JICLT
Journal of International Commercial Law and Technology
Vol. 6, Issue 4 (2011)

Security Safeguards on e-Payment Systems in Malaysia: Analysis on the Payment Systems Act 2003

Sonny Zulhuda & Ida Madieha Abdul Ghani Azmi
International Islamic University Malaysia
Corresponding author: sonny@iium.edu.my

Abstract. Central to the infrastructure of electronic commerce activities is the electronic payment system. This encompasses not only the issues of technical sophistication but also legal readiness. In the context of electronic commerce environment in Malaysia, this paper seeks to highlight and examine the Malaysian legal readiness in the aspect of electronic payment system, focusing on its Payment Systems Act 2003. The discussion is limited to the issue of electronic security measures embodied in the law. Within its restricted scope, this paper seeks to demonstrate how the law recognizes the importance of security measures in order to build confidence and trust among the public and mainly the users of electronic payments in the country.

1. Introduction

Malaysia regards electronic commerce as a powerful driver for the national development and economic growth. This belief has been reinforced by the setting up of national policies and enactment of laws seeking to ensure that processes, tools and technologies are put in place to facilitate the electronic commerce. Among those laws is the Payment Systems Act 2003 (Act 627). This piece of legislation was enacted to provide the framework for the regulation and supervision of the payment systems and payment instruments in Malaysia. The ultimate goal is to enhance the efficiency of payment system and to specifically provide the mandate to the banking regulator to effectively oversee and facilitate greater development of such system in the country. This law is expected to be influential in facilitating the electronic commerce in Malaysia, particularly its electronic banking practices.

Nevertheless, among the biggest stumbling block to this law this law needs to pass through is the fear over security and privacy of the payment system itself. In order to do this, there is consequently a pressing need to identify whether or not the law has sufficiently addressed this issue. In particular, there is a need to identify the extent to which such legal instrument recognizes and requires the necessary security measures in the payment system in Malaysia.

This paper attempts to answer two main questions: first, what are, conceptually speaking, the e-security measures required in electronic commerce system, especially the electronic payment system? Secondly, how does the Malaysian Payment Systems Act 2003 address those security measures? This paper is purely a legal, doctrinal and analytical study focusing mainly on the electronic commerce laws in Malaysia, in particular on the e-payment system as required in the Payment Systems Act 2003. This brief analysis is significantly important due to the lack of research currently undertaken on the system security implication of this particular legislation.

2. E-Payment and Security

The notion of electronic security or information security is strongly linked to the value of information itself. In other words, only when a value of thing is feared to be threatened or attacked, the security of such thing is required and prevention of related risk is therefore warranted (Schneier, 2003). The more individuals and organisations value their assets, the bigger their concern over security. According to Merriam-Webster

Dictionary, security in general is the quality or state of being secure, that is, to be free from danger. In a more operational sense, security is defined in the Oxford dictionary as measures that are taken to guarantee the safety of a country, person, thing of value, etc. Schneier (2003) states that security is about preventing adverse consequences from the intentional and unwarranted actions of others. The objective of security is, therefore, building protection against adversaries from those who would do harm, intentionally or otherwise (Whitman & Mattord, 2005).

Information security therefore is the protection of information and its critical elements, including the electronic systems and hardware that use, store and transmit that information (Whitman & Mattord, 2005). The international standard of ISO/IEC 17799—subsequently renumbered ISO/IEC 27002:2005 in July 2007—on information security management defines information security as "the protection of information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities." Based on this observation, therefore, our proposition as to the meaning and scope of information security is that it is a series of mechanisms and measures to protect the value of information assets ('information' being the *process*, the *knowledge* and the *thing* in general) from unwarranted, intentional or unintentional adversaries in the form of external and internal threats that may cause loss, harm or danger to the information asset.' Such process of information security does involve the assessment and evaluation of risks and the identification of the right countermeasures.

For electronic system such as e-payment environment, security is considered a business requirement, as it is closely related to the investment in the long-term. In this context, Calder and Watkins (2005) argued that business needs are reflected in at least four dimensions. First, information security protects the organisation's ability to function. Secondly, it enables a safe operation of applications implemented on the organisation's IT systems. The third dimension is that information security protects the data that organisation collects and uses. Last but not least, information security safeguards the technology assets used at the organisation.

Besides being a business need, information security is in fact becoming a legal necessity (Pipkin, 2000). Companies must adequately protect their business assets or be subject to stockholder suits, and they must protect information about individuals in their custody or they may face legal suits on privacy infringement.

3. CIA Principles of E-Security

Information security (or e-security for this purpose) is a complex issue and deals with the confidentiality, integrity and availability (CIA) of data (Calder & Watkins, 2005). Due to its centrality in the information security, CIA principles have become integral part of the definition of information security in many literature and industrial standards. The Information Technology Security Evaluation Criteria (ITSEC) issued in June 1991 by the Commission of the European Communities, for example, adopted the CIA principles (Tryfonas, et. al., 2000). In the US, the model of information security developed by the Committee on National Security System (CNSS), formerly known as the National Security Telecommunications and Information Systems Security Committee (NSTISSC), has evolved from a concept developed by the computer security industry known as the CIA (Confidentiality, Integrity and Availability) Triangle (Whitman & Mattord, 2005).

The CIA principles have also been adopted by standards and codes developed by two prominent international bodies, namely the International Organisation for Standardisation ('ISO') and the British Standard Institute (BSI). The British Standard (issued by the BSI) 7799-1:1999 on 'Code of Practice for Information Security Management' elaborates that information security is characterized by what it seeks to preserve, i.e. confidentiality, integrity, and availability of information. Calder & Watkins (2005) highlighted that this British Standard has been further adopted as an internationally recognised best practice in 2000 by the International

Organisation for Standardisation and is known as ISO/IEC 17799, which reflects similar concern when defining the parameters of information security.

According to the principle of confidentiality, the information security measures need to guarantee that information is being transmitted from a known source to an intended recipient only (Toscano, 2000). This means that information in all of its forms (electronic or otherwise), and in all of its states (stored, transmitted, in-use), and in all of its locations (file cabinet, printouts, computer storage, disks), must be protected from unauthorised access. Pipkin (2000) reckons that the ability to maintain the confidentiality is largely based on the quality of managing the sensitivity classifications assigned to the information.

The integrity principle seeks to safeguard the accuracy and completeness of information and the authentic ways in which it is processed. Integrity therefore has to do with the validity of the data and is concerned with whether it has been modified since its creation. Under this objective, any security measures must enable such information assets to be stored, transmitted, processed, or used *without compromise, alteration, or corruption* (Toscano, 2000). Loss of integrity—including the loss of accuracy—is potentially devastating. For instance, medical prescriptions may be fatal if it is based on incomplete or inaccurate information on the patients or on the drug databases. Thus, in order to achieve the preservation of information integrity, efforts need to be taken throughout the whole life-cycle of the information resources, and in particular on the collection and the storing of the information. This goal derives certain sub-principles such as authentication and verification (Pipkin, 2000). While the former is concerned with proving positively that the entity is what it claims to be, the latter involves the process of validating the accuracy of information.

Furthermore, information resources need to be available when they are needed. The challenge is that such information resources may not always be there when the owners or the users need to refer to them due to many things intentional or otherwise. This loss of availability may therefore turn into a loss of productivity. As a goal of information security, availability principle seeks to ensure that authorised users have access to information and associated assets whenever required. The information and information resources must therefore be in a usable presence. Indeed, business depends on the availability of business information and processing. This is, as asserted by Pipkin (2000), a very important principle bearing in mind that the rampant threat of denial of service could mainly make data or resources unavailable to intended users.

4. Salient Features of Payment Systems Act 2003

The Malaysia's Payment Systems Act ('PSA') 2003 (Act 627), which came into force on 1st November 2003, is a principal legislation which provides for the framework for the regulation and supervision of the payment systems and payment instrument in Malaysia. When anticipating the birth of this law, the Central Bank Governor (Aziz, 2003) emphasized that the study on the legal and regulatory framework was undertaken "to enhance the efficiency of payment system and to specifically provide the mandate to the Central Bank of Malaysia to effectively oversee and facilitate greater development of such system in the country."

The ultimate objectives of PSA 2003 are reflected in its preamble as *"to promote monetary stability and a sound financial structure."* This was meant to promote a reliable, efficient and smooth operation of the national payment and settlement systems and for ensuring that the national payment and settlement systems policy is directed to the advantage of Malaysia. This noble task is spearheaded by the Central Bank or Bank Negara Malaysia or BNM (Bank Negara Malaysia, 2007).

This task of the Central Bank is not only important but is also very urgent. As digital transactions have become widespread, alternative payment methods would essentially be issued and used by variety of institutions. Some would even extend beyond the reach of national boundaries. The Central Bank Governor noted that e-cash and e-commerce will make it increasingly difficult to define and measure monetary aggregates, national income and wealth (Aziz, 2001). Thus, it was noted that capacities and capability of institutions need to be enhanced,

financial infrastructure needs to be put in place and consumers and markets educated accordingly. This Payment Systems Act would provide essential remedies to offer in this new financial environment.

5. Classifications of E-Payment Operators

The PSA 2003 imposes certain obligations on two classes of e-payment system operators, i.e. the operator of designated payment system (DPS) and the operator of designated payment instrument (DPI).

'Payment system' is defined in section 2 as any system or arrangement for the transfer, clearing or settlement of funds or securities. It, however, excludes a payment system operated by the Bank under the Central Bank of Malaysia Act 1958; a clearing house recognized under the Securities Industry Act 1983; a clearing house licensed under the Futures Industry Act 1993; an in-house payment system operated by a person solely for his own administrative purposes that does not transfer, clear or settle funds or securities for third parties; a system that solely facilitates the initiation of payment instructions; and such other systems or arrangements as may be prescribed by the Bank. Whereas 'payment instrument' means any instrument, whether tangible or intangible, that enables a person to obtain money, goods or services or to otherwise make payment. It therefore includes credit cards, charge cards, debit cards, and e-money.

A payment system will be classified as 'designated payment system' ('DPS') under section 6(1) if that payment system poses a systemic risk or that such designation is necessary to protect the interest of public. Systemic risk means "the risk that the failure of a participant or operator to meet his payment or settlement obligations; (1) will cause another participant to be unable to meet his payment or settlement obligations when due, or (2) may cause significant liquidity or credit problems that might threaten the stability of financial markets." Until recently, it is noted that BNM has so far designated two payment systems as DPS, namely the 'Real Time Electronic Transfer of Funds and Securities System' or 'RENTAS', a real time gross settlement system for the transfer and settlement of funds and book-entry scripless debt securities; and the '*Sistem Penjelasan Informasi Cek Kebangsaan secara Elektronik*' or 'eSPICK', a cheque clearing system for the clearing of cheques.

A payment instrument can be classified as a 'designated payment instrument' ('DPI') under section 24 provided that such instrument may be of widespread use as a mean of making payment and may affect the payment systems of Malaysia; and that it is necessary to protect the interest of the public or it is necessary to maintain the integrity, efficiency and reliability of a payment instrument. Three types of payment instrument have been so far designated by BNM as DPI, namely (1) charge cards; (2) credit cards; and (3) electronic money which stores funds electronically in exchange of funds paid to the issuer and is able to be used as a mean of making payment to any person other than the issuer (see, Payment Systems (Designated Payment Instruments) Order 2003, section 2).

The above definitions were given judicial notice in the first court case involving the Act, *i.e*. the case of *Diana Chee Vun Hsai v Citibank Bhd* [2009] 5 MLJ 643; an originating summon which was heard in Kuala Lumpur High Court. The court asserted that the MasterCard credit card in issue was a designated payment instrument, and the issuing entity, i.e. Citibank Bhd, was an operator or issuer of a designated payment system under section 25 of the Payment Systems Act 2003.

In that case, the applicant was a MasterCard credit card holder issued by Citibank (the respondent). She had lost her credit card and the respondent had subsequently deducted RM1, 859.01 being charges incurred by unauthorised use of her credit card. The applicant argued that the limit of liability for a lost credit card is RM250 as stated in the Bank Negara Guidelines on Credit Card. The respondent however relied on the terms of the credit card agreement and claimed that the guidelines were incorporated in the said agreement with some modifications. The applicant filed legal suit claiming declarations that the respondent should not have modified the Bank Negara Guidelines arguing that the guidelines have the force of law. Furthermore, she also claimed that

the terms and conditions of respondent's credit card relied upon by the respondent to deduct a sum of RM1,859.01 from the applicant's account were hence illegal, void and contrary to public policy. The court finally allowed the applicant's application and declared that the respondent has contravened the law and public policy as articulated in the PSA 2003. In relation to credit card agreements, the court enunciated one particular importance of the Act when Mohamed Apandi J. asserted that the terms and conditions of the credit card agreement, as a contract, are deemed to be read, governed and construed in accordance with laws of Malaysia, and in this case, the Payment Systems Act 2003.

6. E-Security Safeguards and the Duty of E-Payment Operators

This Act upholds the information security framework in many ways. The first apparent reason is that because this Act was clearly drafted and passed with high regards to the advances of information technology and online working environment. The definition in section 2 of 'payment instrument' that includes intangible instruments is a witness to this; and so are the words 'data', 'computer' and 'computer output'. The use of these words and their definition arguably offers important support for the interpretation and enforcement of law when it comes to online environment and computer-related cases in the future.

The PSA is also an important part of information security legal framework for e-commerce in Malaysia being that the objective is to ensure the sustainability and competitiveness of the economy through the creation of a sound financial structure. A *sound* financial structure should necessarily mean a financial infrastructure which is reliable and secure. This should be viewed together with the emphasis of public interest protection as required in the designation of DPS and DPI as earlier highlighted (e.g. in section 24). On the designation of payment instruments, section 24(1) furthermore requires the element of public security *or* the maintenance of the integrity, efficiency and reliability of a payment system. This arguably means that the need for system security is on equal importance with the need for the protection of public security.

Such proposition can also be supported by other aspects in the PSA 2003. As noted, among the obligations of the operators of e-payment system, each of the DPS and DPI operators would have to comply with certain requirements including governance and operational requirements. In terms of governance requirements, e-payment operators shall establish adequate governance arrangements which are effective, accountable and transparent to ensure the continued integrity of such designated payment system or instrument (ss. 13 and 27 respectively). Governance involves the issues of management, directorship, internal and external control as well as designating roles and responsibilities within the organization. In a corporate sense, as defined by the Organization of Economic Cooperation and Development (OECD), governance is a system by which business corporations are directed and controlled. Therefore, this necessarily indicates that an effective, accountable and transparent governance has a direct causal effect towards system integrity and hence system security.

Whereas under the provisions of operational requirements (under sections 14(d) and 28(c) for DPS and DPI respectively), e-payment operators are obliged, among others, to put in place measures to ensure the safety, security and operational reliability of the designated payment system or instruments (whichever applies) including contingency arrangements. This is a clear obligation to ensure all the necessary security measures are installed and implemented. It is argued that the phrase security in the above provisions should be understood in the light of the CIA principles of information security as earlier examined. In other words, such security measures must ensure the confidentiality, integrity and availability of the payment system. It is noteworthy that failure to comply with governance and operational requirements can each trigger a penal sanction amounting to a maximum fine of RM3 million or a maximum imprisonment of 3 years or to both (section 56 and the Schedule). The provision of penal sanctions is arguably another critical framework in upholding and implementing sound, secure and reliable financial infrastructure in Malaysian e-payment system.

Beside the provisions that oblige certain duties to e-payment operators, PSA 2003 also impose secrecy and confidentiality requirement. It prohibits in section 73 for anyone –internal or external parties alike–who for any

reason, has by any means access to any record, book, register, correspondence, or other document, or material, relating to the affairs or, in particular, the account, of any particular operator of a designated payment system, participant of a payment system or user of a payment instrument, to give, produce, divulge, reveal, publish or otherwise disclose to any person, or make a record for any person of, any information or document relating to the affairs or account of such operator of a designated payment system, participant of a payment system or user of the payment instrument. This obligation of secrecy is also accompanied by penal sanctions in case of breach; i.e. a fine not exceeding RM500, 000.00 as generally provided in section 57 of the Act.

Given the mandate of this Act, the Central Bank of Malaysia or BNM assumes a huge oversight responsibility for the payment and settlement systems in the country considering the high numbers of usage in Malaysia. According to Bank Negara Malaysia (2007: pp. 20-23), the number of users and subscribers of payment instruments in 2007 (including credit cards, charge cards, debit cards and e-money) was over 85 million usage with a total value of transaction reaches RM 4.6 million, including Interbank Giro. For this purpose, too, BNM requires that each of the DPS and DPI operator to identify, document and submit measures that ensure the safety, security and operational reliability of the payment system/instrument, respectively, including contingency arrangements. These requirements were prescribed in the Payment Systems (Submission of Documents and Information) Order 2003, section 2(f)(v) and 2(g)(v).

The authority of BNM was further strengthened by the above case of *Diana Chee Vun Hsai v Citibank Bhd.* The Court asserted that to ensure the compliance of the approval under section 25 of PSA 2003, BNM was empowered to issue the Credit Card Guidelines (BNM/RH/GL-012-1) pursuant to section 70 of the Act. In assessing such authority under section 70, the court maintained that BNM "may, generally in respect of this Act, or in respect of any particular provision of this Act, or generally in respect of the conduct of all or any of the operators of payment systems or issuers of payment instruments, issue such guidelines, circulars, standards or notices as the Bank may consider desirable." On top of that, that Credit Card Guideline, the court further held, shall be treated to have the force of law. This court's decision has certainly upheld the role of BNM in ensuring a sound financial infrastructure in Malaysia as desired by the PSA 2003.

7. Final Remarks

It is reiterated here that the PSA 2003 plays an enormous role in providing and upholding security safeguards especially in respect with electronic payment and settlement system which is a very integral part of country's economic and commercial infrastructures. If there is one sector that requires maximum security for its information system, this would be the commercial and financial sector, which is sought to be protected significantly by the Payment Systems Act 2003.

Given the criticality of e-payment systems, it is just natural that the Bank's oversight activities are directed towards ensuring the reliability of the major payment and settlement systems and mitigating risks in these systems. That is why, in practice, the role played by the BNM is not only on systemic risk reduction, but also is extended to promoting an efficient payment and settlement infrastructures and services (Bank Negara Malaysia, 2007). This also includes fostering payment innovations and driving towards enhancing safety, security and efficiency of the payment systems. The ultimate objective is to sustain and enhance public confidence in promoting electronic payments.

Since the law is still at its infancy, there are not many court cases that can invoke judicial insights into this legislation. But sooner rather than later, one can be assured that more court cases will strengthen the position of the law in the future. In sum, for all the security safeguards provided in the Act, it is argued that Malaysian e-payment system, spearheaded by the Central Bank, is already in the right track to provide one competitive commercial infrastructure that will significantly support the country's digital economy.

References

1. Aziz, Z. A. (2001). Impact of E-Banking and E-Commerce on Central Banking Functions. Bank Negara Malaysia. Retrieved September 7, 2010, from http://www.bnm.gov.my/index.php?ch=9&pg=15&ac=34
2. Aziz, Z. A. (2003). Electronic Banking: The Way Forward. Bank Negara Malaysia from http://www.bnm.gov.my/index.php?ch=9&pg=15&ac=131 (Access:9-7-10)
3. Bank Negara Malaysia. (2007). Financial stability and payment system report. Kuala Lumpur: Bank Negara Malaysia.
4. Calder, A. & Watkins, S. (2005). IT governance: A manager's guide to data security and BS 7799/ISO 17799 (3rd edn.). London: Kogan Page.
5. *Diana Chee Vun Hsai v Citibank Bhd* [2009] 5 MLJ (Malayan Law Journal) 643
6. Labuschagne, L. (2000). A framework for electronic commerce security, Sihan Qing, Information security for global information infrastructure. Boston: Kluwer
7. Pipkin, D. L. (2000). Information security: Protecting the global enterprise. New Jersey: Prentice Hall.
8. Schneier, B. (2003). Beyond fear: Thinking sensibly about security in an uncertain world. New York: Copernicus Books.
9. Toscano, P. (2000). Toward an architecture of privacy for the virtual world. The John Marshall Journal of Computer & Information Law, 19 J. Marshall J. Computer & Info. L., 151.
10. Tryfonas, T., Gritzalis, D. & Kokolakis, S. (2000). A qualitative approach to information availability. In Sihan Qing (ed.) Information security for global information infrastructure (pp. 37-38). Boston: Kluwer Academic Publishers.
11. Whitman, M. E. & Mattord, H. J. (2005). Principles of information security (2nd edn.). Massachusetts: Course Technology.