FINTECH AND CYBERSECURITY: LEGAL FRAMEWORKS AND EMERGING REGULATORY TRENDS IN MALAYSIA

The efficiency and accessibility of new and evolving technology has transformed our management of finances and data. This transformation has brought with it new challenges, particularly in regulating the fast-growing sectors of Fintech and Cybersecurity. Strong legal frameworks are imperative to ensure the safety of financial and personal information while cultivating innovation.

Financial technology ("**Fintech**") merges cutting-edge technology with financial services to drive innovation and accessibility. By leveraging solutions like mobile banking, digital wallets, crowdfunding, and cryptocurrencies, Fintech continues to challenge traditional financial systems, offering transformative ways for individuals and businesses to engage with financial services.

Cybersecurity encompasses the practices, technologies, and policies designed to safeguard systems, data, and financial assets against threats such as malware, phishing scams, and data breaches. It plays a critical role in ensuring the resilience and integrity of Fintech platforms and the broader digital ecosystem.

This article outlines the existing framework and legislation in Malaysia, along with anticipated changes that could potentially arise in the future, for both Fintech and Cybersecurity.

FINTECH

Existing Framework

In Malaysia, Fintech activities involving banking, investment banking, insurance or takaful, money changing, remittance, payment systems, and issuance of payment instruments are regulated by the Central Bank of Malaysia (Bank Negara Malaysia) ("**BNM**"). Currently, Malaysia does not have a specific regulatory regime applicable to Fintech participants, and the existing regulatory framework that applies to the traditional financial services industry also applies to Fintech participants. The framework includes legislation such as:

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my |T: +603 2201 5584

1. **Financial Services Act 2013 (FSA)**

    - Contains provisions on prudent business conduct, consumer protection, anti-money laundering, and safeguards against the financing of terrorism.

    - Regulates conventional financial institutions, payment systems, and operators.

    - Provides oversight of the money market and foreign exchange market.

2. **Islamic Financial Services Act 2013 (IFSA)**

    - Regulates the Islamic financial sector, including Islamic banking and insurance

    - Addresses the application of Shariah principles in financial transactions.

3. **Capital Markets and Services Act 2007 (CMSA)**

    - Governs the regulation of activities in the capital markets, such as stockbroking, provision of investment advice, financial planning, dealing in derivatives, and advising on corporate finance.

    - The Securities Commission of Malaysia ("**SC**") is primarily responsible for enforcing the CMSA and oversees the regulation of digital assets, such as cryptocurrencies and security token offerings (STOs), whereas BNM primarily regulates the financial services sector with jurisdiction over activities related to digital banking, electronic payments, and Fintech.

    - Capital Markets & Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019:

        - The SC has established a framework for the digital assets industry through the Capital Markets & Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 ("**Prescription Orde**r"), enabling it to implement guidelines to regulate the offering and trading of digital assets.

- Following the issuance of the Prescription Order, the SC has also introduced several guidelines to regulate players in the digital asset ecosystem, including the Guidelines on Recognized Market Operators and the Guidelines on Digital Assets.

4. **Money Services Business Act 2011 (MSBA)**

   - Regulates money changing and remittance businesses in Malaysia.

   - Enhances compliance measures to prevent illicit financial activities within money service businesses.

Recent Updates

On 29 February 2024, BNM issued and announced the Financial Technology Regulatory Sandbox Framework ("**Policy Document**") to drive Fintech innovation.

The Policy Document supersedes the version issued on 18 October 2016 by introducing two key enhancements:

1. Simplifying the Stage 1 eligibility assessment criteria of the Standard Sandbox pathway to ensure that the rigor of assessment is proportionate and better aligned with the development cycle of new innovations.

2. Introducing a risk-proportionate accelerated track (namely "**Green Lane**"), which facilitates faster testing of innovative solutions by granting regulatory flexibility to financial institutions with a strong track record in risk management, governance, and compliance capabilities.

It is worth noting that Fintech companies may have concerns about the introduction of the Green Lane. Under the previous Sandbox regime, Fintech startups could participate on their own to test and launch new products and services. However, with the introduction of the Green Lane, their ability to do so is now limited. While they are permitted to collaborate with financial institutions on sandbox projects, such collaborations are subject to BNM's approval. This restriction may pose challenges for smaller and emerging Fintech startups, potentially slowing down their ability to test and deploy innovative solutions in view of the requirement for regulatory approval over such collaborations.

Anticipated Changes

The Fintech industry is evolving with rapid transformations and significant market fluctuations. In recent years, the landscape has been especially volatile, particularly after the COVID-19 pandemic, with the rise of neobanks and the emergence of digital assets such as cryptocurrencies and NFTs accelerating the reshaping of the financial sector.

Following the enactment of the Cyber Security Act 2024 (described further below), various sectors under the Fintech umbrella have been classified as National Critical Information Infrastructure ("**NCII**"), requiring enhanced cybersecurity diligence and regulatory compliance.

As online transactions between individuals or businesses continue to increase, the demand for robust security measures by NCII involved in Fintech will only intensify. Technologies such as blockchain, artificial intelligence (AI), and big data will not only play a critical role in securing transactions and detecting fraudulent activities but also act as vital components in bolstering cybersecurity defences.

Financial service providers must therefore navigate a complex regulatory landscape while implementing strong security protocols that align with broader cybersecurity frameworks. An increase in regulatory support is anticipated to address key challenges such as enhancing data protection measures, mitigating fraud risks, and ensuring compliance with international cybersecurity standards.

CYBERSECURITY

Existing Framework

Hacking incidents have become increasingly common worldwide. As technology continues to integrate into society, such integration significantly enhances efficiency but also introduces new risks that need to be managed with agility and under a strong governance framework.

Prior to the introduction of the Cyber Security Act 2024 ("**CSA 2024**"), legislation that addressed the growing challenges of cybersecurity included:

1. **Computer Crimes Act 1997** – Prohibits activities such as hacking, the distribution of computer viruses, and the unauthorized sharing of access credentials to a computer.

2. **Communications and Multimedia Act 1998** - Governs the operations of license holders, including network facilities providers, network service providers, application service providers, and content application service providers, as well as individuals who make use of the services they offer.

3. **Personal Data Protection Act 2010** - Governs the handling of personal data in commercial transactions.

4. **Penal Code** - Although the Penal Code does not specifically address cybercrime, its provisions can still be broadly applied to various offenses in the digital realm. These include acts such as data theft, unauthorized access, dishonest use of digital assets, receiving stolen digital property, and online fraud. By leveraging existing legal frameworks, Malaysia has the capacity to address certain aspects of cybercrime even as it develops more targeted cybersecurity regulations.

Recent Updates

On 26 August 2024, the CSA 2024 came into force, which:

1. Establishes the National Cyber Security Committee ("**Committee**"), chaired by the Prime Minister, to oversee cybersecurity policies.

2. Empowers the National Cyber Security Agency ("**NACSA**") with regulatory and enforcement responsibilities related to cybersecurity matters. The Chief Executive of NACSA is tasked with advising the Committee and implementing cybersecurity policies, with the authority to order enforcement actions and investigations.

3. Identifies specific sectors as NCII, including Government; Banking and Finance; Transportation; Defence and National Security; Information; Communication and Digital; Healthcare Services; Water, Sewerage and Waste Management; Energy; Agriculture and Plantation; Trade, Industry and Economy; and Science, Technology and Innovation.

4. Obligates NCII Sector Leads to regulate entities which fall under the identified NCII sectors ("**NCII Entities**"). These Sector Leads are tasked to prepare sector-specific codes of practice and implement decisions made by the Committee.

5. Imposes various obligations on NCII Entities concerning cybersecurity matters.

6. Stipulates that violations of the CSA 2024 could result in criminal penalties, including fines, imprisonment, or both.

7. Has extraterritorial application, extending the CSA 2024 to offences affecting NCII Entities, either wholly or partly, in Malaysia.

8. Mandates that cybersecurity service providers must be properly licensed, with penalties for failure to obtain the required licenses.

In conjunction with the implementation of the CSA 2024, four subsidiary regulations were introduced:

1. **Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024 [P.U. (A) 219/2024]** - NCII Entities are now required to conduct a risk assessment at least once a year and undergo an audit every two years to ensure ongoing cybersecurity resilience.

2. **Cyber Security (Notification of Cyber Security Incident) Regulations 2024 [P.U. (A) 220/2024]** - NCII Entities must notify the relevant authorities of any cybersecurity incident within six hours of becoming aware of it. Additionally, within 14 days of the initial notification, they are required to provide detailed supplementary information, including actions taken to mitigate the incident.

3. **Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024 [P.U. (A) 221/2024]** - Clarified the licensing requirements for cybersecurity service providers, ensuring that all providers operate under a recognized and regulated framework.

4. **Cyber Security (Compounding of Offenses) Regulations 2024 [P.U. (A) 222/2024]** - Specific offences have been identified as compoundable offenses, offering flexibility in enforcement.

Anticipated Changes

The CSA 2024 imposes specific obligations on NCII Entities, making it imperative for them to develop strategic plans to ensure compliance with these requirements. Although codes of practice for the NCII Entities have yet to be developed,

their introduction is anticipated in the near future. While non-NCII entities are not directly bound by the CSA 2024, aligning with its principles and adhering to relevant codes of practice can significantly enhance their cybersecurity posture and protect against cybercrime.

In fact, neighbouring Singapore recently amended its Cybersecurity Act 2018, extending regulations to cover virtual critical information infrastructure, in addition to physical computers and systems. This change reflects the evolving nature of IT systems, which are increasingly cloud-based rather than confined to physical premises. Malaysia is expected to potentially follow suit and adopt similar changes in the future.

CONCLUSION

As Fintech and cybersecurity continue to evolve, strong legal frameworks and regulations are critical to address emerging challenges. The CSA 2024 and updates to the Financial Technology Regulatory Sandbox demonstrate Malaysia's commitment to securing its digital landscape.

While Fintech innovation drives growth, a strong cybersecurity foundation is key to a secure and thriving digital economy. All sectors must assume responsibility through constant attention and teamwork. By balancing innovation with regulation, Malaysia is poised to lead in creating a secure, resilient digital economy that can handle future challenges and foster trust and success globally.