("BSP") has been strongly pushing for the adoption of new means to facilitate reliable and competitive payment systems in the Philippines to reduce the cost of exchanging goods and services.

In recent years, aside from closely monitoring the shift to online platforms of various retailers, the Philippine government has started to encourage electronic payment systems through the adoption of PhilPaSS or the real time gross settlement (RTGS) system owned and operated by the BSP; and the National Retail Payment System, which introduced the automated clearing houses PESONet and InstaPay.

BSP Circular No. 980, Series of 2017 or the *Adoption of National Retail Payment System ("NPRS") Framework* was released by the BSP on 06 November 2017. The NRPS is a policy and regulatory framework that aims to provide direction in carrying out retail payment activities through BSP supervised financial institutions (BSFIs) by defining high-level policies, principles, and standards, which when adopted, would lead to the establishment of a safe, efficient and reliable retail payment system.

As a recognition of Congress of the growing shift to electronic payment systems, Republic Act No. 11127, otherwise known as the National Payment Systems Act ("NPSA") was passed and signed into law on 30 October 2018. During the past year, to implement the provisions of the NPSA, the BSP has also issued BSP Circular No. 1049, series of 2019 providing for the *Rules and Regulations on the Registration of Operators of Payment Systems* ("OPS")[20] and Memorandum No. M-2019-023 dated 25 September 2019 for the *Guidelines on the Registration and Notification Requirements of OPS*.

2. Which official agency regulates payments in Philippines?

The NSPA designates the BSP as the authority which shall oversee the payment systems in the Philippines and exercise supervisory and regulatory powers for the purpose of ensuring the stability and effectiveness of the monetary and financial system.[21] The NPSA requires registration of payment system operators with the BSP.[22] The BSP is further empowered to issue, through the Monetary Board, rules and regulations governing the standards of operation of payment systems, conduct of examination of the participants, adequacy of resources of operators, qualifications and disqualifications of individual directors or officers of the operators, and other appropriate measures to ensure stability and confidentiality of payment systems in the Philippines.[23]

[18] See https://www.philstar.com/business/business-as-usual/2020/02/24/1995467/philippine-fintech-industry-flourishing-says-dti (last accessed 22 June 2020).
[19] *Id.*
[20] Issued on 09 September 2019.
[21] Section 5, Republic Act No. 11127, otherwise known as the "National Payment Systems Act" dated 30 October 2018 ("NPSA").
[22] Section 10, NPSA.
[23] Section 6(d), NPSA.

Philippines

3. What are the main sources of laws regulating payments services in Philippines?

The main legislation regulating payments services in the Philippines is the NSPA. Pursuant to its regulatory authority, the BSP has implemented regulations to facilitate registration of operators of payment systems, as mandated under the NPSA, for securing prior authority from the BSP. In line with this, the BSP has issued Circular No. 1049, series of 2019 and Memorandum No. M-2019-023, which provide for the process and requirements for registration of OPS with the BSP.

4. Describe the regulatory framework(s) for payment services operating in Philippines, and the type of payment services that are regulated.

The BSP is empowered under the NSPA to designate payment systems, require OPS to secure prior authority from the BSP, and issue rules and regulations governing the standard operation of payment systems, among others.[24]

Pursuant to the rule making powers of the BPS, the following activities are considered operations of a payment system, and entities performing such activities are required to register as an OPS:

- Maintains the platform that enables payments or fund transfers, regardless of whether the source and destination accounts are maintained with the same or different institutions;
- Operates the system or network that enables payments or fund transfers to be made through the use of a payment instrument; and
- Provides a system that processes payments on behalf of any person or the government.

If an OPS is also a BSP supervised financial institution engaged in payments and settlements, it shall additionally comply with the provisions of the NPRS. The NPRS Framework requires BSP supervised financial institutions to ensure retail payment systems demonstrate sound risk management and effective and efficient interoperability.

5. How does Philippines's payments licensing laws apply to cross-border business into your jurisdiction?

The scope of the NSPA and the authority of the BSP covers only payment systems in the Philippines.[25] Hence, the NSPA licensing requirements cover only local or foreign entities doing business in the Philippines. However, the BSP is mandated to coordinate with other regulators and other concerned government agencies to avoid gaps, inefficiencies, duplications and inconsistencies in their respective regulation of other systems which are related to or interconnected with payment systems.[26] The BSP is also mandated to coordinate with the overseers of payment systems of other countries to facilitate safe, efficient and reliable cross-border payment transactions.[27]

[24] Section 6, NPSA.
[25] Section 5, NSPA.
[26] Section 9, NSPA.
[27] *Id.*

Philippines

6. What are the main requirements to be licensed for payments in Philippines?

As provided under BSP Circular No. 1049, the following are the main requirements to be licensed as an OPS:

- Duly accomplished Application for Registration;
- Business Plan;
- Copy of the business registration/permit; and
- Registration fee.[28]

If the applicant is a Bank or Electronic Money Issuer("EMI")that is currently operating, or will later operate as an OPS, the only requirement is a notification to the BSP of its activities as an OPS.[29] The notification shall include a description of its existing business as an OPS, business model, and target markets.[30]

7. What is the process to become licensed for payments in Philippines?

The company shall first conduct a self-assessment to determine whether it is considered as an OPS and shall register itself through BSP's online site. Upon registration through the BSP's online site,[31] the BSP issues a Provisional Certificate of Registration ("PCOR").[32] The validity of the provisional license shall be indicated in the PCOR.[33] Thereafter, the BSP shall conduct an evaluation to determine if the company is indeed an OPS as defined under the NPSA.[34] The BSP shall inform the company for additional documentary requirements it must submit and, once complete, shall issue a Certificate of Registration ("COR").[35] The BSP shall inform the OPS once the COR is ready to be issued. In certain instances, such as where a longer period for evaluation is necessary or when circumstances warrant extension as determined on a case-to-case basis, the validity period of the PCOR may be extended.

8. What payment services "passporting" arrangements does Philippines have with other countries, if any?

The Philippines does not have any specific "passporting" or a multi-jurisdictional payment system arrangement with other countries like the passporting arrangements in the European Union.

[28] BSP Circular No. 1049
[29] *Id.*
[30] *Id.*
[31] BSP Memorandum No. M-2019-023.
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*

Philippines

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Philippines.

Under the Anti-Money Laundering Act of 2001, as amended ("AMLA"), its 2016 Revised Implementing Rules and Regulations ("Revised IRR"), which took effect on 07 January 2017 and the 2018 Implementing Rules and Regulations ("2018 IRR"), which took effect on 22 November 2018, covered persons, which are persons supervised or regulated by the BSP, such as banks; non-banks; quasi-banks; trust entities; pawnshops; non-stock savings and loans associations; electronic money issuers; and all other persons and their subsidiaries and affiliates supervised or regulated by the BSP[36], must register with the Anti-Money Laundering Council ("AMLC") through an electronic reporting system in order to transmit and report covered transactions and suspicious transactions.[37]

The AMLA and its Revised IRR list the following as covered transactions that covered persons are obligated to report within five (5) working days to the AMLC, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from the occurrence thereof:[38]

- Transactions in cash or other equivalent monetary instrument exceeding Five Hundred Thousand Pesos (PhP 500,000.00); and
- Transactions exceeding One Million Pesos (PhP 1,000,000.00) in the case of jewelry dealers, dealers in precious metals and dealers in precious stones.[39]

The AMLA and the Revised IRR also require the reporting of suspicious transactions within the same period as that for covered transactions. A suspicious transaction is one where, regardless of the amount involved, any of the following circumstances exists:

- There is no underlying trade or legal or trade obligation, purpose or economic justification;
- The client is not properly identified;
- The amount involved is not commensurate with the business or financial capacity of the client;
- Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA;
- Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the covered person;
- The transaction is in any way related to an unlawful activity or any money laundering activity or offense that is about to be committed, is being or has been committed; or
- Any transaction that is similar, analogous or identical to any of the foregoing.[40]

[36] Section 1(a)(1)(f), 2018 IRR.
[37] Rule 35, Section 1(b), 2018 IRR of Republic Act No. 9160.
[38] Revised IRR, Rule 3.C.
[39] Revised IRR, Rule 3.G.
[40] Revised IRR, Rule 3.H.

Philippines

10. Describe the technology risk requirements that apply to payment services in Philippines.

Under the NSPA, the BSP is empowered to issue rules and standards to ensure that the designated payment systems have a high degree of security and operational reliability and have contingency requirements for timely completion of daily processing commitments. As of date, there are no rules issued yet by the BSP on this matter.

Technology risk requirements in the Philippines area also include privacy laws and regulations. Under Republic Act No. 10173 or the Data Privacy Act of 2012 ("DPA") and its implementing rules and regulations ("DPA IRR"), personal information pertaining to a person's age and marital status, as well as those issued by government agencies peculiar to an individual (i.e. Tax Identification Number, Passport Number, Driver's License information), often processed by payment services platforms, are considered sensitive personal information[41] accorded higher protection by the DPA relative to mere personal information. Necessarily, personal information controllers such as a payment services platform must implementing reasonable and appropriate organizational, physical and technical security measures to protect its data.[42] In the event of a personal data breach or data security incidents, the payment services platform must inform the personal information controller of the same in a timely manner, such that the personal information controller may notify the NPC of such breach within 72 hours of the payment services platform's knowledge of or reasonable belief that a personal data breach requiring notification has occurred.[43]

11. Describe the data privacy requirements that apply to payment services in Philippines.

As the operation of payment services involves processing that is not occasional, poses a risk to the rights and freedoms of data subject or may involve the sensitive personal information of at least 1000 individuals, under the DPA, a payment services platform is required to register its personal data processing systems with the National Privacy Commission ("NPC").[44] This is in addition to the requirement to designate and register with the NPC a data protection officer, compliance officer or other officer accountable for ensuring compliance with pertinent regulations on data privacy and security.[45]

As suppliers/online stores effectively outsource to these payment services platform the processing of customers' personal data for said suppliers'/online stores' purposes (i.e. payment for its good and services), they must enter into a data processing outsourcing agreement with the payment services platform, which shall stipulate that the payment services platform shall process the personal data only upon the documented instructions of the supplier/online store.[46]

If the operator of the payment system will be processing personal data for its own commercial purposes and not pursuant to the purposes and instructions of the supplier/online store (i.e. marketing), it must enter into a data sharing agreement with the personal information controller. Further, the consent of the data subject must be acquired. The data subject must be provided with the following information prior to collection or before data is shared: (a) Identity of the personal information controllers or personal information processors that will be given access to the personal data; (b) Purpose of data sharing; (c) Categories of personal data concerned; (d) Intended recipients or categories of recipients of the personal data; (e) Existence of the rights of data subjects, including the right to access and correction, and the right to object; (f) Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

[41] Section 3(t), DPA IRR.
[42] Section 25, DPA IRR.
[43] Section 38, DPA IRR.
[44] Section 47, DPA IRR.
[45] Section 26, DPA IRR.
[46] Section 44, DPA IRR.

Philippines

12. Describe how innovations and inventions are protected by law in Philippines.

Under Republic Act No. 8923 or the Intellectual Property Code of the Philippines, any technical solution of a problem in any field of human activity which is new, involves an inventive step and is industrially applicable shall be considered a patentable invention.[47] As such, the inventor has patent rights.[48] The term of a patent is 20 years from the filing date of the application.[49] A patent confers on its owner the following exclusive rights[50]:

- Where the subject matter of a patent is a product, to restrain, prohibit and prevent any unauthorized person or entity from making, using, offering for sale, selling or importing that product;
- Where the subject matter of a patent is a process, to restrain, prevent or prohibit any unauthorized person or entity from using the process, and from manufacturing, dealing in, using, selling or offering for sale, or importing any product obtained directly or indirectly from such process.

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

Cryptocurrencies or virtual currencies and virtual currency exchanges are primarily regulated by the Bangko Sentral ng Pilipinas ("BSP") under BSP Circular No. 944. BSP Circular No. 944 does not, however, cover the issuance of virtual currency. There are currently no existing rules regulating the issuance of virtual currencies in the Philippines.

Under the existing regime, any person or entity may be able to convert fiat currency into virtual currency and vice versa through a BSP-licensed virtual currency exchange. Virtual currency refers to any type of digital unit that is used as a medium of exchange or a form of digitally stored value created by agreement within the community of virtual currency users. A virtual currency exchange refers to any entity that offers services or engages in activities that provide facility for the conversion or exchange of fiat currency to virtual currency or *vice versa*.

In parallel with the BSP's virtual currency exchange license, the Cagayan Economic Zone Authority ("CEZA") introduced its Financial Technology Solutions and Offshore Virtual Currency ("FTSOVC") License in 2019. The legislation regulating the issuance of a FTSOVC License is Financial Technology Solutions and Offshore Virtual Currency Business Rules and Regulations of 2018 of the Cagayan Economic Zone Authority (CEZA).

The FTSOVC License allows a company based in the Cagayan economic zone to engage in crypto-trading activities outside the Philippines. A FTSOVC-licensee is only allowed to provide its services to non-Philippine residents.

[47] Section 21, IP Code.
[48] Section 28, IP Code.
[49] Section 54, IP Code.
[50] Section 71, IP Code.

Singapore

1. What is the payments landscape in Singapore:
The types of activities, state of development of the market and new trends eg FinTech if any?

For several decades, payment services and payment systems in the traditional sense were regulated by the Monetary Authority of Singapore. In the last five years however, FinTech innovation has driven financial inclusion and digital payment services. It has been reported that, as at 2019, almost half of the fintech businesses in Southeast Asia has chosen Singapore as their base. There are nearly 500 registered members of the Singapore FinTech Association—a majority of them in the payments space, with others in lending, wealth management, blockchain, data management and crowdfunding.

Fintech solutions geared towards payments, both domestic and cross-border, continue to rise. This was sparked by the much anticipated Payment Services Act, which came into effect on 28 January 2020.

The government-helmed Project Ubin explores the use of distributed ledger technology (DLT) for clearing and settlement of payments and securities. Its successful experiment on cross-border and cross-currency payments using central bank digital currencies was announced in May 2019, and will pave the way for eventual widespread and government-led adoption of technology-enabled payments.

2. Which official agency regulates payments in Singapore?

The regulatory body overseeing the Payment Services Act 2019 is the Monetary Authority of Singapore ("MAS"), which has multiple roles as central bank, financial services regulator and industry promoter.

3. What are the main sources of laws regulating payments services in Singapore?

In Singapore most, if not all, of the financial products and services provided by banks / organisations that involve public interest are regulated.

There are different legislation enacted for the different types of services / products offered. In this regard, some of the more notable legislation are as follows:

- ***Payment Services Act 2019***, which provides for the licensing and regulation of payment service providers and payment services in Singapore.
- ***Securities and Futures Act***, which regulates the activities and institutions in the securities and derivatives industry, including leveraged foreign exchange trading, of financial benchmarks and of clearing facilities.
- ***Moneylenders Act***, which regulates moneylending, the designation and control of a credit bureau, and the collection, use and disclosure of borrower information and data.
- ***Commodity Trading Act***, which regulates certain types of commodity trading.
- ***Insurance Act***, which regulates the insurance business in Singapore, insurers, insurance intermediaries and related institutions.

Singapore

4. Describe the regulatory framework(s) for payment services operating in Singapore, and the type of payment services that are regulated.

Payment service providers and payment systems are both regulated under the Payment Services Act 2019 ("PS Act"). Payment service providers are licensed to provide specified payment services under the PS Act. Payment systems facilitate the transfer of funds between or among participants and may be designated under the PS Act for closer supervision.

MAS regulates seven payment services under the PS Act (descriptions below from the MAS website):

- ***Account issuance service*** - The service of issuing a payment account or any service relating to any operation required for operating a payment account, such as an e-wallet (including certain multi-purpose stored value cards) or a non-bank issued credit card.
- ***Domestic money transfer service*** - Providing local funds transfer service in Singapore. This includes payment gateway services and payment kiosk services.
- ***Cross-border money transfer service*** - Providing inbound or outbound remittance service in Singapore.
- ***Merchant acquisition service*** - Providing merchant acquisition service in Singapore where the service provider processes payment transactions from the merchant and processes payment receipts on behalf of the merchant. Usually the service includes providing a point-of sale terminal or online payment gateway.
- ***E-money issuance service*** - Issuing e-money to allow the user to pay merchants or transfer to another individual.
- ***Digital payment token service*** - Buying or selling digital payment tokens ("DPTs") (commonly known as cryptocurrencies), or providing a platform to allow persons to exchange DPTs.
- ***Money-changing service*** - Buying or selling foreign currency notes.

5. How does Singapore's payments licensing laws apply to cross-border business into your jurisdiction?

There is no automatic transfer of the licensed status of a foreign payment services company into Singapore. Foreign entities that wish to offer payment services in Singapore must establish a local presence (branch, subsidiary or related company) and apply for a license under the Payment Services Act.

6. What are the main requirements to be licensed for payments in Singapore?

According to the MAS Guidelines on Licensing for Payment Services Providers, a legal entity (at least 51% owned by Singaporean persons) desiring to be a payment services provider must apply for a license and satisfy the MAS that it will, inter alia, meet certain governance and ownership requirements, have a minimum stipulated base capital, is 'fit and proper', have key management persons with the requisite expertise and experience, provide financial security guarantees to the MAS, and establish certain compliance, technology risk management and audit arrangements so as to run the business properly.

Singapore

7. What is the process to become licensed for payments in Singapore?

There are three licenses under the Payment Services Act 2019 – a money changing license (MC), and standard payment institution (SPI) license, and a major payment institution license (MPI).

Together with the MAS-prescribed application form, the applicant must also submit a detailed business plan, enterprise-wide AML/CFT risk assessment, and AML/CFT manual for the MAS' evaluation.

It is usual that the MAS will interview the key personnel from the applicant entity, and thoroughly examine the application documents, before making a decision to grant the license. MAS customarily first grants an approval-in-principle, setting out a list of conditions that must be fulfilled (together with deadlines) before the license itself is granted. The entity is not allowed to conduct business until the license is granted.

8. What payment services "passporting" arrangements does Singapore have with other countries, if any?

There is no automatic transfer of the licensed status of a foreign payment services company into Singapore. In late 2017, the MAS, together with IFC, a member of the World Bank Group and the ASEAN Bankers Association (ABA), introduced an industry FinTech sandbox for financial institutions and FinTech firms as part of the ASEAN Financial Innovation Network (AFIN). The AFIN initiative aligns with announced goals to develop the ASEAN Economic Community, enhance the active collaboration of ASEAN banking institutions, and promote best-in-class banking practices among ASEAN countries. It can be regarded as a regional sandbox for financial services innovation (including payment services); however it presently does not constitute regional 'passporting'. Foreign entities that wish to offer payment services in Singapore must establish a local presence (branch, subsidiary or related company) and apply for a license under the Payment Services Act.

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Singapore.

The MAS has issued several Notices relating to Anti Money Laundering and Countering the Financing of Terrorism ("AML/CFT"). Different notices are addressed to regulated entities in different sectors. Licensed payment service providers are subject to inter alia Notice PSN01 (specified payment services) and Notice PSN02 (digital payment token services).

The AML/CFT regime is aligned with the recommendations of the Financial Action Task Force (FATF), of which Singapore is a member state. The MAS takes a risk-based (as opposed to prescriptive) approach to supervising licensees for AML/CFT risk. "Customer due diligence" (CDD) requirements are broadly in line with FATF recommendations. Identification and verification of account holders, customers, beneficiaries, connected parties are required, and so are checks for sanctioned parties and politically exposed persons (PEPs). Licensees are expected to perform risk assessments on their customers, as well as transaction monitoring.

The other two key pieces of Singapore legislation in this area, the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act and the Terrorist (Suppression of Financing) Act apply generally, including to payment services providers.

Singapore

10. Describe the technology risk requirements that apply to payment services in Singapore.

The MAS Guidelines on Risk Management Practices - Technology Risk contains risk management principles and best practice standards to guide regulated entities in managing technology risks so that they can establish a sound and robust technology risk management framework; strengthen system security, reliability, resiliency, and recoverability; and deploy strong authentication to protect customer data, transactions and systems.

In particular, Notice PSN05 Technology Risk Management applies to payment service providers and sets out requirements for a high level of reliability, availability and recoverability of critical IT systems and for such entities to implement IT controls to protect customer information from unauthorised access or disclosure.

MAS Notice PSN06 Cyber Hygiene applies to payment services providers and sets out measures that they must take to mitigate the growing risk of cyber threats. It prescribes security requirements on securing administrative accounts, applying security patching, establishing baseline security standards, deploying network security devices, implementing anti-malware measures and strengthening user authentication.

11. Describe the data privacy requirements that apply to payment services in Singapore.

The collection, use and transmission of personal data is regulated in Singapore. This is mainly governed by the Personal Data Protection Act 2012 ("PDPA") whose main purpose is to *"govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstance"*. (Section 3 of the PDPA.)

The nine main personal data obligations under the PDPA are:

- Consent
- Purpose Limitation
- Notification
- Access and Correction
- Accuracy
- Protection
- Retention Limitation
- Transfer Limitation
- Openness

Under the PDPA, there are strict provisos to organisations transferring personal data to a country or territory outside of Singapore. Notably, such transfer would only be permitted if the organisation ensures that the transferee outside of Singapore provides a standard of protection of the personal data that is comparable to that provided under the PDPA.

The PDPA has no extra-territorial reach and only affects organisations established outside of Singapore if they conduct their businesses in Singapore or collect/ process personal data in Singapore.

Singapore

As part of doing business, payment services providers require the regular collection of customer and transaction data. These are used for "Know Your Client" purposes and also to serve customers well. Every payment services company in Singapore must appoint a data protection officer and implement a data protection regime.

12. Describe how innovations and inventions are protected by law in Singapore.

Innovations and inventions that are man-made are classified as intellectual property ("IP"). There are three mechanisms the exclusive rights to IP can be registered in Singapore- a patent, a copyright or a trademark.

Other than common law principles (such as the law on confidential information) that would apply, there is legislation that operates to govern these mechanisms for the registering of an IP right. Some of the more notable legislations include:- the Copyright Act, Registered Designs Act, Patents Act, and the Trade Marks Act.

Infringements of these rights can result in common law remedies such as damages and injunctions, and criminal penalties such as fines and imprisonment.

The Intellectual Property Office of Singapore ("IPOS") Act was enacted to establish the IPOS as a statutory board under the Ministry of Law, responsible for advising and administering IP laws. IPOS also plays a significant role in supporting the growth of fintech innovations in Singapore.

Patents

A person who wants to apply for a patent in Singapore can file for one with the Registry of Patents either in person or online. The Registry of Patents in part of IPOS. If the person wants to apply for a patent in multiple jurisdictions, is able to do so under the Patent Cooperation Treaty (administered by the World Intellectual Property Organisation ("WIPO")) using the Singapore's Registry of Patents as the receiving office.

Copyright

There is no official registration of copyrights before the right exists. A copyright will arise immediately upon creation and the right will arise in a work or subject matter in Singapore in the following scenarios:- (1) if the work or subject matter was first published or made in Singapore or in a member country of the Berne Convention or the World Trade Organisation; or (2) the creator of the work or subject matter was a citizen or resident of Singapore or of a member country of the Berne Convention or the World Trade Organisation at the time when the work was first creation.

Trademarks

Trademarks can be registered through IPOS either online or in person. In this regard, a person can choose to register the trademark only in Singapore or internationally through the Madrid Protocol (WIPO's international registration system of trademarks). Registration of the trademark will be effective on the day it is filed. Moreover, under the Trademark Act in Singapore, there is statutory protection for foreign businesses that are well known in Singapore (such as Apple or Nike) whereby these businesses can avail themselves to the rights and remedies provided under the act even without registering their trademarks.

Singapore

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

Cryptocurrencies/cryptoassets businesses are present in Singapore. The regulations that apply depend on the type of cryptocurrency/cryptoasset in question.

If the cryptocurrency/cryptoasset has the attributes of a commodity, the Commodity Trading Act is the relevant legislation. This act regulates business activities involving, among others, "spot commodity trading" which is defined under the act as "... the purchase or sale of a commodity at its current market or spot price, where it is intended that such transaction results in the physical delivery of the commodity". The regulatory body overseeing the Commodity Trading Act is Enterprise Singapore.

If the cryptocurrency/cryptoasset has the attributes of a digital payment token, the relevant legislation is the Payment Services Act 2019, which governs the licensing and regulation of payment service providers and payment systems in Singapore. A digital payment token refers to a digital representation of value that is expressed as a unit, is not denominated in any currency and is not pegged by the issuer to any currency, is intended to be used as a medium of exchange, and can be transferred, stored or traded electronically. The regulatory body overseeing the Payment Services Act is the MAS.

If the cryptocurrency/cryptoasset has the attributes of a capital market product, the relevant legislation is the Securities and Futures Act. Capital market products include securities, units in a collective investment scheme, derivatives contracts, and spot foreign exchange for the purpose of leveraged foreign exchange trading. The regulatory body overseeing the Securities and Futures Act is the MAS.

South Korea

1. What is the payments landscape in Korea:
The types of activities, state of development of the market and new trends eg FinTech if any?

The payments landscape in the Republic of Korea ("Korea") is ever-evolving. Despite heavy reliance on paper money in the previous years, the types of payment activities that are taking place currently include paper payments, card-based payments, e-commerce payments and alternative payments. Alternative payments have been gaining traction in recent years with the increasing usage of platforms including Samsung Pay, KakaoPay, Naver Pay and QuickPass. As such, Korean tech giants are delving into FinTech with several payment options.

The payments industry has already experienced high growth and maturation. Although the Korean population has one of the highest smartphone possession, it was still a bothersome process to make basic money transfers until recently. Previously, it would take several steps for consumers to transfer a small amount of money – as small as $10. However, with the emergence of new FinTech platforms offering mobile payments, the process was simplified to a single password and one click.

With the support of the government, companies spanning from internet-platform providers such as Naver and Kakao to fintech startups such as Toss have been given permission to offer services to Koreans that make mobile payments and money transfers easier and faster. Previously, cumbersome government regulations and old-fashioned ways of thinking inhibited such advancements. Now, consumers have diverse payment options, such as Samsung Pay, KakaoPay, Naver Pay, Toss and more.

As Korea's startup ecosystem grows and attracts more global attention, the Korean government is keen to help foster the ideal environment in which to grow and breed more successful companies. Being on par with the government agenda has allowed Korea's FinTech scene to accelerate.

New trends in the Korean payments landscape include the emergence of digital-only banks, trend for a cashless society, expected growth of debit cards and government schemes to support FinTech startups.

The emergence of banks pioneered by tech giants is likely to further accelerate the shift towards electronic payments. The country's innovation leaders are pursuing FinTech adoption with payment solutions such as Kakao Pay by Kakao, N Pay by Naver, and Samsung Pay. Digital-only banks, namely Kakao Bank by Kakao and K Bank by KT Corp, are also popular, with Kakao Bank app having more than 5 million users and K-Bank app having more than 1 million users. By allowing consumers to open bank accounts in-app, these platforms are transforming the traditionally brick-and-mortar banks right to the convenience of consumers' smartphones.

In June 2017, electronics manufacturing company LG launched its mobile payment solution LG Pay, which can be used to make contactless mobile payments. In April 2018, South Korea-based payment solutions provider HAREX InfoTech and Jeju Bank together launched a mobile app, UBpay, which allows users to make payments in their method of choice: in-store or online, via a merchant's QR code, a barcode, or contactless. The contactless payment option suits the current global atmosphere of promoting social distancing.

South Korea

To reduce the dependence on cash for smaller-value transactions, the Bank of Korea (BOK) (the country's central bank) launched the Coinless Society Project with a pilot in April 2017. This allowed merchants to transfer the remaining balance from the total payment value to a customer's bank account or other electronic payment instrument (such as a prepaid card), instead of returning it as physical money. If successful, BOK may expand this initiative to include more merchants, helping to drive electronic payments.

Among all financial cards in South Korea, debit cards are expected to record the fastest growth, due to favorable government policy to deduct income tax and active product development from operators to attract more customers to their debit card products. The South Korean government offers higher tax deduction rates for debit cards compared with other financial cards, such as credit cards.

FinTech startup activities are also vibrant. There were an estimated 400 FinTechs in South Korea, operating in diverse areas including payments, remittance, personal finance and more. The ecosystem benefits from access to funding from financial service players as well as large tech companies, besides the regulator's measures to bring regulatory clarity to FinTech operations. Financial services players are eager to connect with FinTech startups through funding and incubation. Combined with the Korean government's schemes to support startups, the era of FinTech startups in Korea is near.

Citations: Kim, Joey. "Why South Korea Is Primed for Fintech Growth." International Banker, 5 Dec. 2019, internationalbanker.com/technology/why-south-korea-is-primed-for-fintech-growth/.

"Payments Landscape in South Korea: Opportunities and Risks to 2022." GlobalData, June 2018, store.globaldata.com/report/fs0140ci--payments-landscape-in-south-korea-opportunities-and-risks-to-2022/t. "Financial Cards and Payments in South Korea." Euromonitor, Euromonitor International, Nov. 2019, www.euromonitor.com/financial-cards-and-payments-in-south-korea/report.

Mittal, Varun. "South Korea FinTech Landscape." ResearchGate, Jan. 2019, https://www.researchgate.net/publication/330701592_South_Korea_FinTech_Landscape.

2. Which official agency regulates payments in Korea?

The Financial Services Commission ("FSC") regulates payments in South Korea. The FSC is a government agency with statutory authority over financial policy and regulatory supervision. The FSC shares its functional responsibilities with the Securities and Futures Commission ("SFC") and subordinate bureaus.

The seven subordinate bureaus are Planning & Coordination Bureau, Financial Consumer Bureau, Financial Policy Bureau, Financial Industry Bureau, **Financial Innovation Bureau** (*formulate policy on financial innovation and fintech industry*), Financial & Corporate Restructuring Policy Bureau and Capital Markets Bureau. The regulators have taken some measures over time to bring more clarity to FinTech operations and facilitate them by easing requirements placed thereon.

Citations: "Specialized Credit Finance Business Act", As Amended by Act No. 11758, Apr. 5, 2013 "Organization Chart." Financial Services Commission, Financial Services Commission, www.fsc.go.kr/eng/new_about/organization_chart.jsp?menu=08.

South Korea

3. What are the main sources of laws regulating payments services in Korea?

In Korea, various laws regulating payments services are in place. The Specialized Credit Finance Business Act ("SCFBA") applies to payments that are made with credit, debit and pre-paid cards. The Electronic Financial Transactions Act ("EFTA") and the Foreign Exchange Transactions Act ("FETA"), applies to payments made with foreign currency or made between Korea and other countries. These payments are also regulated by the licensing requirements under the FETA.

Financial Investment Services and Capital Markets Act

This Act seeks to promote the financial innovation and fair competition of the capital markets and seeks sound development of the financial investment industry. Among its many objectives, it seeks to strengthen investor protection. The Act unifies financial services related to capital markets – including the securities industry, asset management industry, futures industry, and trust industry – to financial investment services.

Regarding the different areas of FinTech, the Act was amended in 2016 to provide a legal framework for equity-based crowdfunding. Accordingly, there are limits to the amount of funding that can be raised and the type of companies that can use this method of funding.

Bank of Korea Act

The Act provides the Bank of Korea with a legal basis for its operation and management of national payment systems. Under the Act, the Monetary Policy Committee of the BOK formulates the basic policy on oversight of payment systems and operation of BOK-Wire. The Bank of Korea operates the BOK-Wire system, oversees payment systems and develops new payment arrangements to ensure the safety and efficiency of payment and settlement in Korea.

Framework Act on Electronic Documents and Transactions

This Act consists of provisions regarding electronic messages, largely derived from the UNCITRAL Model Law, and other provisions on policy measures such as data protection, consumer protection, certified electronic data depositaries and e-Commerce Dispute Mediation Committee unique to the Korean e-Commerce environment.

Digital Signature Act

This Act together with the Framework Act on Electronic Documents and Transactions gives legal certainty to paperless electronic documents and digital signatures used in e-commerce. Furthermore, this Act helps ensure authenticity and non-repudiation in e-commerce.

Citations: "Laws and Regulations." Bank of Korea, Bank of Korea, www.bok.or.kr/eng/main/contents.do?menuNo=400046.
"Payment Systems in Korea." Bank of Korea, Bank of Korea, www.bok.or.kr/eng/main/contents.do?menuNo=400045.
"Financial Investment Services and Capital Markets Act", As Amended by Act No. 12383, Jan. 28, 2014

South Korea

4. Describe the regulatory framework(s) for payment services operating in Korea, and the type of payment services that are regulated.

A. The Electronic Financial Transaction Act (EFTA)

The EFTA covers (i) the rights and obligations of the parties to an electronic financial transaction (ii) provisions to ensure the safety of electronic financial transactions and protection of uses and (iii) authorization, registration and specific scope of activities of electronic financial businesses.

The type of payment services that are regulated

The following activities are listed as "electronic financial business" under the EFTA: (a) issuance and management of electronic currency, (b) electronic funds transfer services, (c) issuance and management of electronic debit payment services, (d) issuance and management of electronic prepayment services, (e) electronic payment settlement agency services, (f) depository service for settlement of transactions, and (g) intermediary electronic collection and payment services between payers and payees. Other than the issuance and management of electronic currency, which needs to be licensed by the FSC, the above types of electronic financial businesses must be registered with the FSC and are supervised by the FSC and the Financial Supervisory Service (FSS).

B. Bank of Korea Act – 'Payment System Operation and Management Regulations'

The law allows the right by the Bank of Korea to require other institutions to submit materials if needed for enhancement of the security of payment services. It regulates how the Bank of Korea can monitor other institutions' payment services practice. It uses 'the important principles of payment services system' made by BIS (Basel Accords) as the standard for security and efficiency of payment services.

C. The Personal Information Protection Act (PIPA)

The PIPA is the overarching personal data protection law in Korea that may apply to fintech businesses operating in Korea. The PIPA prescribes detailed measures for each of the stages involved in the processing of personal data such as collection and use, provision to a third party, outsourcing and destruction.

The PIPA and the Network Act prescribe detailed technical security and administrative requirements for cyber security, such as (i) the establishment and implementation of an internal management plan for the secure processing of personal information (ii) installation and operation of an access restriction system for preventing illegal access to and leakage of personal information, and (iii) the application of encryption technology to enable secure storage and transfer of personal information.

D. The Foreign Exchange Transaction Act

The Act regulates foreign exchange businesses, including the issuance or dealing of foreign exchange and payment, collection and receipt between Korea and a foreign country.

E. The Act on Consumer Protection in e-Commerce

The Act regulates online retailers, including persons engaged in the business of selling goods or services by providing information relating to such goods or services and soliciting offers to purchase from customers by means of mail or telecommunications networks.

Citations: 연구논문: 비은행금융기관의지급결제서비스에관한법제연구 (한정미), Korea: Fintech 2019

South Korea

5. How does Korea's payments licensing laws apply to cross-border business into your jurisdiction?

A. Access to new customers in Korea

Where a fintech business established out of Korea wishes to access new customers in Korea, it will need to consider whether it requires authorization from a Korean regulatory authority. A fintech business established outside of Korea may be subject to Korean laws and regulations if it carries out regulated activities in Korea. Where an overseas fintech business performs regulated activities in Korea, it will need to obtain authorization from the relevant Korean financial regulatory authority such as the FSC or the FSS. Generally, the standard to determine the applicability of Korean laws to foreign fintech businesses is whether the foreign fintech businesses target Korean customers (e.g., Korean website) or allow payment in Korean won.

B. Data privacy

Regarding data privacy, the PIPA applies to all personal information processing entities regardless of whether they are located overseas. In addition, sector-specific privacy laws such as the Network Act would apply to overseas online service providers collecting personal information in Korea. Further, the Credit Information Act would also apply to overseas entities handling financial transaction information and credit information of individuals or entities in Korea. Although the PIPA, the Credit Information Act, and the Network Act do not specifically address their jurisdictional scope of overseas entities, the Korean regulatory authorities have measures to ensure compliance by overseas entities with these laws.

C. Cyber activities that may be criminalized

Further, the EFTA criminalizes certain types of cyber activities that may apply to fintech businesses operating in Korea. The EFTA criminalizes cyber activities that: (a) intrude on electronic financial infrastructure without proper access rights or by surpassing the scope of permitted access rights or altering, destroying, concealing or leaking data that is saved in such infrastructures; and (b) destroy data, or deploy a computer virus, logic bomb or program such as an email bomb for the purpose of disrupting the safe operation of electronic financial infrastructures.

Citations: 연구논문: 비은행금융기관의지급결제서비스에관한법제연구 (한정미) , Korea: Fintech 2019

6. What are the main requirements to be licensed for payments in Korea?

To be eligible as providers of payment services in Korea, businesses need to be registered and acquire licenses from the relevant authority such as the Financial Services Commission or the Ministry of Strategy and Finance.

A. Electronic Payment

To perform services for electronic payments in Korea, the operator of the financial company needs to obtain permission from the Financial Services Commission and register with the FSC and the financial company needs to have a minimum capital amount as provided for in EFTA, the amount of which is determined based on what type of company the financial company is. On top of holding the necessary capital, the business also needs to meet the requirements stated in EFTA and (1) be equipped with professional human resources, and physical installations, such as computer equipment, sufficient to protect users and carry out the intended business, (2) meet the standards of financial soundness, (3) have a proper and sound plan necessary to execute the business concerned, and (4) secure the major investors with sufficient investment capability, sound financial state, and social credit.

South Korea

B. Financial Investment Services

An entity wishing to engage in financial investment business has to be a (1) stock company incorporated under the Commercial Act or a financial institution specified by presidential Decree, or (2) a foreign financial business entity with a branch office or any other business office necessary for conducting the business it runs in the foreign country.

Businesses meeting the above requirements shall have: (1) equity capital of at least KRW 500 million; (2) a feasible and sound business plan; (3) human resources or sufficient electronic computer systems and other physical facilities; (4) appropriate executive officers; (5) major shareholders or foreign financial investment business entities with sufficient investment capabilities, good financial standing, and social credibility; and (6) a system preventing conflicts of interest between the financial investment business entity and investors as per the Financial Investment Services and Capital Markets Act (FISCMA).

C. Foreign Exchange Transaction Services

Anyone intending to conduct foreign exchange business needs to be registered with the Minister of Strategy and Finance. To be approved and provide such services the person intending to conduct such business needs to meet the requirements set out in the Foreign Exchange Transaction Act. These include (1) having the appropriate capital size and financial structure pursuant to the standards of the Financial Services Commission, (2) being equipped with the appropriate computerized facilities connected to the foreign exchange computer network, (3) having at least two persons per business office with experience in the foreign exchange business for more than two years or with educational background prescribed by the Minister of Strategy and Finance.

Anyone who wants to conduct small overseas remittance services needs to be registered with the Minister of Strategy and Finance. To be approved for registration and provide such services, the person intending to conduct such business needs to meet the requirements set out in the Foreign Exchange Transaction Act. These include (1) having a capital of at least KRW 1 billion pursuant to the Commercial Act, (2) meeting the standards of financial soundness announced by the Minister of Strategy and Finance, (3) having the foriegn exchange information center and the computer network be connected, (4) having the appropriate computerized equipment, (5) having at least two persons with experience in the foreign exchange business for more than two years or with educational background prescribed by the Minister of Strategy and Finance, and (6) having executives who are not subject to disqualification under the Act on the Governance of Financial Companies.

D. Regulatory Sandbox

The financial services can also be licensed for a limited time period if designated as an "innovative financial service" under the Special Act on Support for Financial Innovation. This temporary license is to allow for startup fintech companies to provide innovative services without being prevented by strict financial regulations. Those who are eligible for designation are (1) financial companies (2) under the Commercial Act, the business places of which are domestically located.

For further authorization of payment services after the designation period, the Innovative financial service provider needs to (1) provide that the purposes of the designation of innovative financial services have been achieved and (2) submit documents proving that he or she is able to comply with financial regulations, the application of which is postponed during the designation period.

In addition to the Regulatory Sandbox, there are recent movements towards approving small or provisional licensing which would allow further subdivisions for allowing such provisional licenses and lower the entry threshold for payment service providers. This amendment to the Financial Innovation Act would provide legal foundation for companies hoping to continue provision of payment services after the regulatory sandbox period.

Citations: 금융위 "금융규제샌드박스내실화"...혁신서비스 4건지정, 뉴시스, May 28, 2020,
Retrieved from: https://newsis.com/view/?id=NISX20200528_0001039987&cID=10401&pID=10400

South Korea

7. What is the process to become licensed for payments in Korea?

To provide payment services in Korea, one is required to register with the relevant authorities such as the FSC or the Ministry of Strategy and Finance.

The process for being registered and licensed as a financial investment service provider would be as follows:

Financial Investment Services and Capital Markets Act
Article 13 (Application for Authorization and Examination)

- An entity that wishes to obtain authorization for a financial investment business shall file an application for authorization with the Financial Services Commission.
- The Financial Services Commission shall, within three months of receiving an application filed in accordance with paragraph (1) examine the application to determine whether authorization for financial investment business shall be granted, and shall notify the applicant in writing of its decision and the grounds therefor, without delay. In such cases, the Commission may demand that the applicant make a supplementary correction, if any deficiency exists in the application for authorization.

The process for being licensed to provide electronic payment services would be as follows:

FSC, Regulation on Supervision of Electronic Financial Transactions
Article 45 (Licenses, etc.)

- An applicant shall provide the Financial Services Commission with an application for a license and necessary accompanying documents, as determined by the Governor of the Financial Supervisory Service, after performing the terms of, and conditions to, the preliminary license, etc.
- The Financial Services Commission shall examine and determine whether to accept an application for a license, etc. based on the relevant Acts and subordinate statutes and the detailed guidelines on licenses, etc. set forth in the Act.
- If the Financial Services Commission accepts an application for a license, etc., it may attach conditions thereto; and if it rejects such an application, it shall notify the applicant in writing thereof.
- The Financial Services Commission may conduct an on-site inspection to verify whether the terms of, and the conditions to, a preliminary license, etc. have been performed, and the relevant applicant shall actively cooperate therein.
- If any condition has been attached to a preliminary license, etc. or a license, etc., the relevant applicant shall report its performance status to the Financial Services Commission without delay after the designated deadline for performance.

Article 46 (Submission of Supplementary Documents, etc.) The Financial Services Commission may require an applicant to provide supplementary documents and other additional data by a prescribed deadline if it needs such documents or data in examining the application for a preliminary license, etc. or for a license, etc.

Article 47 (Public Announcement of Licenses, etc.) When the Financial Services Commission accepts an application for a license, etc., it shall immediately announce the details in the Official Gazette and notify the public thereof via the Internet or by other means.

South Korea

8. What payment services "passporting" arrangements does Korea have with other countries, if any?

With Passporting arrangements, companies from different countries can trade freely in other countries with minimal additional authorization. Although Korea does not have traditional passporting arrangements there is a similar form of passporting in the funds management industry which involves payment services provided by fintech companies between South Korea, Australia, Japan, New Zealand, and Thailand under the Asian Region Funds Passport (ARFP) which commenced on Feb. 1, 2019.

The ARFP allows collective investment schemes (CIS) established and regulated in one Participant's economy to be offered to investors in another Participant's economy.

In Korea, a foreign collective investment scheme (CIS) operator offering ARFP funds to Korean investors need to first register the funds with the Financial Services Commission/Financial Supervisory Service.

Citation: (Asia Region Funds Passport, Retrieved from: https://fundspassport.apec.org/)

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Korea.

A. **Money laundering**

A corporation is not held jointly liable with the offender, when the corporation has not been negligent in exercising care and supervision of the employee who violated relevant anti-money laundering laws.

B. **Mobile payment services**

Allows non-bank and non-securities account holders to make payments with mobile phones. However, payment service providers may be non-traditional financial institutions with widely varying controls and supervision measures.

C. **Mobile money services**

Subscribers are able to store actual value on their mobile phone. They may use phone credits or airtime as tender for payment. Such systems offer versatility but may often fall out of regulation and prudential supervision altogether.

D. **Mobile financial information services:**

Users may view personal account data and general financial information, but there is no capability for any financial transaction and therefore may be considered low risk.

South Korea

E. Authorities

The Financial Intelligence Unit (FIU) is entitled to:
Gather and analyse financial transaction information relating to suspected illegal assets or money laundering acts.
Provide information to the District Prosecutor's Office, the police, the National Tax Service, Korea Customs Service and the Financial Supervisory Service when the information is necessary in:

- Conducting a criminal investigation;
- Implementing a regulatory inspection;
- Performing an audit of financial transactions; and
- Exchanging information and cooperating with foreign governmental agencies.

Citation: "Figure 2f from: Irimia R, Gottschling M (2016) Taxonomic Revision of Rochefortia Sw. (Ehretiaceae, Boraginales). Biodiversity Data Journal 4: e7720. Https://Doi.org/10.3897/BDJ.4.e7720." doi:10.3897/bdj.4.e7720.figure2f.

10. Describe the technology risk requirements that apply to payment services in Korea.

Operational Risk Exposure

A. Fraudulent transaction

Transactions resulting from fraud have always been a source of operational risk with respect to check processing. While automated software detection systems are designed to interface with various payment systems and detect fraud, payments that span multiple payment channels are still difficult to catch. Some fraud types have declined with the introduction of this software but, with new payment instruments available, this is a constant struggle to ensure Bank Secrecy Act/Anti-Money Laundering systems can be attributed to all payment instruments.

B. Interconnectivity

The complex interconnections between systems and vendors in the financial services industry also increase operational risk. It is difficult to find a firm that is not somehow connected to a shared service provider or other financial entities, as the nature of payment systems is to allow for settlement to take place across accounts and financial organizations. Even so, with greater connectivity, there is the risk that a single point of failure or malicious threat could have a compound impact.

C. Technology innovations

New technology is used to innovate the payment instrument offerings, as well as the payment clearing and settlement process itself. The use of still unproven technologies or products deployed from them has the ability to provide points of failure, as well as fraud or malicious exploitation. Further, controls over each payment instrument must be carefully considered prior to deployment to ensure it does not introduce unintended risks to the broader payment system.

D. **Nonbank**

Fueled by the latest technologies and customer demands for new financial products and services, some non bank entities serve as competitors while others have products that maybe used or acquired by financial institutions or competing service providers. Regulatory scrutiny over such entities is significantly different. Consequently, the ability for these entities to offer a stable, secure product or handle customer information in a compliant manner may pose a direct or indirect risk to payment systems.

E. **Cybersecurity**

Threats to cybersecurity continue to build as attacks evolve and the introduction of more electronic payment channels offer additional access points to be exploited. System availability has grown in importance, as more transactions and real time information is expected; thus, the threat of cybersecurity also poses a risk that a system or information will not be available or accurate when needed.

F. **Process failures**

Processes resulting in limitations of system automation or errors in human controls can also be a significant source of operational risk, either by allowing fraud or malicious actions to be taken or unintentional errors and omissions to occur.

Citation: *201805-Information-Technology-Risk-Payment-Systems-and-Operations*.

11. Describe the data privacy requirements that apply to payment services in Korea.

Personal Information Protection Act (PIPA)

In South Korea, all entities that process personal data for business purposes must follow the Personal Information Protection Act. PIPA is the main governing law that calls for security during establishment and the implementation of personal data, prevention of illegal access and leakage and the use of encryption technology when handling personal information. It follows that the business must inform and receive consent from the data subjects in regards to the purpose of the collection and use of the personal data, the type of information that will be collected, duration of the possession, as well as the full disclosure that the data subject has a right to refuse and any consequences that may follow.

Act on the Promotion of Information and Telecommunications Network Use and Information Protection (The Network Act)

The Network Act complements the Personal Information Protection Act (PIPA) but focuses it on protecting the personal information in the context of online service providers. Under the Network Act, they must fully disclose the purpose of the collection and use, information that will be gathered, duration of the possession, as well as consent similar to PIPA. In addition, high measures of security are required in order to prevent the information from being damaged, altered, stolen or leaked. There are more detailed regulations such as a plan for the protection of personal data, regulation of the access to the personal data systems, prevention of manipulating personal data as well as computer viruses and lastly restriction on the act of duplicating personal data records. There is also a requirement that biometric information and passwords be one-way encrypted to prevent decoding and a secure algorithm protecting credit card numbers and bank account number, and encryption of the personal data that will be delivered through communication networks. Lastly, in the event that any entity's rights are infringed then they possess the right to make the operator take down the content as an obligation.

The Credit Information Act

The Credit Information Act serves to both regulate and protect information related to financial transaction and credit card information.

South Korea

12. Describe how innovations and inventions are protected by law in Korea.

Intellectual Property Rights (IP Rights)

In South Korea, intellectual property rights, also known as IP rights, protect and provide the legal right to an entity's innovations and inventions. There are three main types of IP rights which are the industrial property rights, copyright and the new intellectual property rights. In industrial property rights, there are patent rights, utility model rights, design rights and trademark rights which protects the major invention, minor invention, design and symbol of the company respectively. Copyright consists of just copyright, neighboring right and database which is more concerned with protecting the creative work of performers and producers. The new intellectual property rights uses industrial copyright and information property rights to provide protection on newly emerging industries.

Patent Act, Utility Model Act, Design Act, Trademark Act

In the context of fintech, there are certainly industrial property rights that must be in focus which are patent rights, utility model rights, design rights and trademark rights.

According to the Patent Act, fintech in regards to the software of business methods may create a patent as long as it meets the requirements of industrial applicability, but also that it is not a currently existing technology, and is not easily conceivable. In the case that the invention does not meet the requirements for a patent, then it may be protected under the Utility Model Act, which requires a lower technical content. However, due to the fact that fintech is mainly software and business-based it may make it not eligible to be used for utility methods.

The Design Act will most likely protect fintech software's graphical user interfaces and the trademark act would protect anything like the service, collection or business emblems.

Copyright Act

The Copyright Act provides protection in the context of morals and economic rights in order to ensure the honor and economic benefit of the producer is given rightfully. The creation of the work automatically brings a copyright to the work, which means that others must receive proper permission from the copyright owner before using it for their benefit.

Trade Secret

A "Trade Secret" is protected if it is useful for the business, unknown to the general public, contains independent economic value and reasonable effort is necessary to maintain secrecy. This may apply to fintech software's source code. In the event that these rights are infringed, a lawsuit may be executed within ten years of the infringement or within three years of becoming aware of the infringement and the identity of the infringing party.

South Korea

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

Cryptocurrency has been quite prevalent in the Korean market and the Korean government recently in March 2020 passed a new legislation addressing the topic. The new legislation is an amendment to the **Act on Reporting and Using Specified Financial Transaction Information** (the "Act"). The Act has completely legalized cryptocurrency in Korea and will provide a framework for the regulation and legalization of cryptocurrencies and crypto exchanges. This will authorize Korea's financial regulators to effectively oversee this budding industry and develop rules around anti-money laundering which is based on the standards set by the Financial Action Task Force ("FATF"), the global money-laundering watchdog. The new legislation will require all virtual asset service providers to register with regulators and partner with a single bank for deposits and withdrawals. This will be a challenge for mid-sized and small sized exchanges as banks have been reluctant to provide such service for them. Nevertheless, by requiring real-name accounts with an approved Korean bank associated with every exchange (the real-name verification system), the Act seeks to prevent money laundering. The Act will enter into force in September 2021 after a six-month grace period.

Currently, individual's crypto profits are not taxable. However, the Ministry of Economy and Finance, which oversees Korea's economic policy, has recently announced that capital gains tax will be applied to cryptocurrency trading starting next year (2021). Although there was disagreement on how income from cryptocurrency trading should be viewed as, whether it be as transferable income or as 'other income', the Ministry adopted the taxation scheme used in the United States, which is capital gains.

Taiwan

1. What is the payments landscape in Taiwan:
The types of activities, state of development of the market and new trends eg FinTech if any?

E-payment activities are regulated by the E-Payment Act (the Act Governing Electronic Payment Institutions, enacted in 2015) and its related regulations.

Please see our response to *Question 4* for the three main types of activities that an "electronic payment institution" may carry out under current law. Currently, besides banks (as banks may also be permitted to, concurrently, conduct such activities with FSC's approval), there are nine "electronic payment institution" license holders. Most of them are either the e-payment arm of a medium / large sized corporate group (e.g., electronic commerce, game, convenience store, telecom, etc.) or owned by government.

2. Which official agency regulates payments in Taiwan?

FSC (Financial Supervisory Commission).

3. What are the main sources of laws regulating payments services in Taiwan?

E-Payment Act (the Act Governing Electronic Payment Institutions, enacted in 2015) and its related regulations.

4. Describe the regulatory framework(s) for payment services operating in Taiwan, and the type of payment services that are regulated.

The E-Payment Act regulates the activities of an "electronic payment institution", acting in the capacity of an intermediary between payers and recipients to engage, principally, in:

i. Collecting and making payments for real transactions as an agent;
ii. Accepting deposits of funds as stored value funds; and
iii. Transferring funds between e-payment accounts.

An electronic payment institution should obtain a license from the FSC unless it engages only in (i) above and the total balance of funds collected and paid and kept by it as an agent does not exceed the specific amount set by the FSC.

Taiwan

5. How does Taiwan's payments licensing laws apply to cross-border business into your jurisdiction?

No foreign entity may carry out e-payment business in Taiwan without a license issued by the FSC.

6. What are the main requirements to be licensed for payments in Taiwan?

Main requirements for applying to the FSC for the license of an "e-payment institution" include, among others, the following:

- Minimum capital requirements: TWD 500 million (but TWD 100 million for item (i) of *Question 4* (i.e., collecting and making payments for real transactions as an agent)).
- Requirement for reserve
- Trust or bank guarantee (for funds stored/deposited by users)
- Information security *(see Question 10 for details)*

7. What is the process to become licensed for payments in Taiwan?

Major steps for application to the FSC for the license of "electronic payment institution":

- Application to the FSC for approval
- Application to the Investment Commission for foreign investment approval (in case the future shareholder is a foreigner)
- Application to the corporate registration authority for company establishment
- Application to the FSC for business license

8. What payment services "passporting" arrangements does Taiwan have with other countries, if any?

No.

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Taiwan.

E-payment institutions are subject to Taiwan's AML law (MoneyLaundering Control Act) and its related regulations. Under Taiwan's AML law, an e-payment institution is required to, among others, implement its own internal AML guidelines and procedures, check and verify the customer's identity (KYC), keep transaction records, report to the government on suspicious transactions, etc.

Taiwan

10. Describe the technology risk requirements that apply to payment services in Taiwan.

E-payment institutions must comply with the FSC's regulations governing the "security control" standards. Relevant mechanisms include the security control for, among others, identity verification, transactions, the platform (e.g., IT system, software program for physical channel, etc.), connection to users' bank deposit accounts, personal data protection, the overall IT security policies of the e-payment institution, etc.

11. Describe the data privacy requirements that apply to payment services in Taiwan.

E-payment institutions are subject to Taiwan's Personal Data Protection Act (PDPA).Under the PDPA, unless otherwise specified under law, a company is generally required to give notice to (notice requirement) and obtain consent from (consent requirement) an individual before collecting, processing or using any of said individual's personal information, subject to certain exemptions. To satisfy the notice requirement, certain matters must be communicated to the individual, such as the purposes for which his or her data is collected, the type of the personal data and the term, area and persons authorised to use the data.

12. Describe how innovations and inventions are protected by law in Taiwan.

The issue here would be whether fintech business models and related software can be protected by intellectual property rights such as copyright or patent.

Copyright

Under Taiwan's Copyright Act, there are no registration or filing requirements for a copyright to be protected by law. However, there are certain features that qualify for a copyright, such as originality and expression. Therefore, while there is a type of copyright called 'computer program copyright' under Taiwan's Copyright Act, whether a work is copyrightable would still depend on whether the subject work has the required components (such as the features described above), especially the feature 'expression' (instead of simply an 'abstract idea').

Patent

As to patent, an inventor may file an application with Taiwan's Intellectual Property Office, and the patent right will be obtained once the application is approved. According to the Patent Act of Taiwan, the subject of a patent right is 'invention' and an invention means the creation of technical ideas, utilising the laws of nature. As a general rule, business methods are regarded as using social or business rules rather than laws of nature, and therefore may not be the subject of a patent right. As for a fintech-related software invention, if it coordinates the software and hardware to process the information, and there is a technical effect on its operation, it might become patentable. For instance, a 'method of conducting foreign exchange transaction' would be deemed as a business method and thus not patentable; however, a 'method of using financial information system to process foreign exchange transactions' may be patentable.

Taiwan

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

Cryptocurrencies, which are not linked or tied to the currency of any nation, are currently not accepted by the Central Bank of the Republic of China (Taiwan) ("Central Bank") as currencies. In an FSC's press release in 2014 ("2014 Release"), the FSC ordered that local banks must not accept bitcoin or provide any other services related to bitcoin (such as exchange bitcoin for fiat currency).

In response to the rising amount of Initial coin offerings ("ICOs"), the FSC also expressed its views on ICO through a press release issued in December 2017 ("2017 Release"), indicating that the classification of an ICO should be determined on a case-by-case basis — if an ICO involves offer and issue of securities, it should be subject to the Securities and Exchange Act ("SEA").

On 3 July 2019, the FSC, by issuing a ruling, officially designated cryptocurrencies with the nature of securities, i.e. security tokens, as 'securities' under the SEA ("2019 Ruling"). According to the 2019 Ruling, security tokens refer to those which:

- Utilise cryptography, distributed ledger technology or other similar technologies to represent their value that can be stored, exchanged or transferred through digital mechanism;
- Are transferable; and
- Encompass all of the following attributes of an investment:
  i. Funding provided by investors;
  ii. Providing funding for a common enterprise or project;
  iii. Investors expecting to receive profits; and
  iv. Profits generated primarily from the efforts of the issuer or third parties.

Since mid-2019, the FSC and the Taipei Exchange ("TPEx") have been setting out the set of regulations governing Security Token Offering ("STO"), and such rules ("STO Rules") were finalized in January of 2020. The FSC differentiates the regulation of STOs with the threshold of 30 million New Taiwan Dollar (NT$). For an STO of NT$30 million or less, the STO may be conducted in compliance with the STO Rules; an STO above NT$30 million must first apply to be tested in the "financial regulatory sandbox" pursuant to the Sandbox Act and, in case the experiment has a positive outcome, should be conducted pursuant to the SEA. Please see below summary of certain key provisions of the STO Rules (i.e., for STOs of NT$30 million or less):

- **Qualifications of the issuer**
  The issuer must be a company limited by shares incorporated under the laws of Taiwan and not a company listed on the Taiwan Stock Exchange or TPEx or traded on the Emerging Stock Market.
- **Types of security tokens that can be issued**
  The issuer can only issue profit-sharing or debt tokens without shareholder's rights.
- **Eligible investors and amount limits**
  Only "professional investors" are eligible to participate in STOs; where the professional investor is a natural person, the maximum subscription amount is NT$300,000 per STO.

Pursuant to the STO rules, there are also some other requirements and restrictions including those regarding trading (secondary market), the STO platform operator (licensing requirements – securities dealer licence, with minimum paid-in capital of NT$100 million, etc.), real-name basis, New Taiwan Dollar only, etc.

Thailand

1. What is the payments landscape in Thailand:
The types of activities, state of development of the market and new trends eg FinTech if any?

Payment Services under the BOT:

A. During the past few years, Thailand is one of the ASEAN countries that has a fast development in the FinTech industry. As of July 2019, Thailand has around 140 FinTech firms, and under half of which are startups, while 43% of the FinTech industry in Thailand focuses on E-Payments.

B. The Thai government initially elaborated a reliable platform designed to support the expansion and development of digital financial services. While the Bank of Thailand ('BOT') has implemented the regulatory policies for supporting payment system businesses and created the special department dedicated to the growth of digital payment systems. More importantly, the Government, in collaboration with the BOT, had launched the National E-Payment initiative called 'PromptPay'. Since then, the number of PromptPay users has been incredibly surged.

C. PromptPay infrastructure enables the public and the business sectors to transfer funds using mobile phone number, national identification number, corporate registration number, or e-wallet number.

D. As of February 2020, the number of PromptPay registration, as announced by the BOT, reached nearly 50 million numbers and an average of 9.1 million transactions per day. Apart from 'PromptPay, the government, in collaboration with the BOT, has developed another e-Payment platform using 'Q.R. Code' technology to support the small businesses (merchants). As of July 2019, the number of merchants accepting payment via standardised Thai QR Code reached 5 million.

E. Because of the popularity of the electronic payment system, it is an excellent opportunity for new players coming from private companies such as tech startups and commercial banks. The BOT has welcomed theses players to come and join the electronic payment platforms because they will implement the innovative technology to booth efficiency of the financial system of Thailand to be more inclusive, cheaper and more comfortable.

F. Types of payment activities under the BOT Notifications are as follows:

- Inter-institution Fund Transfer System Service
- Payment Card Network Service
- Settlement System Service
- Credit Card, Debit Card or ATM Card Services
- E-Money Service
- Acquiring Service
- Payment Facilitating Service
- Electronic Money Transfer Service
- Electronic Money Service (Limited Scope)

Thailand

G. Since there are tons of new startup companies using innovative technologies to create one of the payment platforms, as aforementioned, and trying to steal market shares in payment system from commercial banks. Thus, the banks need to adapt themselves and bring breakthrough technology to develop their original payment platforms in order to compete with these new startups.

H. Before starting operating e-Payment platforms, these startups and commercial banks need to bring the advanced technology and business model to be participated in 'Regulatory Sandbox' launched by the BOT. If the testing program is successful following the BOT's methods, these startups and commercial banks can submit forms to be licensed by the BOT after that.

I. The significant technologies behind these e-payment platforms are as follows:

- Distributed Ledger Technology (DLT) and Blockchain
- Artificial Intelligence (A.I.)
- Application Programming Interface (API)
- Big Data

J. Recently, the BOT in collaboration with 8 commercial banks and a technology partner called 'R3' has developed the new financial infrastructure called 'Project Inthanon'. This Project aims to explore potential benefits of the DLT in enhancing Thailand's financial infrastructure, especially for payment system by creating the decentralised Real-Time Gross Settlement system by using the wholesale Central Bank Digital Currency (CBDC).

K. So far, the Project is in Phase III and collaborating with the Hong Kong Monetary Authority (HKMA) to explore the interoperability amongst ledgers to achieve cross-border funds transfer.

L. As of now, the outbreak of COVID-19 has forced customers to change their consumers' behaviour by doing business or buying goods and services online, which results in the fast growth of e-Payment transactions.

M. Based on the data from TrueMoney, the largest prepaid e-wallet platform in Thailand, it shows that as of March 2020, the new registration users had increased by 1 million accounts from 12 million active users at the end of last year. The delivery food service called 'foodpanda' grew by 25%, while the transactions via Lazada, one of the largest e-commerce platforms in Thailand, increased by 40% in March.

N. Therefore, a new trend in the payment system will be shown in the competition amongst startups and commercial banks in developing advanced technology and business models.

O. Apart from the payment services regulated by the BOT, there is also a significant movement by the Securities and Exchange Commission (SEC) regarding Digital Assets, and the Office of Insurance Commission ('OIC') regarding the 'regulatory sandbox' for FinTech, reflecting their institutional priorities.

Thailand

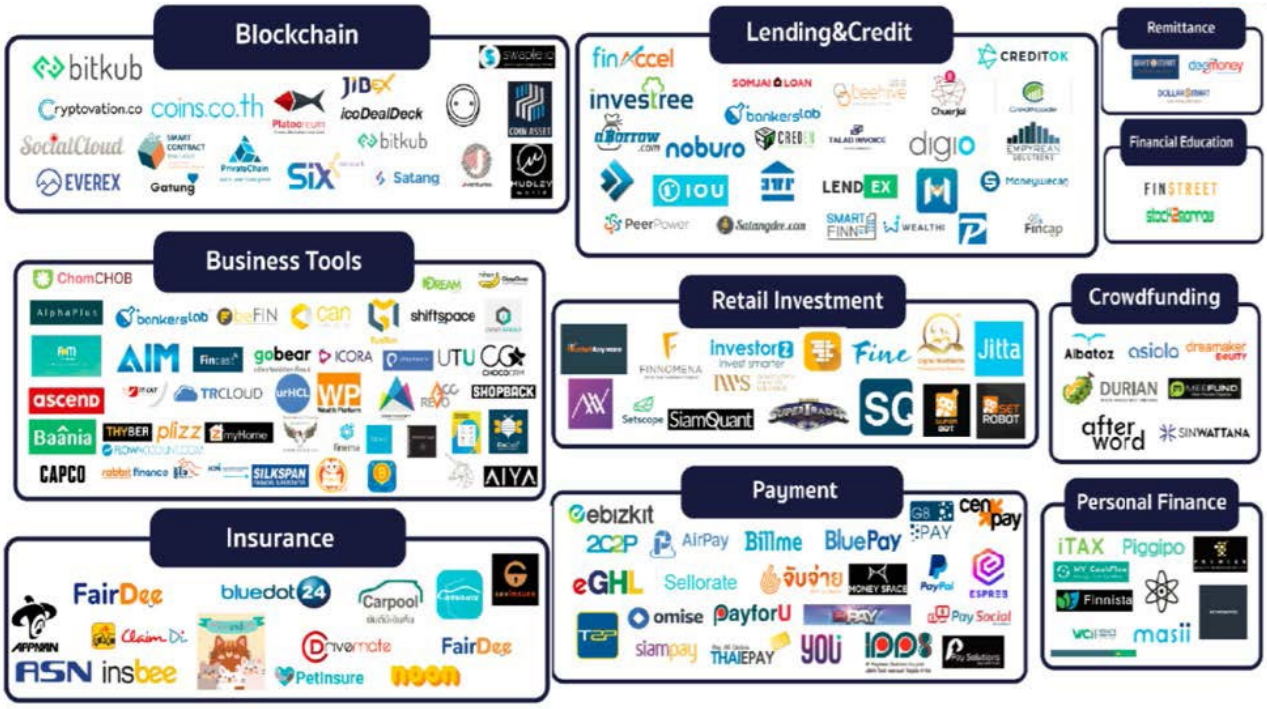
Financial Technology in Insurance Business under the OIC:

A. Since several players are launching 'InsurTech' startup companies, the OIC had established the formal institution called "Center of InsurTech" to focus on the Tech Ecosystem to integrate insurance firms and tech startups to drive the domestic insurance industry forward. The FinTech firms and Technology firms have to cooperate with insurance companies or brokers in regulatory sandbox project to allow participants to test the new technology applicable to insurance transactions, sale process, product launching, complaint filing, smart contract, compensation, and other transactions approved by the OIC.

B. As of May 2020, one of the leading insurance company in Thailand launched the innovative platform aiming to return 'premium' to the customers who had previously purchased COVID-19 insurance. The premium will be returned in the form of digital currency called 'T.P. Coin', which is equivalent to 100% payment, via 'TIP COIN by THINK BIT'. The customer can use the coins to buy goods or use as the discount for insurance policies or as an exchange for COVID-19 protection kits.

This chapter focuses on digital payments platforms supported by the BOT and a partial section relevant to Digital Assets regulated by the SEC.

FinTech Types on Thai Fintech Association:



Source: Thai Fintech Association (2019)

Thailand

2. Which official agency regulates payments in Thailand?

- The key responsible agency is the BOT in collaboration with the Digital Government Development Agency (DGA) and private organisations such as Thai FinTech Association.
- The Securities and Exchange Commission (for Digital Assets).
- The Office of Insurance Commission ('the OIC')

3. What are the main sources of laws regulating payments services in Thailand?

- Payment System Act B.E. 2560 (2017)
  (The most significant act to regulate the payment services)
- Electronic Transactions Act B.E. 2544 (2001)
- Personal Data Protection Act B.E. 2562 (2019) (pending to be enforced)
- Emergency Decree on Digital Assets Business B.E. 2561 (2018)
- Emergency Decree on the Amendment of the Revenue Code (No. 19) B.E. 2561 (2018)
- Regulations on Supervision for System Operator of the Highly Important Payment Systems SorNorChor. 1/2561
- Regulations, Procedures and Conditions on Application for License to Undertake Designated Payment Systems Business SorNorChor. 3/2561
- Regulations, Procedures and Conditions on Application for License and Registration to Undertake Designated Payment Service Business SorNorChor. 5/2561
- Regulations on General Supervision of Undertaking Designated Payment Service Business SorNorChor. 6/2561

4. Describe the regulatory framework(s) for payment services operating in Thailand, and the type of payment services that are regulated.

A. Currently, the BOT has formulated the Payment System Roadmap No. 4 to be a direction for developing Thailand payment's systems during 2019 – 2021.

B. However, during 2017 – 2019, Thailand's digital payment has experienced rapid development, and the public has widely become accustomed to making payments or using fund transfer service via mobile phones. The main contributing factor to this shift has been the implementation of the National E-Payment Master Plan, under which the BOT takes responsibilities for the 'PromptPay' project and the card usage expansion.

C. In Thailand, Payment Systems are divided into 3 main groups which are:

- **Highly Important Payment Systems**

  The payment systems that are the key infrastructure of the country whose problems or disruptions would be likely to affect Thai citizens continually and broadly. This system consists of:

  i. BAHTNET system
  ii. ICAS system (Imaged Cheque Clearing and Archive System)

  ***Please note that these two systems are not open to other private companies or FinTech startups or any commercial banks, the BOT is the only organisation which develops and controls these systems.*

Thailand

- **Designated Payment Systems**

  The payment systems that are the centre or network between system users which may affect public interests, public confidence or stability and security of the payment systems. The system consists of:

  i. Handling Funds Transfer (for retail customers)
  ii. Payment Card Network
  iii. Settlement System

- **Designated Payment Services**

  The payment services which are used widely and have a widespread impact as follows:

  i. Credit Card, Debit Card, or ATM card services
  ii. E-money services
  iii. Accepting E-payment for and on behalf of others/ Payment Facilitating
  iv. E-money Transfer Services
  v. Services with innovative technologies

D. Some of the most famous e-Payment services which have been granted licenses by the BOT include Rabbit-Line Pay, AirPay (Thailand), True Money, 2C2P Plus (Thailand).

E. The Payment Systems Act empowers the BOT to regulate on 3 groups of the payment systems by using a supervisory framework consisting of 5 areas which are summarised as follows:

- Financial Status: to ensure that service providers have sufficient money to continue providing business under both normal and emergencies.
- Governance: to ensure management and internal control of the businesses.
- Risk Management and Security: systematic risk, operational risk including the security of I.T. system (Security, Integrity, Availability)
- System user/Consumer Protection: to ensure that the service providers adequately disclose information related to services to users.
- Promotion of Efficiency and Competitiveness: to promote the level of playing field for both domestic and oversea service providers, and foster competitiveness.

F. Apart from the 5 areas as aforementioned, each group of payment will be regulated in accordance with international standards called Principles for Financial Market Infrastructures (PFMI), which is different based on the type of payment systems as follows

- Systemically Important Retail Payment Systems (SIRPS): for BATHNET
- Prominently Important Retail Payment System (PIRPS): for ICAS, and Interbank Transaction Management and Exchange (ITAX or for PromptPay system)
- Other Retail Payment Systems (ORPS): such as Payment Card Network.

G. Co-operative Oversight: BOT has been working with the Securities and Exchange Commission (SEC) for Securities Settlement Systems (SSS), and Hong Kong Monetary Authority (HKMA) for U.S. Dollar Clearing House Automated Transfer System having linkage to the BAHTNET system.

Thailand

5. How does Thailand's payments licensing laws apply to cross-border business into your jurisdiction?

Payment Service under the BOT:

Designated Payment Services *who operate only 'Payment Card Network'* from other countries who wish to provide cross-border payment services in Thailand need to have the following conditions for submission to be granted a licence (SorNorChor. 3/2561)

A. The foreign company has a branch/ representative in Thailand.

B. There is at least one appointed person who is responsible for operating the business in Thailand. Have at least one director with Thai nationality and domiciled in Thailand.

- The applicant must be the registered business provider of the designated payment services intending to provide payment services or any operations relating to payment services to support payment service providers from other countries, who wish to provide cross-border payment services in Thailand.
- The provision of payment services to the service provider from abroad must not be arranged to facilitate any evasion of or non-compliance with the laws on payment systems.
- Additional Documents once applying the BOT
  - i. A copy of a juristic person registration certificate according to foreign law.
  - ii. A copy of articles of association or objectives (if any).
  - iii. A copy of the register of shareholders of a juristic person and/or report of list of shareholders and percentage of top 10 shareholdings of the juristic person including shareholders' nationalities.
  - iv. Names, nationalities, domiciles, working experiences and qualifications of all directors and persons with managerial power; together with the certification of qualifications of persons appointed as directors or persons with managerial power of the person intending to undertake designated payment systems business.
  - v. Corporate group structure such as parent company, subsidiaries and affiliates including duties, responsibilities and relationship related to the person intending to undertake designated payment systems business.
  - vi. A copy of license certificate to undertake payment systems business according to foreign law (if any).
  - vii. A copy of a certificate for business operation of foreigners or a copy of company registration certificate, showing the establishment of a branch office or representative office in Thailand, including details of location, list of persons responsible for engaging in affairs for and on behalf of the juristic person in that office and telephone number of the branch office in Thailand.

Thailand

6. What are the main requirements to be licensed for payments in Thaildand?

First, only two groups are consisting of 'Designated Payment Systems and Designated Payment Businesses', who can be licensed and registered from the BOT.

A. Designated Payment Systems

Under the Payment Systems Act Section 17 and Section 18 and Bank of Thailand Notification no. SorNorChor. 3/2561, the applicants who wish to undertake Designated Payment Systems must have the following requirements:

- Be a juristic person
  i. Limited company or public company that is registered in Thailand with the objective to undertake payment systems; or
  ii. Financial Institution, specialised financial institution or state enterprise: or
  iii. Foreign company especially for Payment Card Network only.
- Have paid-up capital at the amount of 50 – 200 million Baht depending on each type of payment service.
- Have a sound financial position and operation status, which represent the capability of undertaking business and providing service with continuity without any risks that may cause damages to service users.
- Must never be temporarily suspended of its entire or partial business operations.
- Must never be sentenced or ordered by the court that its properties shall be forfeiture for the benefits of the state or never been sentenced by the final court judgement on the ground of committing an offence relating money laundering.
- Have directors or persons with managerial power who are not being less than 20-year-old, and qualifying not prohibited under Section 18 and Section 14 of the Payment Systems Act.
- Have at least one director with Thai nationality and domiciled in Thailand.

B. Designated Payment Services

Under the Payment System Act Section 17 and Section 18 and Bank of Thailand Notification no. SorNorChor. 5/2561, the applicants who wish to undertake Designated Payment Services must have the following requirements:

- Be a juristic person
  i. Limited company or public company that is registered in Thailand with the objective to undertake designated payment services; or
  i. Financial Institution, specialised financial institution or state enterprise.
- Have paid-up capital at the amount of 10 – 100 million Baht depending on each type of payment service.
  i. For E-money : 100 million Baht
  ii. For Acquiring : 50 million Baht
  iii. For Payment facilitating : 10 million Baht
  iv. For Accepting e-Payment for and on behalf of others : 10 million Baht
  v. For e-Money transfer service : 10 million Baht

Thailand

- Other requirements are the same as A.
- **Please note that if the applicants have invented or implemented new or advanced technologies, they are required to bring such technologies to be tested in **'Sandbox'** before submitting applications to be licensed or registered.

"Sandbox"

- Financial Technology or FinTech is playing a significant role in the commercial banks as well as non-bank institutions. The technology itself can decrease the business cost and increase the capacity of financial services to the customers. However, technology can cause any risks to financial services, which can affect the financial system of the country.
- Thus, the BOT is the key person to control any risks incurring from the new technology to protect the financial system of Thailand. The BOT has established the specific platform called 'Regulatory Sandbox' allowing such technologies, which will be implemented in financial products, to be tested in a limited environment and under the BOT supervision carefully before the technologies will be released to the public.
- Offering innovative technology through the Sandbox can assure the consumers that the technology has already passed the BOT evaluation and remain under BOT supervision. Hence, critical concerns regarding consumer protection and data security are already emphasised, which will make consumers feel comfortable and less hesitate once trying FinTech products.
- The Sandbox is applied to commercial banks, non-banks under BOT supervision, FinTech companies, and Technology Firms.
- How to apply to the Regulatory Sandbox
  i. Submit an application form.
  ii. Submit a complete set of supporting documents/ information such as
    - Business Model
    - Technologies to be used
    - The Scope of the test (e.g. target group, transaction volume, duration)
    - Innovation Test or Research results
    - Benefits to the service providers, consumers and financial system
    - Consumer Protection Measures
      (Good Corporate Governance, Measures regarding consumers' money and assets, consumer data protection, duties to comply with the laws on anti-money laundering and counter-terrorism and proliferation of weapons of mass destruction financing (AML/CTPF))
- The BOT has emphasised that the technologies to be tested has to be innovative involving new technology not already available in Thailand or which will enhance the efficiency of existing products or services.
- The Duration of the Test should not be more than 1 year. However, the BOT may grant an extension to the test period provided that the applicant applies for an extension not less than 30 days before the expiration date.

- After the Sandbox:
  i. Successful Result
  If the test eventually meets the Key Success Indicator within the duration period, then the applicant can submit an application to be licensed or registered to bring the technology to be implemented for the public.

  ii. Unsuccessful Result
  If the technology fails to meet all Key Success Indicators, the applicant has to stop the service after already notifying to the customers (target group), and then submit the report to the BOT explaining the cessation of the test within 30 days after the stopping date.

In addition, the applicant must provide the exit and transition plan for customers in the Sandbox (target group) as well as the resolution plans, and how the business would run or be terminated if the technology is successful or discontinued.

7. What is the process to become licensed for payments in Thailand?

- An applicant sends a letter or an e-mail requesting an appointment with the BOT to discuss and clarify the business model and other related information.
- The applicant submits the required documents in an electronic format. Once the BOT checks for accuracy and completeness, the BOT will schedule an appointment for the applicant to submit an application along with original supporting documents in person.
- In case the proposed service is innovative or complicated, before submitting an application, the applicant must request an additional appointment with the BOT to discuss the business model and have a consideration on participating in the testing process under the BOT Regulatory Sandbox.
- The applicant satisfying all qualifications required by the law shall submit the application along with supporting documents certified true copy by the authorised signatory through the specified service channels.
- The processing time shall start from the date that the BOT receives and verifies that all submitted documents are correct and complete as specified in this public handbook, and issues an acknowledgement of receipt as evidence.
- The BOT shall notify the applicant of the result of its deliberation within 7 days after the decision is made as per Section 10 of the Licensing Facilitation Act B.E. 2558 (2015).
- To facilitate the application process, the applicant may submit the application and other supporting documents to the BOT for preliminary verification via e-mail: Payment-Sup@bot.or.th.

Thailand

8. What payment services "passporting" arrangements does Thailand have with other countries, if any?

- Since the fees of oversea funds transfer via money transfer agencies is costly, leading commercial banks in Thailand in collaboration with FinTech companies have created innovative methods to transfer money with the aim to mitigate cost and fees to the customers or users in Thailand.
- Recently, Siam Commercial Bank (SCB), one of the leading banks in Thailand, has announced that SCB has partnered with Ripple, the enterprise blockchain solution for global payments, to extend SCB Global Payment strategy launching 'Outward Remittance Service' via SCB Easy application after the BOT sandbox approval. Aiming to deliver convenience, speed, safety 24*7, and zero-fee service to retail-customers when making international transfer payment. As of May 2020, the users can transfer money across 12 countries (e.g. the U.S., the U.K., Singapore, E.U. countries) with 4 currencies (USD, GBP, Euro, and Singapore Dollar).
- While another competitor, Kasikorn Bank has collaborated with FinTech partners using API technology to develop a new feature for oversea funds transfer in 6 currencies (USD, GBP, HKD, SGD, AUD, and Euro) via K Plus application across 24 countries. KBank aims to expand the oversea funds' transfer service across the globe by the end of this year.

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Taiwan.

Payment System under the BOT

A. According to Section 3 of Anti-Money Laundering Act, financial institutions mean:

- Commercial banks under Financial Institutions Businesses Act;
- Designated Payments Systems and Designated Payment Services under the Payment Systems Act;
- e-Money services;
- Card Network Services

Thus, all these services considered as the financial institutions under the AML Law has to establish policies, and procedures in line with the AML laws which include "Know Your Customer (KYC)' Procedures" and "Customer Due Diligence (CDD)".

B. Under the KYC Procedures, the services must establish KYC policies by interviewing and requesting customers identification to rate customer risk exposure. In order to mitigate the risks of financial institutions from being intermediaries for money laundering, the institutions have to develop the guidelines and procedures for operating transactions including electronic transactions with risky customers at least as of the followings:

- KYC standard must be consisting of 1) Identification and 2) Verification and must be compliant with both domestic and international laws regarding Anti-Money Laundering, Combating Financing of Terrorism and Combating Proliferation Financing (AML/CFT/CPF).

Thailand

- The customer identification process is in place to keep track of customers possibly enlisted in AMLO lists, databases of criminal organisations, or high-risk persons specified by FATF (The Financial Action Task Force).
- The risk assessment process has been developed for conducting a financial transaction with new customers.
- The monitoring and accounting management process are adequate and coherent with risk exposure of individual customer groups.

C. Under the CDD procedures, there should be the followings:

- Financial Institutions have classified customers into groups with risk rating assigned to each group for the purpose of developing customer database, which higher-risk customers are required more information than regular customers.
- All factors such as customer history, country of origin, social status, transactional account, transaction types and risk indicator tools must be considered.
- Financial Institutions need to have more extensive due diligence for individuals with a high net worth whose source of funds is unclear, high-risk individual specified by FATF, customers whose addresses are unidentified, or customers who are suspected of being associated with terrorism.
- For high-risk customers, approval for account opening should be taken exclusively at senior management level.

D. Practically, an applicant is required to submit 'Policy and measures for anti-money laundering and counterterrorism and proliferation of weapons of mass destruction financing that meet the minimum regulations as prescribed by the Anti-Money Laundering Office (AMLO) under Anti-Money Laundering Act to the BOT once submitting a request application to the BOT.

F. In March 2020, the BOT also issued another significant Notification regarding the KYC measure applied specifically to e-Money services (e.g. True Money, Rabbit Line-Pay, AirPay, 2C2P Plus) under the Payment Systems Act.

G. Notification no. SorNorChor. 1/2563 will help protect the customers and financial systems from criminal activities, hiding identities to launder dirty money, or using the e-Money platform to support the terrorists. According to the Notification, E-Money services can apply different KYC procedures to the services (products) depending on the risk ratio of each type of product as follows:

- E-money for only domestic payments (not allowed to transfer) = being in accordance with general KYC procedures under the AML Act.
- E-money applicable for payments and transfer to others (both domestically and internationally)
  - i. Face-to-Face measure by requesting for I.D. Smart Card and inspecting whether the identifications match with the customers or not.
  - ii. Non-Face-to-Face measure by using the Biometric Comparison registered in the government system.

F. Risk assessment procedures and other internal risks management such as:

- Have Strict and Applicable policies for Identification and Verification
- Protection and Inspection measures for fraudulent activities such as a limitation of transaction values, monitoring transactions.
- Have an appropriate and updated Data Governance policies, including Data Classification Policy being in line with the risk ratio.

Thailand

10. Describe the technology risk requirements that apply to payment services in Thailand.

The BOT has defined the framework for policies and measures on the security of information technology systems which consist of

- Access control and authentication
- Information confidentiality and system integrity
- Service availability and
- Security audit of information technology systems.

This aims to use them as the guidelines on determination of security measures of information technology systems relating to the highly important payment systems, the designated payment systems and the designated payment services, and to ensure the security measures should cover and prevent from the risk of information technology systems efficiently in compliance with the international standard guidelines (Bank of Thailand Notification No. SorNorChor. 11/2561 Re: Policies and Measures on Security of Information Technology Systems).

11. Describe the data privacy requirements that apply to payment services in Thailand.

Personal Data Protection Act (PDPA)

A. After several legislative attempts, the Thailand Personal Data Protection Act (PDPA) was finally approved by the Thai National Legislative Assembly in February 2019. Following the passage of the bill, the PDPA was published in the Royal Thai Government Gazette and came into effect on May 28, 2019. Initially, the Act was supposed to be fully enforced on 27 May 2020. However, the enforcement of most sections in the PDPA is already postponed by a year (31 May 2021) as a result of the COVID-19. The PDPA was enacted to serve the data protection landscape in Thailand as this was the country's first consolidated law on the subject.

B. The PDPA has the similar concepts as the GDPR, and the PDPA intends to protect data owners (i.e., data subjects under the GDPR) in Thailand from the unauthorised or unlawful collection, use, or disclosure and processing of their personal data. The PDPA applies to organisations outside of Thailand that either offer products and services to individuals in Thailand (regardless of whether any payment is required) or monitor the behaviour of individuals in Thailand. The law is expected to have a significant effect on online service providers based outside of Thailand that hope to continue to serve the Thai market.

C. Thailand's PDPA borrows a number of requirements from the GDPR. For instance, the law establishes a set of lawful bases organisations must use to process data owners' information. Like the GDPR, these lawful bases include consent, legal obligation, public interest, and legitimate interest.

D. If the PDPA had been already enforced since 27 May 2020, Section 19 of the Act would have been applicable for the payment systems in this case.

Thailand

E. Under Section 19, the Data Controller shall not collect, use, or disclose Personal Data, unless the data subject has given consent before or at the time of such collection, use, or disclosure. A request for consent shall be explicitly made in a written statement, or via electronic means. In requesting consent from the data subject, the Personal Data Controller shall inform the purpose of the collection, use, or disclosure of the Personal Data.

F. Unfortunately, the PDPA had not been enforced during the blooming period of payment services in the past, and it is still not enforced at the present while the e-Payment and FinTech industries are glowing.

Regulations of the BOT

A. Therefore, before the PDPA, all payment services, including FinTech companies serving e-Payment services, must follow the rules and regulations issued by the BOT.

B. According to ....., all designated payments systems and designated payment services must follow the BOT measures regarding 'Service User Protection' which describes that 'In order to ensure that payment business providers protect data privacy of service users as well as handle complaints appropriately, business providers shall comply with the following regulations:

(2) Must protect the data privacy of service users by complying with the following requirements:

(2.1) Establish a policy to protect the data privacy of service users, determine the level of confidentiality for data access, and identify persons who have access rights to such information, as well as arrange the data storage system that is accurate and reliable to prevent the unauthorised person from accessing to or modifying the data maintained.

(2.2) Protect service users' confidentiality and data privacy by not disclosing such information during and after the course of services, except for the following cases:

(2.2.1) Disclosure of information upon receiving consent in writing or by any other electronic means which business providers of payment services have agreed upon with the service users.

(2.2.2) Disclosure for the purpose of investigation or trial.

(2.2.3) Disclosure to the auditor of business providers of payment services.

(2.2.4) Disclosure for the purpose of compliance with laws.

(2.2.5) Disclosure for the purpose of oversight of payment systems of the BOT.

Thailand

12. Describe how innovations and inventions are protected by law in Thailand.

- **Innovations and inventions are mainly protected by Intellectual Property (I.P.) law.** I.P. is a legal term that refers to copyright, trademarks and patents. It also includes the protection of undisclosed information/trade secrets. The value of I.P. assets relative to physical assets has increased because of the importance of technology and creative works in the modern economy. I.P. consists of new ideas, original expressions, distinctive names, and appearance that make products unique and valuable. Therefore, innovations, inventions and Financial Technology are always related to I.P. law.
- Logos, pictures, photos, software, designs, systems, etc. are the components of FinTech Business and E-Payment platform, in which case, I.P. is the main component of value in the transaction. I.P. is significant since the things of value that are appeared on the Internet must be protected. The system which allow the Internet to function software, networks, designs are often protected by I.P. rights.
- Traditional financial institutions and startups are both competing and constructively working together to develop FinTech products and services. Companies should define and protect their I.P. with registrations. A company may control use of its I.P. rights, including permitted use under licensing and collaborative arrangements.

Copyright

Computer code, visual interface features, audio, video guides, application programming interface (API) structure and other works can be protected by I.P. rights. Computer code may cover particulars such as source code, pseudo-code, machine code and purpose-built hardware or firmware. Copyright is a significant asset for a FinTech company, particularly if the program design provides computational and usability efficiencies.

Trademarks

Trademarks are an essential part of Fintech business, as branding, customer recognition and goodwill are protected by trademarks and unfair competition law. Trademarks can prevent competitors from unlawfully passing off on or diluting the goodwill of a brand. FinTech companies develop their brands with quality customer service and trust to establish goodwill in their brand with customers and the general public. A strong brand helps FinTech companies differentiate their products and services from competitors.

Patents

Patents provide a mechanism to exclude others from making, using or selling the patented technology, which may help companies obtain or maintain market share, and protect research and development investments. Patents can provide a competitive advantage and may also be used defensively as a negotiation tool. For example, an organisation may protect core innovation in response to assertions of patents by third parties by cross-licensing with another organisation. Patent publications can also be cited against subsequently filed applications to prevent grant. Granted patents may be enforced against third parties that make, use or sell the claimed invention, despite independent development. Obtaining patent protection, however, may be a costly and lengthy endeavour in comparison to other I.P. rights.

Thailand

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

Apart from the positive feedback of the payment services regulated by the BOT, the Securities and Exchange Commission ("SEC") has also supported cryptocurrencies trading. The Emergency Decree on the Digital Asset Business B.E. 2561 ("A.D. 2018") was issued with the aim to regulate the use of digital assets as the fund-raising instruments and medium of exchange. This Emergency Decree also aims to protect the investors by facilitating more precise and adequate disclosure of information for investment decision making, reducing risks of fraud and deception by dishonest people, and preventing the exploitation of digital assets from supporting illegal transactions. According to this Emergency Decree, digital assets can be categorised in two types which are "Cryptocurrency" and "Digital Token".

- Cryptocurrency means an electronic data unit built on an electronic system or network which is created to be a 'medium of exchange' for the acquisition of goods, services, or other rights, including the exchange between digital assets.
- While Digital Token means an electronic data, unit built on an electronic system or network for the purpose of specifying the right of a person to participate in an investment in any project or business.

Even though the SEC states that 'Cryptocurrency' can be a 'medium of exchange' for acquiring goods or services, the BOT does not agree nor disagree on this point. The BOT states that Cryptocurrency is still not a 'legal tender' under the Currency Act and cannot be used as similar to coins or banknotes. However, the BOT does not prohibit people from using Cryptocurrency as the medium of exchange.

Digital Asset Businesses under Royal Decree are categorised into 3 types which are:

- **Digital Asset Exchange**
  A centre or a network established for the purpose of purchasing, selling, or exchanging of digital assets, operates by matching or arranging the counterparty or providing system or facilitating a person who is willing to purchase, sell, or exchange digital assets to be able to enter into an agreement. Ex. BITKUB, Satang Pro.
- **Digital Asset Broker**
  A person who services or holds himself out to the public as available to be a broker or an agent for any person in the purchase, sale or exchange of digital assets to other people in consideration of a commission. Ex. Coins T.H.,
- **Digital Asset Dealer**
  A person who services or hold himself out to the public as available to purchase, sale or exchange of digital assets for his account outside the digital asset exchange. Ex. Coins T.H.

Please note that the SEC does not allow juristic persons registered under foreign laws to undertake any type of Digital Asset Business in Thailand. There must be only juristic persons registered under Thai laws.

Digital Assets and Anti-Money Laundering

In order to prevent the exploitation of digital assets as the channel for money laundering, Digital Asset Businesses are regarded as 'Financial Institutions' according to Section 7 of the AML Act; thus, all types of digital assets businesses are legally required to follow the legal obligations under the Act.

Thailand

Emergency Decree on Digital Assets also imposes that the issuers of Digital Tokens who are willing to accept Cryptocurrencies in the offering process or the operators of digital asset businesses who are willing to accept Cryptocurrencies from the counterparties in any transaction will only accept Cryptocurrencies obtained from or deposited with operators of digital asset businesses regulated under the Royal Decree. The rationale is to preserve the integrity of markets by ensuring that cryptocurrencies being transacted come from traceable sources.

Digital Assets Tax

The Royal Decree on Amendment to the Revenue Code (No. 19) ("Royal Decree No. 19"), B.E. 2561 ("A.D. 2018") was published on 13 May 2018 in the Government Gazette, and became effective on 14 May 2018.

- Under Section 3 of the Royal Decree, it adds only 2 sub-categories of assessable income under Section 40 (4) of the Revenue Code. The additional types of income will be as follows:
  i. The share of profits or any benefits of a similar nature derived from holding or possessing digital tokens (Section 40 (4) (g)); and
  ii. The benefit derived from the transfer of cryptocurrency or digital tokens which exceeds the cost of the investment (Section 40 (4) (h)).
- In addition, Section 4 of the Royal Decree states that the payment of assessable income under Section 40 (4) (g) and (h), is subject to 15% withholding tax.

This withholding tax requirement is added to Section 50 of the Revenue Code (Section 50 (2) (f)). The 15% withholding tax applies to both resident and non-resident companies.

14. Other Tax Matters related to e- Payment Services

A. The Revenue Code Amendment Act No. 48, B.E. 2562 (2019) (the "**Revenue Code**"), commonly known as e-payment law. The law became effective on 21 March 2019.

B. The amendments to the Revenue Code include:

Section 3/17: Reporting Obligations to the Revenue Department

- After the Revenue Code becomes effective, financial institutions, state financial institutions, and e-money service providers are obliged to make reports of specific transactions which are in their possession to the Revenue Department by the end of March every year.
- The transactions of their clients that are required to be reported to the Revenue Department are:
  i. 3,000 deposits or receipts of money transfer or more; or
  ii. At least 400 deposits or receipts of money transfer or more that are worth at least 2 million Baht.
- An entity having such reporting obligations is required to submit the first report to the Revenue Department by 31 March 2020. If the entity fails to comply with the reporting obligations, the entity will encounter a maximum administrative fine of 100,000 Baht and fine of 10,000 Baht per day until the entity fulfil the reporting obligations.

C. The new tax measures create a huge impact on online shops or e-commerce players as their cash flow can easily tracked by the Revenue Department, and the e-Commerce tax will add up to the cost of businesses.

Vietnam

1. What is the payments landscape in Vietnam:
The types of activities, state of development of the market and new trends eg FinTech if any?

Payment activities in Vietnam are classified into two main types: payment in cash (including COD - cash on delivery) and non-cash payment (including payment by bank cards, QR code, internet banking, mobile banking, SMS banking and e-wallet provided that customers have their bank accounts).

Vietnam is a promising market for payment services in general and electronic payment services in particular. The increase in young population (around 40% of 97 million people is under 24 years old), high usage of electronic devices (including laptops and smartphones), rise of e-commerce(online shopping)and the State's encouragement of policies on non-cash payment following global 4.0 industrial revolution have greatly contributed to the development of payment as well as Fintech market in Vietnam.

In recent years, Vietnam market has witnessed the strong growth in non-cash payment services. By the end of March 2019, the number of financial transactions via the internet increased by about 66%, the value of transactions increased by about 14% compared with the same period in 2018 whilst the number of financial transactions via mobile phones increased by about 98% and the value of transactions increased by about 232.3% compared with the same period in 2018[51].

Number of Fintech companies in Vietnam has increased from about 40 (in 2016) to 154 (in 2019) and Vietnam's Fintech industry reached US$4.4 billion in 2017 in transaction value and is expected to reach US$7.8 billion in revenue by 2020[52].

2. Which official agency regulates payments in Vietnam?

The State Bank of Vietnam ("**SBV**") is the regulatory authority responsible for managing all monetary, banking and payment activities in Vietnam.

The SBV acts as both the Central bank and a Government agency of Vietnam. Its operations aim at stabilizing the value of Vietnamese currency, ensuring safe and sound banking operations and the system of credit institutions, ensuring safety and efficiency of the national payment system, and contributing to socio–economic development under the socialist orientation.

With respect to payment activities, the SBV has the authority to issue and/or submit to the competent authority (such as the National Assembly, the Government and the Prime Minister) to issue relevant legal instruments, to supervise the operation of payment systems within the country, to issue or revoke license for payment services and to inspect and handle violations of laws on payments committed by organizations and individuals.

With respect to electronic payment services, in 2017, the SBV specially established the Steering Committee on Financial Technology. This Committee has the authority to make annual plans to develop Fintech, connect the Government and Fintech companies and propose policies to support Fintech companies.

In addition to the SBV, the Ministry of Information and Telecommunication ("**MOIT**") also has certain authority in electronic payment services since electronic payment services involve significant demands on IT, electronic technology, telecommunications and electronic information.

[51] According to the statistics of the Department on Payment of the State Bank of Vietnam
[52] According to the survey conducted by Institution for development and research in banking technology at Vietnam National University of Ho Chi Minh City (VNUHCM-IBT)

Vietnam

3. What are the main sources of laws regulating payments services in Vietnam?

Vietnam is a civil law jurisdiction and is State governed. It is therefore based on the written laws. Payment services are consequently stipulated and governed in different legal instruments. The principal governing legal instrument is the Civil Code No. 91/2015/QH13 dated 24 November 2015 issued by the National Assembly ("**Civil Code**"). It is one of the most important sources of laws in Vietnam to regulate principles on civil transactions including payment transactions.

The provisions on payment services in Vietnam can also be found in specialized laws, decrees, circulars and decisions issued by competent State agencies, such as Law on Credit Institutions No. 47/2010/QH12 dated 16 June 2010, as amended ("**Law on Credit Institutions**") issued by the National Assembly which regulates the operation of the credit institutions in Vietnam, including payment activities via bank accounts, Decree No. 101/2012/ND-CP dated 22 November 2012 on non-cash payment, as amended ("**Decree 101**") issued by the Government which specifies requirements and operation of payment accounts, and Circular No. 39/2014/TT-NHNN dated 11 December 2014 on intermediary payment services, as amended ("**Circular 39**") which provides for the types, conditions and operation of intermediary payment services.

Recently, the Prime Minister of Vietnam issued Decision No. 283/QD-TTg dated 19 February 2020 on Scheme on restructuring of the service sector to 2020, orientation towards 2025, which set out major tasks for the banking and finance sector, including promoting the application of digital technology, enhancing innovation in the design and distribution of banking products and services, providing a pilot management mechanism for the development of financial technology services in the banking sector, building a regulatory sandbox for financial and banking services based on information technology such as e-wallets, electronic identifiers, peer-to-peer lending, and crowdfunding on the internet.

4. Describe the regulatory framework(s) for payment services operating in Vietnam, and the type of payment services that are regulated.

Payment services in Vietnam may be classified as follows[53]:

A. Payment services via payment accounts include
- provision of payment facilities; and
- provision of payment services for cheques, payment orders, authorized payment orders, collection orders, authorized collection orders, bankcards, letters of credit, monetary remittance, and receipts and disbursements on behalf of others.

Payment services via payment accounts will be carried out via licensed banks in Vietnam.

B. Payment services not via payment accounts consist of money transfer, receipts and disbursements on behalf of others.

Payment services not via payment accounts can be carried out by licensed banks, people's credit funds, microfinance institutions and other permitted organizations.

[53] Articles 14 and 15.1 of Decree 101; Article 2 of Circular 39

Vietnam

The intermediary payment services ("**IPS**") providers have contributed towards the success of payment services provided by banks with the following services:

- Payment support services, which include e-wallet (i.e. provision to customers with e-wallets with which they can top up, and make payments for online/offline products/services), collection and payment support services, support services for electronic money transfer; and
- E-payment infrastructure services covering financial switch, electronic clearing and payment gateway.

5. How does Vietnam's payments licensing laws apply to cross-border business into your jurisdiction?

Cross border payment from foreign countries to Vietnam and vice versa will generally be conducted via bank account systems (with support from IPS providers, particularly the financial switch providers). Vietnam has not issued specific regulations on cross border payments, save for regulations on foreign exchange control which stipulates conditions and permitted purposes of cross border money transfers.

The inflow of foreign currency must be transferred into foreign currency denominated bank accounts established at a licensed credit institution in Vietnam or sold to licensed credit institutions.

The outflow of foreign currency by transfer is only authorised for certain specific purposes. For example, for purposes of donation, aid or others; payments for imports and services abroad; repayment of foreign loan and interests; transfers of profits and dividends in case of organizations, and payment for overseas study and medical healthcare; travel; service fees or price abroad; inheritance and other legal demands in case of individuals[54].

6. What are the main requirements to be licensed for payments in Vietnam?

A. For payments services provided by banks

Payment service is one of banking activities provided by banks. Banks are required to obtain the License for establishment and operation of bank ("**Banking License**") to provide such banking activities, including payment service in Vietnam. Main requirements for obtaining Banking License include[55]:

- Having minimum charter capital of VND3,000 billion (around USD145 million) for establishment of bank and USD15 million for branch of a foreign bank;
- Having managers, executives and controlling board members who fully meet the criteria and conditions under the laws (such as years of experience and diplomas in related sectors); and
- Having an establishment plan and a feasible business plan which neither affects the safety and stability of the credit institution system nor creates monopoly or restricts competition or creates unfair competition within the credit institution system.

[54] Decree No. 70/2014/ND-CP dated 17 July 2014 detailing the implementation of several provisions of the Ordinance on Foreign Exchange Control
[55] Article 20 of the Law on Credit Institutions

Additionally for foreign owned banks:

- The foreign credit institution's operations are healthy and meet requirements on total assets, financial status and safety ratios under the SBV's regulations;
- The operations to be conducted by the foreign owned bank in Vietnam are those the foreign credit institution is licensed to conduct in its home country;
- The foreign credit institution issues written commitments to provide support in finance, technology, governance, administration and operation of the foreign owned bank; and
- The competent authority of the home country has signed an agreement with the SBV on inspection and oversight of banking operations and exchange of information on banking safety oversight and made a written commitment on consolidated oversight of the foreign credit institution's operations according international practices.

B. For IPS provided by IPS providers

An IPS provider is required to obtain a License for providing IPS in Vietnam ("**IPS License**"). Accordingly, IPS provider must satisfy the following key requirements[56]:

- Having minimum charter capital of VND50 billion (around USD2,100,000);
- Having a plan for provision of IPS which is approved by its competent body and contain, inter alia, the technical operation process of the proposed services, the mechanism for ensuring the solvency, the process of internal inspection and control, risk management, security and confidentiality protection, general rules and internal regulations on anti-money laundering, procedures for solving trace requests, complaints and denunciations;
- Meeting technical requirements such as having proper facilities, technical infrastructure, IT systems, technology solutions and independent back-up technology systems; and
- Having personnel who fully meet the requirements of laws.

In addition to the above, Decree 101 also stipulates specific requirements for some types of IPS as follows:

- For financial switching and electronic clearing services, the IPS provider must engage a third party to finalize the payment results between relevant parties; and
- For payment support services provided to customers holding accounts in multiple banks, the IPS provider must associate with a licensed financial switching and clearing services provider.

[56] Article 15.2 of Decree 101

Vietnam

7. What is the process to become licensed for payments in Vietnam?

A. For Banking License

Procedures for setting up banks (i.e. obtaining the Banking License) in Vietnam are generally as follows:

- Investor(s) (including foreign credit institution in case of setting up the foreign owned bank) to submit the application files to the SBV;
- Timeline for issuance of the Banking License is about six months from receipt of the proper application files as required by the SBV[57]. It usually takes longer and is more complicated in practice. The term of the Banking License shall not exceed ninety nine (99) years[58];
- After obtaining the Banking License, the newly established bank will submit application files for obtaining the Enterprise registration certificate ("**ERC**") at Department of Planning and Investment ("**DPI**"); and
- The bank will have to notify its establishment on newspaper at least 30 days before commencing operations.

B. For IPS License

Procedures for setting up IPS provider (i.e. obtaining the IPS License) in Vietnam are generally as follows:

- Before obtaining the IPS License, investor(s) shall submit dossier to DPI for obtaining the Investment Registration Certificate ("**IRC**") (required for foreign owned IPS provider) and the ERC to set up new company engaging in IPS;
- The newly established company shall submit the application files to the SBV for obtaining the IPS License. The application files generally include the incorporation certificate, the regulatory application forms, the plan for provision of IPS and the internal approval on the same, description of technical solution and records on the required personnel;
- The SBV shall thereafter examine, appraise and issue the IPS License or the written refusal to issue the IPS License within 60 days from receipt of the proper application files[59]. It takes longer and is more complicated in practice since the SBV will require the IPS provider to run a trial to evaluate the sufficiency of the IPS provider's operation system; and
- The term of the IPS License is ten (10) years from the date of issuance and can be renewed upon its expiry[60].

8. What payment services "passporting" arrangements does Vietnam have with other countries, if any?

RHTVN:

Save for the WTO Commitments and other treaties on free trade, Vietnam has not entered into any specific arrangements on payment services with other countries which allows service providers of a country party to provide their services across the agreed countries with 'single licence'.

[59] Article 16.1 and 16.2 of Decree 101
[60] Article 16.3 and of 16.5 Decree 101

Vietnam

9. Describe the anti-money laundering (AML) and other financial crime requirements that apply to payment services in Vietnam.

Growth of payment services has created opportunities for money laundering crimes. Therefore, combating money laundering is also a priority of the State of Vietnam in managing payment services in Vietnam.

The SBV is the primary regulator and supervising authority on implementation of laws on AML in Vietnam and the main regulations on AML is Law No. 07/2012/QH13 dated 18 June 2012 on Prevention of and Combating Money Laundering ("**Law on AML**")and its guiding regulations.

In principle, the banks and IPS providers must apply appropriate measures to identify their clients (i.e. Know Your Customer policies) and report to the State authority of any high value transactions, suspicious transactions and transactions of electronic money transfer exceeding the prescribed amounts[61].

Money laundering is a prohibited act and classified as a crime under the Criminal Code No. 100/2015/QH13 dated 27 November 2015, as amended ("**Criminal Code**") which includes:

- Directly or indirectly participating in financial/banking transactions or others to conceal the illegal origin of the money or property obtained through his/her commission of a crime or obtained through another person's commission of a crime to his/her knowledge;
- Using money or property obtained through his/her commission of a crime or obtained through another person's commission of a crime to his/her knowledge for doing business or other activities;
- Concealing information about the true origin, nature, location, movement or ownership of money or property obtained through his/her or commission of a crime or obtained through another person's commission of a crime to his/her knowledge or obstructing the verification of such information; and
- Committing any of the offences specified in above Point in the knowledge that the money or property is obtained through transfer, conversion of money or property obtained through another person's commission of a crime.

Those found in breach will be subject to fines, imprisonment from one to 15 years depending on the severity of the infringement and confiscation of assets.

Other than money laundering, obtaining property/assets by fraud; production, possession, transport, circulation of counterfeit money/other valuable papers or appropriation of property by using computer network, telecommunications network or electronic device are also crimes and subject to various penalties.

[61] Articles 21, 22 and 23 of the Law on AML

Vietnam

10. Describe the technology risk requirements that apply to payment services in Vietnam.

In order to effectively manage risks arising from payment services, banks and IPS providers are required to[62]:

- Identify risks;
- Analyse and identify the impacts and consequences that may arise when risks occur;
- Categorize the risks;
- Identify directions and measures to prevent risks, and pay attention to network security management and information protection;
- Determine the maximum acceptable loss in the event of a risk;
- Not deploy types of electronic banking activities which require risk prevention measures beyond the existing capability;
- Regularly assess and check the results and effectiveness of risk management work; and
- Audit and update risk management process.

In addition, banks and IPS providers must further keep confidential and ensure the integrity and accuracy of information and data in e-payment activities with customers. They must ensure that the customers will be provided with correct and necessary information before execution of any transactions.

In case of cooperating with third parties, they must also evaluate the technical competence and financial capacity of such third parties, clearly specify duties, powers and obligations of relevant parties in the cooperation and supervise and oversee the provision of services by third parties[63].

11. Describe the data privacy requirements that apply to payment services in Vietnam.

Data privacy and protection is one of the most important issue concerned by the service providers as well as their customers during the payment process. The legal basis of data protection is a variety of laws. Principles of collection, storage, processing, use and disclosure of personal data are provided in the Civil Code and other specialized laws (such as Law on Network Information Security, Law No. 51/2005/QH11 on Electronic Transactions dated 29 November 2005, Law No. 24/2018/QH14 on Cybersecurity dated 12 June 2018).

The data processor (such as banks and IPS providers) must comply with the following requirements[64]:

- Obtain the consent of the data subject (i.e. person who are identified or identifiable from personal data);
- Use the collected personal information for other purposes after further obtaining the consent of the data subject; and
- Refrain from providing, sharing or disclosing to third party personal data which they collected, accessed or controlled, unless obtaining the consent of the data subjects.

In addition, the data processor must publish its policy regarding the processing and protection of personal data and provide an adequate level of protection for personal data, and following the technical standards for protection of personal data[65].

---

[62] Article 5 of Decision 35/2006/QD-NHNN dated 31 July 2006 providing regulations on risk management principles for e-banking activities ("**Decision 35**") and Article 7.1 of Circular 39

[63] Articles 11 and 13 of Decision 35

[64] Article 17 of Law No. 86/2015/QH13 on Network Information Security dated 19 November 2015, as amended ("**Law on Network Information Security**")

[65] Articles 16.3 and 19.2 of Law on Network Information Security

There are two exemptions from the data protection rules, including processing of data carried out by the competent authority or as per request of competent authority and processing of data for the purpose of ensuring national defence and security, maintaining social order and safety or for non-commercial purposes[66].

Infringement of data protection regulations (such as infringement upon secret information, mail, telephone, telegraph privacy or other means of private information exchange; illegal provision or use of information on computer networks or telecommunications networks) will be subject to administrative fines or criminal penalties depending on consequences and severity of such infringement.

12. Describe how innovations and inventions are protected by law in Vietnam.

By joining the World Trade Organization (WTO) in January 2007, Vietnam has officially committed to fulfil all intellectual property obligations under the Agreement On Trade-Related Aspects of Intellectual Property Rights (TRIPS) which requires WTO members to provide strong protection for intellectual property rights.

Vietnam has enacted local legal instruments to effectively recognize and protect intellectual properties rights, including Civil Code, Law No. 50/2005/QH11 dated 29 November 2005 on intellectual property, as amended ("**Law on IP**"), Criminal Code and other guiding and implementation regulations.

Whilst the Civil Code principally recognizes intellectual property rights, the Law on IP details regulations on copyrights, related rights to copyrights, industrial property rights (inventions, industrial designs, semi-conductor integrated circuit layout designs, trademarks, trade names, geographical indications, business secrets created or owned by them, and the right to fight unfair competition), rights to plant varieties, and the protection of those rights.

Under the Law on IP, innovations and inventions are a kind of industrial property right. Innovations and inventions will be protected in the form of invention patent or utility solution patent if the conditions prescribed by law are met. Protection titles are valid throughout the territory of Vietnam. Protection title for an invention patent will be valid from the date of issuance and last until the end of twenty years from the date of filing, whilst it is only ten years for the utility solution patent[67].

Violation of intellectual property rights will be subject to administrative fines or penalties as provided in the Criminal Code depending on the severity level of the violation.

The aforementioned laws, as well as their amendments and supplements, have gradually improved Vietnam's legal system on intellectual property in a harmonized manner and have met international standards prescribed in the TRIPS Agreement of which Vietnam is a member.

[66] Articles 16.5 and 17.1(c) of Law on Network Information Security
[67] Articles 58 and 93 of the Law on IP

Vietnam

13. Is the trading of cryptocurrencies permissible in your country? What is the legal regime that governs cryptocurrencies?

"The issuance, distribution and use of Cryptocurrencies are illegal in Vietnam. This is expressly confirmed by the State Bank of Vietnam in Official Letter No. 5747/NHNN-PC dated 21 July 2017. The use of cryptocurrencies in Vietnam will attract both administrative[1] and criminal[2] sanctions.

The only non-cash payments acceptable for use in Vietnam include cheques, payment orders, collection orders, bank cards, and other payment instruments as prescribed by the State Bank of Vietnam[3].

Given the booming growth of cryptocurrencies all over the world, the Prime Minister of Vietnam adopted Decision 1255/QD-TTg dated 21 August 2017 initiating the research and establishment of a new regulatory framework for cryptocurrencies. This will hopefully pave the way for the recognition of cryptocurrencies in the near future."

Notes:

[1] of up to VND200 million (approximately USD8,600)

[2] imprisonment from 6 to 36 months

[3] pursuant to Decree No. 101/2012/ND-CP dated 22 November 2012 on non-cash payment (as amended by Decree 80/2016/ND-CP dated 1 July 2016)

Authors

William Khong
Partner
William.Khong@holdingredlich.com
Australia

Chowdhury Tanzim Karim
Managing Partner
karim@ctkpartners.com
Bangladesh

Vannak Houn
Managing Partner
vannak.houn@rhtlawcambodia.com
Cambodia

Henry Huang
Managing Partner
huangningning@grandall.com.cn
China

Nicole Jiang
Lawyer
jiangyuanxiu@grandall.com.cn
China

Anant Merathia
Managing Partner
anant@merathiacorp.com
India

Genio Atyanto
Partner
atyanto@nacounsels.com
Indonesia

Mohanthas Narayanasamy
Partner
mohansamy@pcalaw.com.my
Malaysia

Franchette M. Acosta
Senior Partner
fm.acosta@thefirmva.com
Philippines

Imperial, Paul Rodulfo B.
Partner
pb.imperial@thefirmva.com
Philippines

Ch'ng Li-Ling
Head, Financial Services (Regulatory) Practice
li-ling.chng@rhtlawasia.com
Singapore

Aaron Lee
Of Counsel, Financial Services (Regulatory) Practice
aaron.lee@rhtlawasia.com
Singapore

Timothy Dickens
Senior Foreign Attorney
tjldickens@draju.com
South Korea

Eddie Hsiung
Associate Partner
eddiehsiung@leeandli.com
Taiwan

Picharn Sukparangsee
Managing Partner
picharn@bgloballaw.com
Thailand

Benjamin Yap
Senior Partner
benjamin.yap@rhtlaw.com.vn
Vietnam

Mai Thi Ngoc Anh
Partner
anh.mai@rhtlaw.com.vn
Vietnam