E-TRANSACTIONS TO M-TRANSACTIONS - SERVING THE NEXT GENERATION CUSTOMERS

Jayantha Fernando
Attorney at Law, Director/ Legal Advisor, ICT Agency of Sri Lanka

1.0 INTRODUCTION

Electronic commercial transactions are very much part of our day to day life. In 2012, B2C e-Commerce sales grew 21.1% to exceed USD 1 trillion for the first time in modern history, according to global statistics published by e-Marketeer[1]. It is estimated that in 2013 e-Commerce sales will grow 18.3% to USD 1.29 trillion worldwide, with Asia Pacific region surpassing North America to become the world's No.1 market for B2C e-Commerce sales[2].

In Sri Lanka too, a similar phenomenon is visible with the exponential growth of the internet, facilitated by the increasing usage of high speed mobile broadband exceeding the traditional fixed-broadband technologies, with mobile operators offering high speed 3.5G or 4G LTE Technology. It is estimated that the mobile usage penetration has exceeded 19.5 Million in Sri Lanka[3], resulting in a common belief that there are more cellular phones and devices than tooth brushes in this country, with a significant number of users having smart-phone capability. Further, Apple or Android devices and associated applications are increasingly being used by the growing young population of the country and this technological evolution coupled with the introduction of mobile payment systems in 2012 have boosted opportunities for growth, whilst providing a readymade formula for success to those in Banking sector willing to capture such opportunities.

The purpose of this article is to provide an overview of the legal framework which facilitates both e-Transactions and m-Transactions in Sri Lanka and the safety measures available through a comprehensive information security framework, which would be applicable to the Banking sector in order to ensure greater consumer confidence when this sector transforms into a fully-fledged electronic mode. This article is in two parts, namely, Legal Considerations relevant to e-Transactions & m-Transactions (Part 1); and Information Security Safeguards and Considerations (Part 2).

---

[1] www.emarketer.com
[2] http://www.emarketer.com/Article/Ecommerce-Sales-Topped-1-Trillion-First-Time-2012/1009649
[3] Estimated at 19,533,274 connections in June 2013 (source http://www.trc.gov.lk/information/statistics.html)

PART 1
Facilitating e-Transactions and m-Transactions – Legal considerations

Evolution of Internet based commercial activity has created numerous opportunities for emerging economies to participate in International trade and other forms of commercial activity and be a part of the global economic community. There is potential for increased trade for SMEs between countries, within and outside economic regions. However, the challenges for many countries is to ensure that their legislation is abreast of international developments and have statutes in place to give legal effect to electronic equivalents of paper based documents.

When the enforceability and legal validity of electronic transactions in Sri Lanka were examined, a variety of concerns were raised. The foremost amongst them was whether **electronic records, electronic documents** and **electronic signatures** satisfy ***writing*** and ***signature*** requirements imposed by a variety of statutes and regulations. Several Sri Lankan statutes imposed certain commercial transactions to be documented in writing and signed by the parties and this posed a significant statutory barrier to the legal acceptance of electronic commercial transactions.[4]

Internationally, model laws governing the recognition and enforceability of electronic transactions have been developed by the United Nations Commission on International Trade Law ("UNCITRAL") Working Group IV on Electronic Commerce[5]. UNCITRAL successfully adopted its Model Law on Electronic Commerce[6] in 1996, the Model Law on Electronic Signatures in 2001[7] and helped formulate the UN Convention on Electronic Communications, adopted by the UN General Assembly in November 2005[8].

The UNCITRAL model law provisions have formed the basis for Electronic Transactions Legislation in several developed and emerging economies, such as USA, Ireland, Australia, Singapore, Japan, China and India.[9] However, whilst adopting the UNCITRAL model laws, many countries have taken different approaches with regard to the types of electronic signature technology[10] which would be given legal recognition.

---

[4] Eg:- The Prevention of Frauds Ordinance of 1840 specifies several types of documents to be in ***writing*** and ***signed*** as per the requirement in section 2, 4 and 18 of the Ordinance. Similar provisions exist in other statutes such as the Bills of Exchange Ord. No. 25 of 1927 and Carriage of Goods by Sea Act 1982

[5] See www.uncitral.org.

[6] See United Nations, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996

[7] See United Nations, UNCITRAL Model Law on Electronic Signatures 2001

[8] UN Convention on the Use of Electronic Communications in International Contracts – See http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

[9] Ian Walden – Regulating e-Commerce Europe in the Global economy (Vol 26 ELR No 6, 2001)

[10] For detailed working and types of e-Signatures see "**Ecommerce, Electronic Signatures & Certification Authorities**" – *Jayantha Fernando,* Bar Association of Sri Lanka, Law Journal [1999] Vol VIII Part I

The varying technology approaches[11] to legislation has caused policy issues in the International arena. Even in the South Asian region, the route to legislation has taken different approaches. Whilst some countries like Singapore and Australia have legislation based on the "technology neutral" or "minimalist approach", the Indian legislation has taken a more "technology specific" or "Prescriptive approach" and Pakistan's Legislation has followed a "Two-tier approach". The UN Electronic Communications Conventions (2005) has now sought to ensure harmonization in this area.

1.1 The Sri Lankan Electronic Transactions Act No. 19 of 2006

The Electronic Transactions Act No. 19 of 2006 of Sri Lanka was enacted by Parliament on 7th March 2006 and brought into operation with effect from 1st October 2007 (vide *Gazette Extraordinary No. 1516/25 of 27th September 2007*). The Act was prepared consequent to a decision of the Cabinet of Ministers, dated 22nd October 2004, directing that legislation be prepared with legal and policy from the ICT Agency of Sri Lanka (ICTA). In the formulation of the Act, the aforesaid UNCITRAL Model Laws as well the UN Electronic Communications Convention provided the underlying framework.

Three fundamental policy principles form the basis of the Sri Lankan Electronic Transactions Act. They are (a) *technology neutrality*, (b) functional equivalence and (c) party autonomy (*emphasis added)*. *Technology Neutrality* is ensured in the Electronic Transactions Act by not dictating the technology which would be given legal preference[12]. The definition and description of "**electronic signature**" in Section 26 ensures that the *authenticating technology* solution for use of *Electronic Signatures*, as envisaged under Section 7, should be "....incorporated in or logically associated with an electronic document, with the *intention* of authenticating and/ or *approving* the same...."[13]. Unlike statutes in some Countries, the Sri Lankan Act does not specify any technology which should be used, allowing the businesses and consumers to determine technology options based on types of usages, thus ensuring a business friendly approach to legislation.

As a follow-up to the enactment of this Act, Sri Lanka became the first country in South Asia (and one of the first three in the Asian Region)[14] to sign the UN Electronic Communications Convention (*United Nations Convention on the Use of Electronic Communications in International Contracts* of 2005) on 6th July 2006.

---

[11] For a description of "Minimalist", "Prescriptive" and "Two-tier" approach to Electronic Commerce Legislation, see "*An Analysis of International Electronic and Digital Signature Implementation Initiatives*" (A study prepared for the Internet Law & Policy Forum, September 2000, by Morrison Foerster, LLP & Steptoe and Johnson, LLP) - available at http://www.ilpf.org/groups/analysis_IEDSII.htm

[12] Section 7 of the Electronic Transactions Act. See also the definition of "Electronic Signature" in Section 26 of the Act

[13] Vide definition of "Electronic Signature" in Section 26 of the Act

[14] China and Singapore were the other three Asian Countries to the sign the Convention along with Sri Lanka

1.2 Key features of the Electronic Transactions Act

The preamble to the Act states that it is "*AN ACT TO RECOGNIZE AND FACILITATE THE FORMATION OF CONTRACTS, THE CREATION AND EXCHANGE OF DATA MESSAGES, ELECTRONIC DOCUMENTS, ELECTRONIC RECORDS AND OTHER COMMUNICATIONS IN ELECTRONIC FORM, IN SRI LANKA; AND TO PROVIDE FOR THE APPOINTMENT OF A CERTIFICATION AUTHORITY AND ACCREDITATION OF CERTIFICATION SERVICE PROVIDERS; AND TO PROVIDE FOR MATTERS CONNECTED THEREWITH OR INCIDENTAL THERETO*"

The **objectives** of the Act, as stated in Section 2, are as follows:-

(a) to facilitate domestic and international electronic commerce by eliminating legal barriers and establishing legal certainty;
(b) to encourage the use of ***reliable forms of electronic commerce***;
(c) to facilitate electronic filing of documents with government and to promote efficient delivery of government services by means of ***reliable forms of electronic communications***; and
(d) ***to promote public confidence in the authenticity, integrity and reliability*** of data messages and electronic communications. (*Emphasis added*)

The Act applies to all business and commercial transactions which are electronic in nature, other than those specific areas that have been excluded by Section 23 of the Act, namely, wills or other testamentary dispositions, powers-of-attorney, sale or conveyance of immovable property, trusts (excluding constructive, implied and resulting trusts), bills of exchange, telecommunication Licences, etc.

Section 3 of the Act gives legal recognition to electronic documents in the form of data messages, electronic records, electronic documents and other communications. The terms "***Data Messages***", "***electronic document***", "***Electronic records***" and "***Communication***" have been defined in Section 26 to give the widest possible connotation so as to legally recognize all forms of electronic transactions and communications. Section 4 provides for the legality of electronic equivalents to instruments which are required to be in writing, provided that the information contained in a data message, electronic record, electronic document or communication, is accessible for subsequent reference.

Sections 5 and 6 of the Act have a similarity to Articles 8 and 10 of the UNCITRAL Model Law on e-Commerce. Section 5 stipulates the minimum standards that must be fulfilled when information usually required to be presented or retained in its *original* form, is made available in the electronic format via data messages, electronic records, electronic documents. Section 6 describes the legal standards required to be satisfied when the retention of information under any law are to be satisfied, when such information is retained in electronic form. Therefore, document archiving in electronic or digital form is now legally valid under the Act.

Section 7 provides for the legal recognition of Electronic Signatures. The provisions contained in this Section and the associated definition of "electronic signatures", contained in Section 26, ensure that all technologies relating to electronic signatures would have legal recognition.

Section 8 describes the modalities for the use of electronic records and electronic signatures in Government institutions and statutory bodies and the procedures to be followed to give effect to such activities. Section 8(2) gives wide powers to the Minister to promulgate appropriate Regulations to transform manual activities and procedures into an electronic paperless mode by setting guidelines and procedures for such transformations in Government (on the recommendation of the respective Government institution).

The regulation making provisions are wide enough to prescribe the manner or methods of payment of any fee or charges for the filing, creation, retention or issue of any electronic record as well as the control process and procedures required in order to secure confidentiality, authenticity and, or, integrity of electronic documents, records, procurements, transactions or payments. These provisions would significantly help in the facilitation of e-Government activities in Sri Lanka, both in the electronic and mobile media.

Sections 11 to 17 of the Act provide for modalities to engage in electronic forms of contracting, including legal recognition of "offer" and "acceptance" in electronic form, enabling businesses and consumers alike to complete the contractual cycle in the electronic mode. Section 11 specifically states that a contract shall not be denied legal validity or enforceability on the sole ground that it is in electronic form. This section has the effect of affirming the application of traditional rules of contract to the electronic environment.

1.3 Facilitating e-Services and m-Transactions through Electronic Transactions Act

The provisions contained in the Electronic Transactions Act have been widely used to facilitate the deployment of several unique e-Government services. For instance the e-Revenue License System made available through "**Lanka Gate**" (accessible through www.srilanka.lk) enables a vehicle owner to renew a revenue license annually from the convenience of his home, through one single web portal. This system which is currently available for all vehicles registered in the Western Province (carrying WP letters in the Registration Number Plates), is also being replicated in the Southern and Sabaragamuwa Provinces. This end to end electronic transaction based government service enables the motor vehicle owners to receive a copy of the renewed license via email and all payments can be done electronically using credit card means. The legal basis for this entire e-Transformation process was enabled through the provisions of Section 8(1) of the Electronic Transactions Act and the Financial Regulations (FR Circular) 447/2010 prepared by a joint task force consisting of ICTA, Central Bank and Treasury officials.

In addition, the online visa application processing service (Electronic Travel Authority or ETA)[15], offered by the Department of Immigration and Emigration, is another electronic government service offered to overseas citizens visiting Sri Lanka. The payment for this service, using the Lanka Government Payment Service (LGPS), allows over 2700 online visa transactions per day, to be processed smoothly. This system also relies on the facilitation provided under the Electronic Transactions Act. Based on these successful e-Government applications, it is expected that over 30 new e-Services would be launched during the period 2013 to 2014, providing citizens with the choice of using the Internet to access Government services.

Currently, Regulations are being formulated under the Electronic Transactions Act to ensure the effectiveness of projects implemented under the e-Government Component of ICTA. For example, the Registrar General has requested ICTA to promulgate regulations to give legal effect to the new format of the birth & death certificates issued under the "*e-Civil Registry System*", with the new Sri Lanka Identification Number (SLIN). These regulations are currently under preparation and are expected to be gazetted under Section 8(2) of the Electronic Transactions Act, before the end of the year. A similar initiative is being undertaken to legitimize and give legal effect to the Revenue Licenses issued through the e-Revenue License System, currently under operation in the Western Province, which will also be completed by end of the year.

The language used in the preamble to the Act, the definitions of "***data messages***", "***electronic records***" etc and the underlying legal principles embodied in various Sections ensure that the Electronic Transactions Act can be used to legally recognize and facilitate m-Transactions as well. It is imperative to note that the term "Electronic Transactions" has been specifically left out in the Interpretations & Definitions[16] and instead only the term "***Electronic***" has been defined to mean "*information generated, sent, received or stored by electronic, magnetic, optical or similar capacities regardless of the medium*". As such, the intention of the legislature has been to ensure that its provisions are technology and platform independent.

Therefore, regardless of the method of electronic communication, the Electronic Transactions Act embodies features to recognize and facilitate the use of all mobile based commerce as well as m-Transactions.

1.4 Payment & Settlements Systems Act and Mobile Payments

In addition to the enabling features contained in the Electronic Transactions Act 2006), another significant piece of legislation having an impact on mobile activity and facilitates m-Transactions is the Payment & Settlements Systems Act No. 28 of 2005.

---

[15] Accessible via www.eta.gov.lk

[16] Section 26 of the Electronic Transactions Act No. 19 of 2006

Sri Lanka's payment instruments and their clearing and settlement processes are wide ranging. Cash is the common mode of payment, because it has finality in settlement of a transaction and is readily and legally acceptable as a medium of exchange. However, the inconvenience of carrying cash and increased security threats have encouraged the use of other payment instruments.

Non-cash payment instruments are considered to be more secure, but paper-based instruments such as cheques, drafts and travellers cheques are not so convenient or efficient instruments. In modern times, card, electronic payments and mobile payments are treated as the most convenient and safer instruments, although they too are subject to certain risks, such as credit card frauds as well as cyber security issues.

As part of the payment systems modernization program initiated by the Central Bank of Sri Lanka in 2001, a series of legal reforms were initiated to improve efficiency and increase the level of integrity in the settlement systems. Consequently, the Payment and Settlement Systems Act No. 28 of 2005 was enacted by Parliament as a comprehensive legislation governing payment, clearing and settlement systems in general and to provide the Central Bank with oversight and regulatory powers over various payment systems and money transfer service providers.

The Act empowers the Central Bank to be the authority responsible for the national payment system, which requires oversight and continuous surveillance of all payment systems to ensure their efficiency and effectiveness. Systemically important payment systems will be reviewed periodically to ensure that their design and operation meet with international standards and best practice. The Cheque Imaging and Truncation System (CITS) as well as Sri Lanka Interbank Payment System (SLIPS), operated and managed by Lanka Clear Ltd[17], functions under this framework.

Both CITS and SLIPS are dependent on the Electronic Transactions Act to provide the legislative basis for the digital certificates issued by Lanka Clear, recognized as the sector specific Certifications Service Provider for the financial sector[18].

On 31st July 2009 "*Service Providers of Payment Cards Regulations No. 1 of 2009*" were gazetted[19] under Section 43 of the Payment and Settlements Systems Act No. 28 of 2005, to better regulate the electronic payment mechanisms in the country and to protect customers as well as the service providers. Pursuant to Regulation No. 21 of the said Service Providers of Payment Cards Regulations, the Central Bank issued Mobile Payment Guidelines No.1 and 2 in August 2011.

---

[17] See www.lankaclear.com - LankaClear (Pvt) Ltd (LCPL) is owned jointly by the Central Bank and licensed commercial banks

[18] See details in Part 2 of this Article – Section 2.3

[19] Gazette Extraordinary No 1612/32 of 31st July 2009

1.5 Mobile Payment Guidelines No. 1 and 2 of 2011

The issuance of the aforesaid Mobile Payments Guidelines under Regulation 21 of *Service Providers Payment Card Regulations No. 1 of 2009*, has facilitated the issuance of South Asia's first and only Mobile Payment License. This has enabled Sri Lanka to be at the forefront in the use of mobile transactions enabling customers to have access to mobile payment methods, thus enhancing the opportunity for tremendous growth of electronic commerce in the country.

The objective of the Mobile Payment Guidelines No. 1 and 2 of 2011 in general is to promote safety and effectiveness of mobile payment services and thereby enhance user confidence. Mobile Payment Guidelines No. 1 of 2011 provide the legal process for the entire regime governing bank led mobile payment services. Customers of banks, who wish to use mobile devices to either debit or credit their accounts, pay bills and check bank balances and engage in banking transactions, would be able to do so provided that the bank concerned has entered into an arrangement with a Licensed Mobile service company to provide the said services. In providing such services using mobile devices, the bank as well as the mobile provider will be regulated under the Mobile Payment Guidelines No. 1 of 2011.

On the other hand the Mobile Payment Guidelines No. 2 of 2011 provide the legal basis for custodian account based system for non-banking service providers, such as mobile operators. The entire guidelines and the rules contained therein allow mobile operators to provide e-Cash to customers, based on physical cash deposited by the mobile company in custodian accounts operated by licensed commercial banks. The legal regime introduced through the Mobile Payments Guidelines No. 2 of 2011 was the basis for the issuance of South Asia's first mobile payment license to Dialog Axiata Plc in April 2012, allowing the said operator to issue mobile money, branded as ***eZ Cash***, that opened the market to both bank and non-bank providers and extended services to Sri Lanka's unbanked population.

Statistics have shown that in the first month since its launch in June 2012, over 300,000 customers signed up for eZ Cash. One year after launch, eZ Cash has more than 1 million customers, 20% of which are active, having conducted at least one transaction in the past 30 days. As a benchmark, in June 2012 only 16 mobile money deployments globally reported to have more than 200,000 active customers. In May 2013, 330,535 transactions were conducted through eZ Cash, exceeding Rs 435 million[20].

[20] See – "Enabling Mobile Money Policies in Sri Lanka – The rise of eZ Cash", by Simone de Castri (July 2013) http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/07/Enabling-Mobile-Money-Policies-in-Sri-Lanka-GSMA-MMU-Case-Study-July2013.pdf

1.6 Electronic Evidence Admissibility in Courts

Another aspect which impacts on consumer confidence in both e-Transactions as well as m-Transactions is the admissibility of electronic evidence pertaining to those transactions. The rules of evidence contained in the Sri Lankan Evidence Ordinance[21] were evolved long before the advent of modern electronic communications. Although the term "document" is defined in the Sri Lankan Evidence Ordinance of 1895 as well as the Indian Evidence Act of 1872 in a rather futuristic way, difficulties have arisen in the proof of an electronic transaction by reason of the necessity to produce the original document in Court.

The Evidence Ordinance expressly lays down the general rule that "documents must be proved by primary evidence".[22] The Ordinance also declares that "primary evidence means the document itself produced for the inspection of the court"[23]. This is problematic in an electronic environment. But secondary evidence is also admissible under Section 63 of the Evidence Ordinance.

A further obstacle towards the production of electronic evidence in courts is known as the "hearsay" rule. This rule, which has been described as an instance of application of the "best evidence rule",[24] is not expressly referred to in the Evidence Ordinance, but the whole structure of the Evidence Ordinance is predicated on the basis that hearsay evidence is meant to be excluded in criminal as well as civil proceedings in Courts in Sri Lanka and countries such as India, Malaysia, Singapore etc.

Thus, in *Benwell v Republic of Sri Lanka*[25] which was a habeas corpus proceeding arising in the context of an application for extradition made by the Australian Government, three computer sheets purporting to be entries of books of accounts maintained in an Australian Bank tendered in terms of Section 34 of the Ceylon Evidence Ordinance, were held to be inadmissible in evidence[26]. Further, in terms of Section 67 of the Sri Lankan Evidence Ordinance[27] proof of signature and

---

[21] Evidence Ordinance of Ceylon No. 14 of 1895(CLE 1956 Official Ed. Cap. 14) as subsequently amended

[22] § 64 of the Evidence Ordinance of Ceylon

[23] § 62 of the Evidence Ordinance of Ceylon

[24] Peiris G.L, *The Law of Evidence in Sri Lanka,* p.42. For an interesting illustration of the application of the rule see,

D.Somasiri v The Queen 75 New Law Report of Sri Lanka (NLR), 172

[25] [1978-79] 2 Sri L.R. 194

[26] Colin Thome J, of the Sri Lankan Supreme Court, in the course of his judgment made the following observation: "Computer evidence is in a category of its own. It is neither original evidence nor derivative evidence and in admitting such a document a Court must be satisfied that the document has not been tampered with. Under the law of Sri Lanka computer evidence is not admissible under any section of the Evidence Ordinance and certainly not under Section 34."

[27] Identical provisions are found in the Indian Evidence Act of 1872 as well

handwriting of a person alleged to have signed or written a document is required before a document could be used in evidence. In a decided case[28], Section 67 has been interpreted to have the effect of requiring proof of signature by reference only to handwritten signatures.

To overcome the aforesaid limitations Parliament responded by enacting two important pieces of legislation, namely, the Evidence (Special Provisions) Act No. 14 of 1995 and the Electronic Transactions Act No. 19 of 2006.

Whilst Section 4 of the Evidence (Special Provisions) Act No.14 of 1995 provides for the admissibility of information contained in contemporaneous recordings, Section 5 of the said Act provides for the admissibility of Information Produced by Computers ("Computer Evidence"). But there are restrictions on admissibility and it is important to note that the Special Provisions Act is applicable to both criminal and civil proceedings.

The Electronic Transactions Act No. 19 of 2006 on the other hand is applicable mainly to Civil and Commercial legal proceedings and expands the modalities through which electronic evidence could be admitted. This is achieved through conditions which are far more flexible than the provisions contained in the Act No. 14 of 1995.

Whilst Section 22 of the Electronic Transactions Act of 2006 excludes the application of the Evidence (Special Provisions) Act, No. 14 of 1995, Section 21(1), (2) and (3) of the Electronic Transactions Act provides for a specific regime expanding the gateway of admissibility. Thus, Sections 21(1), (2) and (3) of the Electronic Transactions Act provides for a specific regime for the admissibility of any data message, electronic document, electronic record or Communication under the said Act. The Committee stage amendment, introduced during the course of the proceedings in Parliament, ***expands the scope of admissibility under the Act*** to cover *information contained* in data messages, electronic documents and electronic records. Therefore, in terms of admissibility and proof, the Electronic Transactions Act No. 19 of 2006 has taken a giant leap, in comparison with other similar legislation in the region.

Consequently, in a judgement delivered by Honorable K. T. Chitrasiri, Judge of the Commercial High Court of Colombo[29], *photocopies* containing screen-shots of Short Message Services (commonly known as "SMS") were allowed to be marked and produced in evidence in a money recovery case. In this case, Marine Star (Pvt) Ltd., the Plaintiff sought to admit photo copies of several SMS's, copied from the messages received on a mobile phone, to prove admission of liability by the Defendant, Amanda Foods Lanka (Pvt) Ltd. Learned Counsel for the Defendant objected to all those documents being produced in evidence stating that no provision in law is available for the Court to admit the contents of such documents in evidence. However, the learned Judge after considering the aforesaid Act, permitted admissibility of the SMS transmissions.

---

[28] *Robin vs Grogan*, Per Howard CJ, (1942) 43 NLR 269, 270

[29] Presently Hon Justice of the Court of Appeal

PART 2
Enhancing User Confidence through Security for Electronic Banking Transactions

With the legal provisions enabling the transition from electronic transactions to mobile based transactions being available in Sri Lanka and the banking sector embarking on new and novel technological solutions to provide better as well as a more efficient service to the consumers, information security issues such as information piracy, data theft, and Phishing attacks and other forms of cybercrime incidents have become widely prevalent. In this scenario, it is imperative for banks and financial institutions to take measures to safeguard and protect their Information systems.

Information security by itself is becoming an expanding area of expertise. Governments together with its affiliated organizations as well as the financial sector are expanding their knowledge and expertise in this field not only to protect themselves, but to safeguard the interests of the public and the consumers so as to ensure greater user confidence in electronic as well as mobile transactions.

In Sri Lanka a combination of Technology, legal and policy measures have been initiated in the area of Information Security to address the numerous concerns arising from the widespread use of information and communications technology. This Part examines the technology as well as legislative and policy measures that have either been already implemented or will be initiated in the near future.

2.1 Technology measures to ensure security - Electronic Signatures and CSPs

In order to enhance the safety and security for electronic as well as mobile based transactions, novel and innovative technological measures are used by the industry to ensure authenticity, reliability as well as security for those transactions.

There are a range of technological solutions available in the market ranging from biometric devices to encryption software tools to digital certificates and PIN based authentication technologies. Just as much as in paper based transactions handwritten signatures or thumb prints are used for authentication of documents and to ensure integrity, digital certificates or digital signatures are commonly used to ensure integrity, authenticity and reliability for electronic transactions.

From a legal perspective the evolution of ***Electronic Signatures*** has ensured that there is a mechanism to reliably and securely prove the origin, receipt and integrity of information and also to identify the parties involved and to associate those parties with the contents of the communication. Electronic signatures could include a sophisticated biometric device, such as a fingerprint computer recognition system or even the simple entry of a typed name at the end of an email message. It has been found that digital certificates or digital signatures can achieve a much higher degree of trust than documents authenticated by placing a hand written signature.

As mentioned earlier, the Electronic Transactions Act provides for a technology neutral regime, meaning that the law does not dictate any specific legal preference for a particular type of technology for the use of electronic signatures. As such all forms of Electronic Signature technologies are recognized by the Act[30]. Further, the term "Certification Service" has been defined in the Act to mean those services connected with cryptographic services and the providers of such services are referred to as ***Certification Service Providers*** (CSPs).

Certification Service Provider (CSP) is a trusted authority which issues and manages security credentials and public key for digital signing and encryption of electronic transactions and data. As part of a Public Key Infrastructure (PKI) a CSP checks with a Registration Authority (RA) to verify information provided by a requester of a digital certificate. Once the Registration Authority (RA) has verified the requester's information, the CSP can issue a digital certificate which can be used for the purpose of signing and encrypting electronic transactions.

2.2 Certification Authority and Certification Service Providers – Legal Framework

In Sri Lanka the applicable legal provisions governing the Certification Authority and CSPs are found in Sections 18-20 of the Electronic Transactions Act[31]. The "*Technology neutral*" nature of the Electronic Transactions Act is an important policy consideration in the establishment of a Certification Authority[32] and Certification Service Providers (or sector specific CAs'[33]), within the framework of the Act.

Section 18 of the Act empowers the relevant Minister to designate any Government Department, Public Corporation, Statutory Body, Institution, or authority or any branch or unit thereof as the Certification Authority (CA) for the purposes of the Act, by an order published in the Gazette.[34] The Powers of the Certification Authority designated under Section 18 are stipulated in Section 19 and are in the nature of a "*Root CA*" or "*National CA*". Section 19 also brings Certification Service Providers (CSPs) under the control and supervision of the Certification Authority (CA) so designated. The powers also envisage setting criteria for accreditation etc.

Unlike many countries, including India, where CSPs are required to be licensed in order to engage in the business of providing certification services, the Sri Lankan legislation does not mandatorily require or insist on a licence. The *accreditation* provided in the Act is also optional. As such our legislative framework has followed a voluntary licensing approach.

---

[30] Section 7 and 26 (definition of "Electronic Signatures")
[31] Regulations relating to the operations of CSP's can also be made under Section 24 of the Act
[32] This could take the form of a "Root CA" or a" National CA" (depending on the functions carried out)
[33] Sector specific CA's such as LGN CA and Lanka Clear CA would be CSPs' under the Act
[34] Section 18(1)of the Electronic Transactions Act,

At the time the Act was brought into operation the provisions of Section 18 and 19 were specifically NOT made effective. This decision in 2007, not to bring into operation Section 18 and 20(1) of the Act, meant that Certification Service Providers (CSPs) were able to function without regulatory burdens, allowing businesses as well as consumers to check the viability of the functions of CSPs. In fact two CSPs have already started operations, covering the Banking as well as the Government sector (See Section 2.3 below).

A decision has now been made by the Government to designate ICT Agency (ICTA) as the Certification Authority (CA) under Section 18. A gazette order to this effect was recently published.[35] The decision to designate ICTA as the Certification Authority would result in an entity under ICTA, such as Sri Lanka CERT, having to undertake the day to day operations of the CA, once the governance framework is finalized. Further, steps will be taken to formalize the National Certification Authority Task Force, comprising Central Bank, Defence Ministry, TRCSL, ICTA and Lanka Clear (Pvt)Ltd.

The Certification Authority (CA) designated under Section 18 has the power to "*issue licences or any other form of authorisation* to CSPs to provide *prescribed services*". Further, it has the power to identify the criteria which will form the basis for accreditation of CSPs, the qualifications required by them, specify the procedure to be followed in granting of accreditations and hearing of appeals in the event of a refusal to grant or renew accreditation under Section 20 (Vide Section 19).

Therefore, based on the provisions of the Electronic Transactions Act, there are three types of CSPs, namely, (a) Certification Service Providers granted an authorization or license to provide "*prescribed services*", (b) Accredited Certification Service Providers (ACSPs) and (c) ordinary Certification Service Providers (CSPs) providing certification services without any licence or accreditation. With respect to all categories of CSPs, irrespective of whether or not they are licensed, authorized or accredited, the Certification Authority (CA) has the power to require CSPs to maintain such records and registers as may be prescribed by Regulations and to call for such information as may be necessary from time to time and to issue directions.

2.3 CSPs in the Banking and Government Sectors in Sri Lanka

Recognizing the need for the banking sector to have a digital certificate framework, so as to have appropriate security safeguards to instill greater customer confidence, the Central Bank of Sri Lanka mandated Lanka Clear (Pvt) Limited (LCPL) to be the financial sector CSP.

On 22nd May 2009, Lanka Clear, which has also been statutorily empowered under Section 98 of the Monetary Law to handle all interbank payments, launched ***Sri Lanka's first Certification Service Provider***. This effectively became the first financial sector specific Certificate Authority issuing Digital Certificates to commercial banks and is branded as ***Lanka SIGN***.

---

[35] Gazette Extraordinary No. 1829/29 of 24th September 2013

The legal and policy measures in connection with the establishment of this *LankaSIGN* CSP were formulated by the ICT Agency of Sri Lanka (ICTA) for the Central Bank.

In the first phase, Lanka Clear has provided application specific digital certificates to commercial banks participating in clearing applications such as Cheque imaging and truncation systems (CITS) and the Sri Lanka Inter Bank Payments Systems (SLIPS). In the second phase, *LankaSIGN* provided email and document signing certificates and SSL (Server Certificates) for any financial sector institution or their customers at a much lower cost than digital certificates purchased from foreign certification authorities. Email and document signing certificates provided by the *LankaSIGN* will benefit the general public with a technological framework having greater security for their documents and emails. The SSL certificates will provide a secure method to identify legitimate web servers.

Since the launch of *LankaSIGN* the volume of SLIPS settlements have increased by over 40%, due to the enhanced safety and security to such transactions resulting in greater user confidence in the system. With LCPL launching ***LankaSIGN***, significant achievements have been made in the payment and settlements area in Sri Lanka. The cheque imaging and truncation system eliminated the cumbersome process of physically carrying bulk cheques to the Central Clearing House. With *LankaSign* it will be possible for Lanka Clear to eliminate the paper based instruments in the long term and help Sri Lanka to engage in secure electronic based transactions and e-Commerce.

In November 2009 the 2nd Certification Services Provider was established under the auspices of ICT Agency of Sri Lanka (ICTA). This became known as the "***Lanka Government Network – Certificate Authority***" (LGN-CA). The LGN CA is designed to facilitate the digital certificate requirements of the public sector Government organizations in Sri Lanka. LGN-CA will issue digital certificates to organizations after following a specified request validation and approval procedure. A digital certificate issued by LGN-CA can be used in many software applications to provide confidentiality through encryption, authenticity and non-repudiation through digital signatures, identification and authorization through authentication protocols, as well as shared secret key distribution for secure session management, etc. Transactions on the Lanka Government Network (LGN) can use these security services to ensure privacy of users on LGN, protect the data being transmitted and ensure that transactions are in compliance with Electronic Transactions Act as well as the Computer Crimes Act.

The public key infrastructure (PKI) capabilities provided by LGN-CA, including digital certificate issuance, renewal, revocation and status verification can be used to implement access control policies to resources hosted on the LGN. The LGN-CA operating model is based on providing different types of digital certificate classes to match different Government organizational security policy levels.

Both LGN-CA[36] as well as *LankaSIGN*[37] would both take the form of ordinary Certification Service Providers (CSPs) or sector specific CAs, providing certification services without any authorization, license or accreditation. When Section 18 of the Electronic Transactions Act is brought into operation and a Certification Authority is designated, such an entity could perform the functions of a "Root CA". There is no reason to have another separate body. The technical functions of a "Root" CA may be outsourced to the national entity.

The "Sector specific CAs'" or "CSPs" (ie Lanka SIGN and LGN-CA) which have already commenced operations, may subject themselves to either a "License", "Accreditation" or an "authorization", once the Certification Authority is gazetted in the near future. As explained earlier this is ***optional*** and not mandatory.

2.4 Information Security - Legal and Policy Measures

Despite the abovementioned technology measures being adopted to enhance security and efficiency in the banking and financial sector, it has been noted that the uptake of technology by the banking customers has been significantly lower than expected. One of the reasons identified is the lack of consumer confidence in the use of new technologies adopted by the financial sector, due to the ever increasing Information Security issues. The negative publicity frequently carried in the international as well as the local electronic and prints media, have added to the woes of customers. In Sri Lanka, a combination of legal and policy measures have been adopted in the area of information security to enhance greater customer confidence.

As a legal response to the challenges in information security, Parliament enacted the Computer Crimes Act No. 24 of 2007, certified by the Speaker on 9th July 2007. In terms of substantive provisions, the Sri Lankan Computer Crime Act covers a broad range of offences, addressing "Confidentiality, Integrity and Availability" issues. All the offences under the Computer Crimes Act could fall into one of two categories, namely, (a) Computer Related crimes (where computers are used as a tool for criminal activity such as theft, fraud etc) and (b) Hacking offences – which affect integrity, availability and confidentiality of a computer system or network (also includes the introduction of viruses, worms etc).

In addition, Sri Lanka also introduced the Payment Devices Frauds Act No. 30 of 2006 to specifically deal with possession and use of unauthorized payment devices. This legislation is couched in the widest possible terms to criminalise behavior where computers or the internet is used to commit offences related to payment devices[38].

Both the Computer Crimes Act and the Payment Devices Frauds Act provide for a unique Investigation and enforcement regime.

[36] Which now functions under Lanka Gov Information Infrastructure Ltd (LGII)

[37] Operated by Lanka Clear (pvt) Ltd

[38] The term "Payment Devices" covers a wide range of instruments, including a credit card or device containing account number or other information relevant to the holder of such device etc (See Section 32 of the Act)

Some of the challenges associated with reporting and investigating cybercrime related cases are dealt with under these two Acts by providing for an "independent" group of experts to assist law enforcement agencies in the investigation of offences under the said statutes[38]. These designated experts are fully empowered and given protection under the legislation[39]. The introduction of the concept of "experts" in these Acts is to ensure that accessing of a computer is done only by skilled resources, capable of performing an efficient detection while at the same time ensuring that the computer hardware and software are not damaged.

Safeguards have also been built in order to protect the businesses and Computer systems that are being investigated[40]. This is to provide the "comfort" measures for organizations and individuals to report crimes committed under the Payment Devices Frauds Act as well as the Computer Crimes Act. Further, a special unit called the "Cyber Crime Investigations Unit" is established in the Criminal Investigations Department (CID) and an Inspector of Police is functioning as the Officer in Charge of this unit. The Inspector General of Police has certified the skills and the competency of the OIC as provided under Section 21(2) of the Act[41]. To further strengthen and enhance the ability of law enforcement to investigate offences under the Computer Crimes Act, the ICT Agency of Sri Lanka (ICTA)[42] established a Digital Forensic Lab for the "Cyber Crime Investigations Unit" of the CID[43].

It is also pertinent to note that a review of the offences under the Sri Lankan Computer Crimes Act, as well as checks and balances in the Investigation & enforcement area, would demonstrate the level of compatibility this Act has with the Council of Europe Convention on Cyber Crime[44]. The Council of Europe Convention is the only Convention on the subject of Cyber Crime which has received global acceptance. Sri Lanka has been an active participant in Council of Europe Cyber Crime related events and is expected to make a request to sign the Budapest Convention, which is available for Non-European countries to accede.

---

[38] Section 17 of the Computer Crimes Act No. 24 of 2007 & Section 8 of the Payment Devices Frauds Act No. 30 of 2006

[39] Section 18 and 28 of the Computer Crimes Act (See also Part II of the Payment Devices Frauds Act)

[40] See for instance Section 20 of the Computer Crimes Act (ordinary course of legitimate business not to be hampered in the course of investigations); and Section 24 (ensuring confidentiality of information obtained in the course of an investigation)

[41] Under Section 21(2) no police officer can access a computer for the purpose of an investigation under this Act unless the Inspector General of Police has certified such officer as a person with who possesses adequate knowledge and skill in the field of Information Communication Technology and he posses required expertise.

[42] www.icta.lk – ICTA is the Apex ICT Policy and Implementation Arm of the Government vested with powers under the Information and Communication Technology Act No. 27 of 2003

[43] See http://epaper.dailymirror.lk/epaper/viewer.aspx & http://www.lankajournal.com/2011/07/cid-to-track-computer-crimes/

[44] Also known as the Budapest Convention (2001)

2.5 Role of Sri Lanka CERT in Information Security

Many countries are increasingly relying on a broad range of resources outside the traditional Governmental law enforcement expertise to address Cyber threats and forensic issues. As such new institutional models have to be created. In this area Sri Lanka has taken unique initiatives.

In mid 2006 Sri Lanka CERT[45](Computer Emergency Readiness Team) was created to address cyber security incidents. Sri Lanka CERT is a subsidiary of ICT Agency of Sri Lanka (ICTA)[46], established with support from development partners, and runs on a private sector driven model with highly skilled incident handlers. The Board consists of a range of key stake holders such as enforcement authorities, bankers, Private sector and academia.

Sri Lanka CERT was admitted as a member of APCERT and became the first South Asian CERT to be admitted as a member of FIRST[47] in 2008. In just a few years Sri Lanka CERT has responded effectively to the Cyber Crime forensic issues. Due to the requests from law enforcement agencies, Sri Lanka CERT started offering digital forensics as a service for law enforcement since the third quarter of 2008. Sri Lanka CERT also carries out forensic investigations for other government establishments in Sri Lanka.

Sri Lanka CERT handles about 200 Facebook and webmail account hijacking incidents on an average per month, of which 70 percent relate to creation of fake accounts, 26 percent are complaints relating to hacked accounts, whilst around 7 percent harassment complaints. They also handle technical forensic investigations and incidents relating to phishing attacks on banking and finance industry. In addition, they carry out consultancy work for application and network security vulnerability assessments for e-government applications that are being rolled out by the ICTA. Sri Lanka CERT has also been designated as the National CERT.

2.6 Information Security Policy Measures – Baseline Security Standards for Banks

In addition to the aforesaid legal and policy measures it is imperative that key institutions, such as Banks and financial sector organizations, collaborate closely with other agencies such as Sri Lanka CERT and have a common framework to manage and mitigate information security incidents.

To address these issues the Central Bank of Sri Lanka (CBSL) along with the Sri Lanka Banks Associations (SLBA) and Sri Lanka CERT (a subsidiary of ICTA) have worked together to establish a common baseline security standard, based on a globally recognized ISO 27000 series of international standards for Information Security.

---

[45] www.slcert.gov.lk
[46] www.icta.lk
[47] www.FIRST.org

These standards once adopted will be known as the "***Banking and Finance Industry Baseline Security Standards***". These standards will be mandated shortly by CBSL and will be managed on behalf of CBSL by the Banking and Financial Sector Computer Security Incidence Response Team (BANK CSIRT), to be hosted by Lanka Clear.

2.7 Bank CSIRT

Bank CSIRT (Computer Security Incident Readiness Team) is being established at Lanka Clear as a centralized body to coordinate security efforts within the banking and finance sector, and as an entity steered and funded by the banks, it will have the prime responsibility and accountability towards them. This is a joint initiative of the Central Bank of Sri Lanka and the Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), which is the Centre for Cyber Security in Sri Lanka that has been mandated to protect the nation's information infrastructure and to coordinate protective measures against, and responses to Cyber Security threats and vulnerabilities.

Bank CSIRT is planning to offer the following five very unique Information Security services:-

(a) Formulating and implementing Baseline Security Standards (BSS), based on ISO Standards.

In order to address gaps in security capabilities among banking & financial institutes, the Central Bank of Sri Lanka (CBSL), the Sri Lanka CERT and the Sri Lanka Banks Association (SLBA) worked towards the establishment of a common baseline security standard, based on the globally accepted ISO27001 standard for information security, which would be managed on behalf of the CBSL by Bank CSIRT, but subject to supervision by CBSL.

Establishment of a minimum acceptable information security posture for financial institutions is the primary benefit. Standardization of Information security policies across the entire spectrum of member banks and financial institutes, including the smaller banks that may not have dedicated Information Security staff. Other internationally recognized standards such as PCI-DSS will be incorporated in to future versions of BSS, as and when they are mandated.

(b) Sharing of Desensitized Fraud, Cyber Crime incidents and threats among Bank CSIRT members.

Bank CSIRT members.will share threat and incident intelligence with Bank CSIRT. This information will be packaged to ensure all confidential data is removed. As a result, all Banks CSIRT members will have information on how to take preventive action against such threats. Additionally, if a member Bank is affected by such an incident, it will now take less time to recover.

(c) Vulnerability, Advisory and Informational Alerts

Alerts such as Security Vulnerability Alerts, Security Advisory Alerts and Informational Alerts will be sent by Bank CSIRT. These Alerts will be obtained and filtered from information originating from over 400 centres belonging to the Forum for Incident Response and Security Teams (FIRST), where Sri Lanka CERT is an active member. Bank CSIRT members do not need to have their own dedicated Information Security team to carry out research on such vulnerabilities and threats. Severity levels and Patch timeframes will be common to all the Bank CSIRT members

(d) Registration of Certified 3rd Party Service Providers

As part of the Bank CSIRT service offering, Sri Lanka CERT will evaluate and accredit Information Security service providers operating in Sri Lanka after conducting an extensive audit based on ISO standards. Based on Sri Lanka CERT's certification, Bank CSIRT members will be provided with a list of certified Information Security service providers from whom services can be obtained.

(e) Incident Response

Bank CSIRT will provide first and second level incident response services to Bank CSIRT members. An incident which needs to be coordinated with CERT's from foreign countries, law enforcement agencies, and legal bodies will be escalated to Sri Lanka CERT as part of the service.

All reported incidents will be processed according to the Service Level Agreement timeframes. Incidents such as active phishing sites which needs to be coordinated with other country specific CERT's (US-CERT, JPCERT, CERT Australia etc) or specific Law enforcement agencies (CID, Interpol) or legal bodies (Attorney General's Department) will be escalated to Sri Lanka CERT and will be coordinated until the incident is resolved.

In view of the recent media hype about the looming cyber security threat affecting Sri Lanka's own IT systems, Banks and financial institutions may need to seriously consider joining Bank CSIRT in order to protect themselves. With a large number of technology savvy customers depending on electronic transactions for their day to day work, the ability of Banks and financial systems to respond individually or collectively to Cyber Crime, threats and incidents would actually determine the level of confidence customers would have in the sector. Collective response by Banks to cyber threats and other related incidents through the Bank CSIRT framework would ensure that the Banking sector as a whole is protected from vulnerabilities looming in the Cyber world.

CONCLUSIONS

The legislative framework in Sri Lanka has kept pace with developments in technology to an extent where all forms of electronic as well as mobile based transactions are legally valid. The Electronic Transactions Act No. 19 of 2006 formulated on the basis of UNCITRAL legal provisions provides a technology neutral framework ensuring legal validity to all forms electronic and mobile transactions.

In addition, the advancements made in the sphere of Payment and Settlement Systems legal reforms have resulted in faster and more efficient inter-bank fund transfers. The launch of mobile cash in 2012 (eZ Cash) has provided a boost to the entire e-Commerce industry, giving consumers greater fund transfer options than ever before.

Therefore, it is submitted that both the technological and policy ingredients required for our economy to transform itself to a knowledge based economy, are present in Sri Lanka. The ability of Banks and financial institutions to respond to customer demands by providing both electronic and mobile based banking services will not only determine their ability to capture the mobile savvy younger generation, but also determine whether or not they have a true formula for success.

However, the extent to which consumers/ customers of Banks as well as Mobile operators would embrace new and innovative technology options for banking transactions would, to a great extent, depend on the level of user confidence created by these institutions by having appropriate safeguards. In this context a number of technology as well as legal & policy safeguards are available in Sri Lanka. But the ability of Banks and Financial institutions to find ways to work together to reach common ground, in order to respond adequately to cyber threats and challenges through frameworks such as Bank CSIRT, would be the factor that would determine the level and extent to which consumers would have greater confidence in e-Transactions and m-Transactions.