

## CATCHING THE FINTECH WAVE IN ISLAMIC FINANCE: REGULATORY APPROACH FOR MALAYSIA

Surianom Miskam  
Department of Law  
Faculty of Shariah and Law  
Kolej Universiti Islam Antarabangsa Selangor (KUIS)  
[surianom@kuis.edu.my](mailto:surianom@kuis.edu.my)

Farah Mohd Shahwahid  
Department of Law  
Faculty of Shariah and Law  
Kolej Universiti Islam Antarabangsa Selangor (KUIS)  
[farahms@kuis.edu.my](mailto:farahms@kuis.edu.my)

Nawal binti Sholehuddin  
Department of Law  
Faculty of Shariah and Law  
Kolej Universiti Islam Antarabangsa Selangor (KUIS)  
[nawal@kuis.edu.my](mailto:nawal@kuis.edu.my)

### Abstract

*Financial technology or FinTech is a new wave of technological innovations taking place in the financial service sector around the globe including Islamic finance. From artificial intelligence to cryptocurrency, rapid advances in FinTech are transforming the financial services landscape, creating both opportunities and challenges for consumers, service providers, and regulators alike. Development in FinTech raises questions as to what impact might technology have on the financial sector, and how should regulation respond to address the challenges posed by FinTech. Legal issues and challenges posed by FinTech are identified and discussed to provide an insight into the legal and regulatory aspects of FinTech application. This paper further examines the regulatory approach taken by the Bank Negara Malaysia in response to rapid advances introduced by FinTech. Being a legal research, this paper employs a qualitative method which is mainly library research by analysing the relevant literatures on the subject and data from journal articles, websites and official reports of the regulators.*

**Keywords:** FinTech, Legal, Regulatory, Islamic finance, regulations

### 1.0 Introduction

Financial Technology or FinTech is a phenomenon that has been accelerating the pace of change at the intersection of finance and technology at a remarkable rate (PwC, 2017). FinTech is taking place in the financial services industry around the globe including Islamic finance. FinTech have now become an essential part of financial service industry and banking institutions have begun to compete beyond financial services facing increasing competition from non-bank financial institutions. Recently, start-up service providers, search engines and social networks have started expanding their services in banking business such as providing payment services via mobile payments and virtual currencies, alternative financing opportunities as peer-to-peer lending and crowd funding, as well as wealth management etc. (Románova & Kudinska, 2016).

Development in FinTech raises questions as to what impact might technology have on the financial sector, and how should regulation respond to address the challenges posed by

FinTech. One of the findings from the Global FinTech Report in 2017 is that legislation is not keeping pace with innovation, creating significant uncertainty. This means that a more adaptable structure in policy making that minimises bureaucratic hurdles could be advantageous under the current dynamic environment to encourage potentially important innovations (PricewaterhouseCoopers, 2017). Regulatory framework for the operation of FinTech should be in place to address issues of consumer protection, market conduct and technological impact to ensure the orderly functioning of financial markets (Laldin, 2018). Despite continuous exploration of a global supervisory and regulatory framework, there are still many discrepancies in terms of policy, guidelines and enforcement among jurisdictions in dealing with FinTech (Artie W. Ng, 2017). As such this study provides an insight into the legal and regulatory aspect of FinTech in Malaysian perspective. The discussion focuses on the regulatory approach taken by the regulator in dealing with the FinTech wave.

Based on this background, this paper aims to provide an overview of the emerging FinTech innovations and its evolution in the Islamic finance industry in Malaysia. Being a legal research, this paper adopts a qualitative method which is mainly library research by analysing the relevant literatures on the subject and data from journal articles, websites and official reports of the regulators. This paper is structured as follows: Section 2 defines FinTech and its evolution in Islamic finance industry. Section 3 identifies and discusses the legal issues and challenges posed by FinTech while section 4 examines the regulatory approach taken by BNM in response to rapid advances introduced by FinTech. Section 5 concludes the paper.

## **2.0 Definition of FinTech and Its Evolution in Islamic Finance Industry**

The term 'financial technology' or "FinTech" has its root in the "Financial Services Technology Consortium" a project initiated by Citigroup back in to stimulate technological cooperation back in 1993. Today, "FinTech" is a noun related to companies that apply modern innovative technologies such as software to enable provision of financial services. It is now seen as a new market that integrate finance and technology thus replacing traditional financial structures with new technology-based processes (Románova & Kudinska, 2016). It has also been defined as the ecosystem of small technology-based start-up firms that either provide financial services to the marketplace or primarily serve the financial services industry (Deloitte, 2017).

The Financial Stability Board (FSB) defines FinTech as technology-enabled innovation in financial services that could result in new business models, processes, applications or products with an associated material effect on the provision of financial services. The definition is further expanded by organising FinTech activities into five categories of financial services namely (i) payment, clearing and settlement; (ii) deposits, lending and capital raising; (iii) insurance; (iv) investment management; and (v) market support (FSB, 2017).

In the Malaysian context, the term 'FinTech' has not been defined in any existing statutes. However, the definition is given in the Financial Technology Regulatory Sandbox Framework as "technological innovations to be utilised in the provisions of the financial services while FinTech company refers to company that utilises or plans to utilise FinTech but excludes a financial institution."

FinTech has also been characterised as the utilisation of mobile devices and other technology platform to access bank account, transaction notifications, debit and credit alerts by means of push notifications via short messaging services or other forms of notification (Stewart & Jürjens, 2018). Nowadays FinTech industry comprises five major areas: finance

and investment, operations and risk management, payments and infrastructure, data security and monetization, and customer interface (Románova & Kudinska, 2016).

Although FinTech has been in the market place for around 15 - 20 years, traditional financial services have only ramped up their own investments and transformation initiatives in the past 5 - 7 years to keep pace with the new breed of technology disruptor dominating most conversations about the future of the industry (Deloitte, 2017). Today, the technology is ripe with higher penetration of mobile and internet across markets. Consumers are becoming more tech-savvy. Digital banking consumers stand at an estimated 670 million in Asia and are expected to reach 1.7 billion by 2020. As for Malaysia, within a population of 31 million, there is high mobile and internet penetration rate at about 141% and 81% respectively. With a diverse population and a growing middle class, Malaysia is an ideal test bed for developing and commercialising FinTech solutions (BNM, 2017b).

As far as Islamic finance is concerned, rapid growth in the Islamic finance industry is driven by the acceleration of innovations by Islamic financial institutions (IFIs) itself. By embracing and embarking on digital innovations, it opens up new and ample opportunities for the industry players to re-ignite productivity growth and increase efficiency of processes. Technology will certainly redefine the future financial landscape; and FinTech is progressing by leaps and bounds in the conventional sphere; and rapidly changing consumer behavior and needs.

In the context of Malaysia, the integration of FinTech solutions in the business models had taken place with the launch of the Investment Account Platform (IAP) in 2015. IAP is Malaysia's first multi bank online platform that combines the credit evaluation expertise of Islamic banks and the power of technology to channel funds from investors to economic venture. This virtual multisided platform facilitates a collection of interesting investment ventures and projects with transparent risk-return rewards for investors. The shareholders banks are Bank Islam Malaysia Berhad, Bank Muamalat, Bank Simpanan Nasional, Bank Rakyat, Affin Islamic Bank and Maybank Islamik.

Another example is Ethis Crowd, the world's first real estate Islamic crowdfunding online platform. Since its operation in 2015, Ethis Crowd has funded a total of 5000 house with close to 500 houses already completed, helping further social goals such as in the provisions of affordable housing (BNM, 2017). After running a successful pilot project with Bank Islam, in the first quarter of January 2018, Ethis Crowd has officially launched Global Sadaqah, a donation-based crowdfunding platform with its key partners such as Mercy Malaysia, Islamic Relief Malaysia and the National Heart Institute Foundation. The Islamic FinTech venture builder also managed to secure 100,0000 Halal Chain Tokens from blockchain start up Halal Chain, the first digital tokens to be received by Global Sadaqah (IFNFinTech, 2018).

In the block chain space, nine Malaysian banks have come together to develop block chain applications for trade finance. There are also growing use of Open Application Program Interface whereby for the past five years have seen the increase in publication of APIs in the financial sectors with an estimated 200 new APIs published every year and more banks are expected to roll out open APIs in the near or medium term At the industry level, BNM has established an open API implementation group with the members drawn from the industry, FinTech community and key stakeholders to develop open API standards for the financial sector as part of efforts to broaden access and promote financial innovations (BNM, 2018).

From the regulators' perspective, disruptive innovations in the industry are very much welcomed. As far as Malaysia is concerned, the issuance of the Regulatory Sandbox Framework in October 2016 provides regulatory clarity; lowers barriers to entry; and accelerates the time-to-market for productive innovations.

Prior to the introduction of the Sandbox Framework, the Financial Technology Enable Group (FTEG) was established by the BNM on June 2016 with the responsibility of formulating and enhancing regulatory policies to facilitate the adoption of technological innovations in the Malaysian financial services industry (BNM, 2016). The FTEG is part of BNM's commitment to support innovations that will improve the quality, efficiency and accessibility of financial services in Malaysia and serves as BNM's dedicated contact point for FinTech related queries including on regulatory matters related to the adoption of FinTech in the financial services industry in Malaysia.

On 29 July 2016 BNM issued a discussion paper on FinTech regulatory sandbox to further encourage innovation and improve the delivery of financial services. The Sandbox allows regulated financial institutions and FinTech companies looking to do businesses regulated by the BNM to experiment with FinTech solutions in a production or live environment, subject to appropriate safeguards and regulatory requirements. The discussion paper sets out the eligibility criteria, minimum standards and requirements as well as proposed approach in operationalising the Sandbox. The introduction of the Sandbox is another key initiative by the BNM in providing conducive regulatory environment for the adoption of innovative FinTech solutions, following the establishment of FTEG in June 2016 (BNM, 2016).

Accordingly, the Financial Technology Regulatory Sandbox Framework was issued on 18 October 2016 following a one-month consultation on the proposed framework which was released on 29 July 2016. Following the comments and feedback received, the BNM has expanded the eligibility criteria to clarify the focus of innovations that the sandbox aims to support. The minimum standards and requirements for participation in the sandbox were also reviewed to encourage wider participation of FinTech companies to take part in the program. The framework aims to provide an environment that is conducive for the deployment of FinTech to foster innovations in financial services that can contribute to the growth and development of the financial sector in Malaysia. A number of innovative financial solutions have been allowed to operate under the Sandbox initiatives, including an electronic Know Your Customer (e-KYC) solution that could revolutionise the Anti Money Laundering and Counter Terrorism Financing framework in the financial sector in Malaysia (BNM, 2017d).

At the moment there are seven companies undergoing testing in the Regulatory Sandbox which comprises of companies involved in financial advisory or insurance aggregator platform, remittance and money changing services, e-KYC and secured chat banking application. BNM has also introduced regulatory boot camp sessions that are held ever quarter which provides an opportunity for FinTech companies to gain deeper knowledge and understanding before entering the Regulatory Sandbox (BNM, 2017).

BNM has also issued the Anti Money Laundering and Counter Financing of Terrorism Policy for Digital Currencies (Sector 6) on 27 February 2018 which has taken into consideration feedbacks received during the public consultation period on the exposure draft released on 14 December 2017. The objective of the policy document is to ensure that effective measures are in place against money laundering and terrorism financing risks associated with the use of digital currencies and to increase the transparency of digital currency activities in Malaysia (BNM, 2018).

More recent, the Digital Finance Innovation Hub was launched by BNM with collaboration with the United Nations Capital Development Fund (UNCDF) and Malaysia Digital Economy Corporation (MDEC) on 26 September 2018 to further support the financial inclusion of Malaysia's middle and low income. The Digital Finance Hub aims to enable services providers including financial institutions and FinTech start-ups, to use technology in promoting inclusive finance, including through the introduction of products and services that meet the needs of the underserved in Malaysia. In partnership with BNM and MDEC, the

UNCDF has also launched the Inclusive FinTech Accelerator Program that aims at solving specific financial inclusion pain points in Malaysia surrounding four key areas namely spending, saving, borrowing and financial planning. The inclusive FinTech Accelerator Program is the first of a series of accelerator programs to be organised jointly by the UNCDF, BNM and MDEC. FinTech start-ups were invited to share their interest to participate in the upcoming accelerator programs and other activities to be organised by the hub from time to time. This effort is expected to contribute to positioning Malaysia as a test-bed for FinTech solutions whilst strengthening its position as a financial inclusion leader (BNM, 2018).

The emergence of FinTech has opened up new opportunities which can greatly benefit the Islamic financial industry. There are three key areas that Islamic finance stand to gain from FinTech. First, by leveraging on technology, industry players are able to create more value and customer focused services. This can be achieved through the delivery of customised solution using for instance biometric technologies, big data and analytics. Technologies such as Application Program Interfaces (APIs) could bring substantial benefits to customers by making banking transactions simpler, quicker and more convenient. Second, the adoption of technology can help Islamic finance reach out to market segments which would not otherwise be cost-effective. This means a great opportunity to serve untapped markets. Third, in term of process, FinTech can assist to improve the efficiency of back-end systems and operations, including through the use of predictive analytics to undertake real time risk management (BNM, 2017).

### **3.0 Legal Issues and Challenges**

Despite the fact that FinTech innovations bring many opportunities that enhances business processes, FinTech may lead to a number of issues and challenges from legal and regulatory point of view. Generally, both traditional financial institutions and FinTech startups face regulatory challenges in capital requirements, anti money laundering, and privacy and security laws. As regulatory changes lag behind the innovation of the industry, FinTech firms need to be more alert of potential changes that may have impact on them and find ways to deal with those changes (Lee & Shin, 2018). The rapid innovation entering into financial industry in general can lead to disruptive innovation, if not properly regulated (Wijayanti & Pradipta, 2017). Thus, regulatory and supervisory authorities should take those issues and challenges into account in order to support the development of a strong and sustainable financial system.

First, the authorities need to determine whether or not the current oversight framework is appropriate to manage operational risks from third-party service providers especially in the areas of cloud computing and data services. The fact is that may third party service providers may fall outside the regulatory parameters of the financial system (FSB, 2017).

Second, recent reports of cyber-attacks underscore the difficulties of mitigating cyber risk associated with FinTech applications. Thus, incorporating cyber-security in the design of the system from the very beginning and FinTech literacy is vital in developing a culture of risk awareness among users and customers. For FinTech applications, critical information may be stored on mobile devices that might get lost or stolen which may compromise the security of the information contained in the mobile device. As consumers can easily file complaints related to data security and privacy breaches to regulatory agencies, FinTech companies need to develop appropriate measures to protect sensitive consumer data from unauthorised access (Lee & Shin, 2018).

Third the authorities have to deal with cross-border legal consideration and legal arrangement through cooperation and coordination among authorities having different legal

frameworks. Legal validity and enforceability of FinTech based contracts and applications require further deliberation among the authorities (FSB, 2017).

Fourth, the complexity of big data analytics that drives transformation across industries makes it difficult for authorities to assess new unforeseen risks in market behaviour. Thus, governance and disclosure framework supporting big data analytics is an area that requires attention by the relevant authorities (FSB, 2017).

Fifth, many FinTech based products and services are based on new technologies, and it is challenging to integrate the FinTech application into existing systems. Certain adaptations are required to suit the existing system and infrastructure which will involve costs and expenses.

In addition, the application of robo-advisers for the fund and wealth management services may expose customers to financial risk and the FinTechs may have to take potentially serious responsibility for any loss due to the algorithmic failure of the robo-advisers (Lee & Shin, 2018). More important is the need to deal with Shariah non-compliance risk that may arise for failure on part of the FinTech system to comply with Shariah requirements. Thus, it is the paramount duty of the Shariah advisers of the Islamic financial institutions to deal with the risk associated with the system and applications.

Last but not least, issue of money laundering and terrorist financing. No doubt that rapid technological developments have offered immense potential for economic growth, but they have also spawned new ways for criminal and terrorist organisations to acquire, move and manage their funds. Terrorist financiers will attempt to benefit from anonymous transactions made possible by innovations of new payment products and services such as internet-based payment systems, prepaid cards and virtual currencies. Likewise fundraising through social media and other online platforms such as crowd funding have increased in prominence, in addition to other more traditional sources of funds such as proceeds of criminal activities, conventional donations and funding from legitimate purposes. On the other hand, while technological misuse poses a danger to the society, technology is also an effective tool to counter terrorism financing. The use of artificial intelligence and big data will have the potential to increase efficiency and accuracy of assessment that is essential in a dynamic environment. Thus, the financial sector needs to adopt the latest and most advanced technologies to improve its risk management framework (BNM, 2017d).

#### **4.0 Regulatory Approach for Malaysia**

The power vested to the BNM to regulate the application of FinTech in the Islamic finance in Malaysia is provided by the law under the Central Bank of Malaysia Act 2009 (CBMA), the Anti Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATF) and the Islamic Financial Services Act 2013 (IFSA). The law allows BNM to issue guidelines from time to time to govern the industry. It must also be noted that the Islamic finance industry is also subject to the laws relating to cyber security and data protection being enforced in Malaysia which are relevant in dealing with FinTech. The relevant provisions of the relevant laws are discussed here.

##### **4.1 The Financial Technology Regulatory Sandbox Framework**

The Framework is introduced to enable innovation of FinTech to be deployed and tested in a live environment within specified parameters and timeframes. The Framework is applicable to:

- (a) a financial institutions as defined under paragraph 4;
- (b) a FinTech company which collaborates with a financial institutions; and

- (c) a FinTech company intending to carry on:
  - (i) an authorised or registered business under FSA 2013 and
  - (ii) an authorised business as defined in the IFSA 2013; or
  - (iii) a money services business as defined in the Money Services Business Act 2011 (MBSA).

The application will be considered based on certain aspects, among others, the potential benefits of the proposed product, service or solution; the potential risks and mitigating measures; and the integrity, capability and track record of the financial institutions or the FinTech companies. The Framework sets out six requirements that the applicant must demonstrate to BNM in the application that:

- (i) the product, service or solution is genuinely innovative with clear potential to improve accessibility, efficiency, security and quality in the provision of financial services; enhance the efficiency and effectiveness of Malaysian financial institutions' risk management; or address gaps in or open up new opportunities for financing or investments in the country's economy.
- (ii) the applicant has conducted an adequate and appropriate assessment to demonstrate the usefulness and functionality of the product, service or solution and identified the associated risks;
- (iii) the applicant has the necessary resources to support testing in the sandbox which includes the required resources and expertise to mitigate and control potential risks and losses arising from offering of the product, service or solution;
- (iv) the applicant has a realistic business plan to deploy the product, service or solution on a commercial scale in Malaysia after exit from the sandbox;
- (v) the provision of the product, service or solution is either wholly or partly incompatible with laws, regulations or standards administered by the BNM. In such cases, the Bank may consider granting relevant regulatory flexibilities for the purpose of testing a proposed product, service or solution that possesses strong value propositions; and
- (vi) the applicant is led and managed by persons with credibility and integrity.

The Framework further requires that the applicant must identify the potential risks to financial institutions and financial consumers that may arise from the testing of the product, service or solution in the sandbox and propose appropriate safeguards to address the identified risks. Successful applicant will be given testing period which shall not exceed 12 months from the start date of the test. The BNM has the power to revoke an approval to participate in sandbox at any time before the end of the testing period if the participant:

- (a) fails to carry out the safeguards referred to in the Framework;
- (b) submits false, misleading or inaccurate information, or has concealed or failed to disclose material facts in the application;
- (c) contravenes any applicable law administered by the BNM or any applicable law in Malaysia or abroad which may affect the participant's integrity and reputation in Malaysia;
- (d) is undergoing or has gone into liquidation;
- (e) breaches data security and confidential requirements;
- (f) carries on business in a manner detrimental to customers or the public at large; or
- (g) fails to effectively address any technical defects, flaws or vulnerabilities in the product, service or solution which gives rise to recurring service disruptions or fraud incidents.

#### **4.2 Anti-Money Laundering and Counter Financing of Terrorism Policy (AML/CFT) – Digital Currencies (Sector 6)**

This document which came into effect on 27 February 2018 lays down the minimum requirements and standards that a reporting institutions must observe to increase the transparency of activities relating to digital currencies and ensure effective AML/CLF control measures are put in place to mitigate risks that reporting institutions may be used as conduits for illegal activities.

BNM reiterates that digital currencies are not recognised as legal tender in Malaysia. Thus, dealings in digital currencies are not covered any prudential and market conduct requirements applicable to licensed and authorised activities, or by established avenues for redress in the event of complaints or losses and damages incurred by parties dealing in digital currencies.

This document is applicable to reporting institutions carrying on the following activities listed in Paragraph 25 of the first Schedule to the AMLAFT which includes:

- (a) activities carried out by any person who provides any or any combination of the following services:
  - (i) exchanging digital currency for money;
  - (ii) exchanging money for digital currency; or
  - (iii) exchanging one digital currency for another digital currency whether in the course of carrying on digital currency exchange business or otherwise.

The document defines 'digital currency' as digital representation of value that function as a medium of exchange; and is interchangeable with any money (including through the crediting or debiting of an account" but excluding electronic money, as defined under the FSA 2013 and IFSA 2013, issued by an approved issuer of electronic money under the Acts.

Among the requirement imposed on reporting institutions under the Policy Document are:

- (a) Reporting institutions are required to declare its details to the BNM which includes among others business information, registered business address, key responsible person and compliance officer.
- (b) Reporting institutions must take appropriate steps to identify, assess and understand their ML/TF risks in relation to their customers, countries and geographical areas and products, services, transactions or delivery channels.
- (c) Reporting institutions are required to conduct CDD on all customers and the persons conducting the transaction in the following circumstances:
  - (i) when the reporting institution establishes business relationship with customer; and;
  - (ii) when the reporting institutions have any suspicion of ML/TF.
- (d) Reporting institutions are required to identify and assess the ML/TF risks that may arise in relation to the development of new digital currencies, products, services and business practices, including new delivery mechanism, and the use of new or developing technologies whether for new or existing solutions.
- (e) Reporting institutions are required to have in place an adequate management information system to complement and support its customer due diligence process;
- (e) Reporting institutions must appoint a Compliance officer whom shall act as the reference point for AML/TF matters within the institutions.
- (f) Reporting institutions are required to submit promptly a suspicious transaction report to the Financial Intelligence and Enforcement Department BNM whenever the reporting institutions suspect or have reason to suspect that the transaction including attempted or proposed transaction, regardless of the amount, appears unusual; illegal; to have no clear economic purpose; to involve proceeds from an unlawful activity and



instrumentalities of an offence; or to indicate that the customer could be involved in ML/TF.

BNM has also initiated the foundational work for the development of a regulatory structure for digital currencies. BNM has designated persons converting crypto currencies into fiat money as reporting institutions under the to prevent the abuse of the system for criminal and unlawful activities and ensuring the stability and integrity of the financial system (BNM, 2017d). As part of efforts to promote greater transparency surrounding digital currency activities in Malaysia, BNM has listed 43 reporting institutions dealing with digital currencies for the public reference.

#### **4.3 Anti Money Laundering, Anti Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATF)**

Even though AMLATF does not make direct reference to FinTech, the provisions relating to non-compliance are relevant to regulate FinTech based activities in the Islamic finance industry in Malaysia. Among the provisions are:

- (a) Section 22 deals with offences in breach of provisions under Part IV on reporting obligations of reporting institutions under the Act. Section 22 provides that any person who contravenes this provision commits an offence and shall on conviction be liable to a fine not exceeding one million ringgit or to imprisonment for a term not exceeding three years or to both, and in the case of a continuing offence, shall in addition be liable to a fine not exceeding three thousand ringgit for each day or part thereof during which the offence continues to be committed.
- (b) Section 86 stipulates that any person who contravenes any provision of the Act or regulations made under it; or any specification or requirement made, or any order in writing, direction, instruction, or notice given, or any limit, term, condition or restriction imposed, in the exercise of any power conferred under or pursuant to any provision of this Act or regulations made under it, commits an offence and shall on conviction, if no penalty is expressly provided for the offence under this Act or the regulations, be liable to a fine not exceeding one million ringgit.
- (c) Section 86A deals with attempts, abetments and criminal conspiracies to commit an offence under this Act which stipulates that it is punishable with the penalty provided for the offence.
- (d) Section 92 provides that the competent authority or relevant enforcement agency, as the case may be, may, with the consent of the Public Prosecutor, compound any offence under this Act or under regulations made under the Act, in an amount not exceeding fifty percent of the amount of the maximum fine for that offence, including the daily fine, in the case of a continuing offence, to which that person would have been liable if he had been convicted to the offence, within such time as may be specified within such time as may be specified in its written offer.

#### **4.4 Financial Services Act 2013 and Islamic Financial Services Act 2013 (FSA and IFSA)**

In this regard, BNM as the governing authority for the FSA and IFSA has from time to time issued guideline to banking and financial institution to enhance and strengthen security measures undertaken by all participating institutions. BNM had issued BNM/GP11 which provides guidelines on consumer protection on electronic fund transfer. It defines the basic framework to establish the rights, liabilities and responsibilities of customers and financial institutions relating to Electronic Fund Transfer (EFT).

Minimum Guidelines on the provisions of Internet Banking Services by Licensed Banking Institutions issued by the BNM sets the minimum guidelines that licensed institutions in Malaysia should observe in providing Internet banking and it further provides that banking institutions are free to adopt more stringent measures and are expected to keep abreast with technological developments and needs of the customers.

#### **4.5 Personal Data Protection Act 2010**

The Personal Data Protection (PDPA) came into effect in 2013 with the aim to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto. With the coming into force of the PDPA, certain class of users are required to register with the Personal Data Protection Commissioner as stipulated by the Personal Data Protection (Class of Data Users) Order 2013 (PDPO 2013). Data users from eleven industries which come under the class of users are communications, banking and financial institution, insurance, health, tourism and hospitalities, transportation, education, direct selling, services, real estate and utilities.

Being among the 11 industries, banking and financial institutions are required to register with the Personal Data Protection Commissioner as part of the implementation of the PDPA 2010. The law requires that business entities and service providers under these categories to comply within three months from the date of the coming into effect of the legislation. It is clear that the financial services sector is covered by the PDPA and PDPO. Besides registration, enforcement of PDPA would require compliance to the personal data principles and the initial step to be taken by data users is by having a privacy policy in place, where the data user guarantees to take steps to comply with the seven data protection principles.

Another important element in discussing the applicability of PDPA is that this law is only applicable to the processing of personal data in respect of commercial transactions. Therefore, any personal data processed for non-commercial or private use is exempted from this legislation. Section 4 of the PDPA defines commercial transaction to mean any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agencies, investments, financing, banking and insurance. The definition provided by the Act does not include credit reporting which is under the purview the Credit Rating Agency Act 2010.

All banking and financial institutions whether conventional or Islamic as the case may be are subject to this requirement. The BNM in exercising their powers under the Central Bank of Malaysia Act 2009 and other relevant legislations are closely monitoring the operations of the financial sector in Malaysia to maintain confidence of the public and investors that their personal data and privacy are protected by the law.

#### **4.6 Digital Signature Act 1997**

The Digital Signature Act 1997 (DSA) sets out the regulatory structure in respect of entities involved in the creation of digital signatures and legalise private key-public key cryptography. The DSA allows individuals and businesses to use digital signatures in commercial transactions. It provides for the licensing and regulations of Certification Authorities which issue digital signatures and certify the identities of the signatories by issuing a certificate.

Section 2 defines digital signature as a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key

that corresponds to the signer's public key; and whether the message has been altered since the transformation was made.

Section 64 specifically provides that a digitally signed message is deemed to be written document if bears in its entirety a digital signature; and that digital signature is verified by the public key listed in a certificate which was issued by a licensed certification authority; and was valid at the time the digital signature was created.

As stipulated under section 43, by accepting a certificate issued by a licensed certification authority, the subscriber named in the certificate assumes a duty to exercise 'reasonable care' to retain control of the private key corresponding to the public key listed in the certificate, and to prevent its disclosure to any person not authorised to create the subscriber's digital signature.

Digital signature technology provides data security which is ensured by the use of encryption algorithms and protocols. Encryption scrambles the data in such a way that it is practically impossible to decipher the data without knowing the decryption key. VISA and MasterCard have introduced a standard known as Secure Electronic Transaction (SET) for the sending of credit card numbers over the Internet to purchase goods or services in a safe and secure environment.

#### **4.6 Computer Crimes Act 1997**

The Computer Crimes Act 1997 (CCA) was introduced in 1997 to provide for offences relating to the misuse of computers as well as to provide that the commission of the offences is extra-territorial. It sets out a framework that defines important term such as proper illegal access, interception and use of computer, outlines the standard for service providers and imposes potential penalties for infringement.

Section 3 makes it an offence if a person causes a computer to perform any function with intent to secure access to any program or data held in any computer; where the access he intends to secure is unauthorized; and he has knowledge of the circumstances when he causes the computer to perform the function. The offence is punishable upon conviction with a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or to both.

Section 4 further states that a person shall be guilty of an offence if he commits with intent to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code; or to facilitate the commission of such an offence whether by himself or by any other person. The offence is punishable with a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both.

Section 5 (1) further provides that a person shall be guilty of an offence if he does any act which he knows will cause unauthorized modification of the contents of any computer. The penalty for this offence is fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both; or be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both, if the act is done with the intention of causing injury as defined in the Penal Code.

Section 6 states that a person shall be guilty of an offence if he communicates directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorized to communicate, and he is liable upon conviction to a fine not exceeding twenty-five thousand ringgit or to imprisonment for a term not exceeding three years or to both.

As far as cross border issues of computers crimes, section 9 provides for extra territorial effect of the Act where an offence under this Act is committed by any person in

any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia. This provision must also be read in light of section 127A of the Criminal Procedure Code which provides on liability for offences committed out of Malaysia; Extra-territorial Offences Act 1976; and the Mutual Assistance in Criminal Matters Act 2002 (Shahwahid & Miskam, 2014).

## 5.0 Conclusion

With the rapid growth of FinTech in Islamic finance, there are both opportunities and risks to financial stability that policymakers and regulator should take into consideration. Policymakers must continue to assess the adequacy of the regulatory framework as adoption and application of FinTech increases, with the objective of taking advantage of the benefits while at the same time mitigating risks. It is essential that the financial sector's risk management strategy remains agile in order to mitigate emerging risks associated with FinTech. This requires not only the development of innovative technology-based deterrents and pro-active detection systems but also effective cooperation between the public and private sector, law enforcement domestically and across borders.

## REFERENCES

- BNM (2016a). Press Release: Establishment of Financial Technology Enabler Group published on 2 June 2016 available at [http://www.bnm.gov.my/index.php?ch=en\\_press&pg=en\\_press&ac=4192&lang=en](http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4192&lang=en)
- BNM (2016b). Press Release: Discussion Paper on FinTech Regulatory Sandbox published on 29 July 2016 available at [http://www.bnm.gov.my/index.php?ch=en\\_press&pg=en\\_press&ac=4224&lang=en](http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4224&lang=en)
- BNM (2016c). Press Release: Financial Technology Regulatory Sandbox Framework published on 18 Oct 2016 available at [http://www.bnm.gov.my/index.php?ch=en\\_press&pg=en\\_press&ac=4273&lang=en](http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4273&lang=en)
- BNM (2017a). Financial Technology Enabler Group (FTEG) Chairman's Opening Remarks at Finnovaisa KL available at [http://www.bnm.gov.my/index.php?ch=en\\_speech&pg=en\\_speech&ac=721&lang=en](http://www.bnm.gov.my/index.php?ch=en_speech&pg=en_speech&ac=721&lang=en)
- BNM (2017b). Assistant Governor's Opening remarks at Islamic FinTech Dialogue 2017 - FinTech and Entrepreneurship available at [http://www.bnm.gov.my/index.php?ch=en\\_speech&pg=en\\_speech&ac=764&lang=en](http://www.bnm.gov.my/index.php?ch=en_speech&pg=en_speech&ac=764&lang=en)
- BNM (2017c). Assistant Governor's Keynote Address at the ASAS Shariah FinTech Forum 2017 [http://www.bnm.gov.my/index.php?ch=en\\_speech&pg=en\\_speech&ac=772&lang=en](http://www.bnm.gov.my/index.php?ch=en_speech&pg=en_speech&ac=772&lang=en)
- BNM (2017d). Governor's Welcoming Remarks at the Third Counter-Terrorism Financing Summit 2017 - Powering Regional Solutions Through Strengthened Alliances and Innovations available at [http://www.bnm.gov.my/index.php?ch=en\\_speech&pg=en\\_speech&ac=776&lang=en](http://www.bnm.gov.my/index.php?ch=en_speech&pg=en_speech&ac=776&lang=en)
- BNM (2018). Deputy Governor's Opening Address at the Asian Banker Digital Finance Convention 2018 available at [http://www.bnm.gov.my/index.php?ch=en\\_speech&pg=en\\_speech&ac=792&lang=en](http://www.bnm.gov.my/index.php?ch=en_speech&pg=en_speech&ac=792&lang=en)
- Deloitte. (2017). *FinTech by the numbers*. Retrieved from
- FSB. (2017). Financial Stability Implications from FinTech.
- IFNFinTech. (2018). Ethis Venture launches Islamic charity crowdfunding platform. *IFNFinTech*, Q3 2018.
- Laldin, M. A. (2018, 3 October 2018). FinTech and Islamic Finance. *IFN Islamic Finance News*, 15, 67.
- Lee, I., & Shin, Y. J. (2018). FinTech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, 61, 35-46.

- PricewaterhouseCoopers. (2017). *Global FinTech Report 2017*. Retrieved from PwC. (2017). Blurred lines: How FinTech is shaping Financial Services.
- Romānova, I., & Kudinska, M. (2016). Banking and FinTech: A Challenge or Opportunity? *Contemporary Studies in Economic and Financial Analysis* (pp. 21-35).
- Shahwahid, F. M., & Miskam, S. (2014, 26 -27 May 2014). *Personal Data Protection Act 2010: Taking the First Steps Towards Compliance*. Paper presented at the Conference on Management and Muamalah (CoMM2014), Selangor, Malaysia.
- Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech Innovation in Germany. *Information and Computer Security*, 00-00. doi:10.1108/ics-06-2017-0039
- Wijayanti, D. M., & Pradipta, H. (2017, 6 September 2017). *Sharia FinTech: Positive Innovation in Consumer Perspective*. Paper presented at the International Seminar Academic Network on Competition Policy, Bali.