

## E-COMMERCE

### A SLOW AWAKENING

Despite numerous government initiatives, Thailand still lacks the proper infrastructure and legal framework necessary to support e-commerce. As a result, most businesses operating in this country have been unable to take full advantage of the opportunities it offers.

However, changes should take place in the near future with the adoption of specific laws related to e-commerce and the forthcoming telecommunications sector deregulation, which will bring security for businesses and users, reduced tariffs, and higher speed connections.

On October 18, 2001, the Thai Parliament gave its final endorsement to the Electronic Transactions Act which came into effect on April 3, 2002. Furthermore, on June 10, 2007, following a draft that had been originally presented for discussion since 2002, the Thai Government enacted the Act on Computer-Related Offenses which came into effect on July 18, 2007.

In addition to the Electronic Transactions Act and Act on Computer-Related Offenses, there are still three e-commerce laws on the agenda—the Universal Access Bill, the Data Protection Bill, and the Electronic Funds Transfer Law. The draft Data Protection Bill is being reviewed by the Council of State, while the Electronic Funds Transfer and Universal Access Laws are still in the drafting stage.

The government has been quite active recently in addressing Thailand's lack of adequate measures to support the development of electronic commerce.

In addition to addressing the lack of an adequate legal framework and the slow implementation of the Telecommunications Master Plan, the government is also working on increasing the number of IT specialists in Thailand. In that respect, the government will adopt measures to improve the IT education system and also open up the sector to highly skilled foreign IT specialists. With this in view, visa and work permit requirements for such specialists may be eased in the near future.

The Board of Investment recently announced its intention to increase existing incentives (tax and other incentives) for e-commerce businesses in order to encourage the establishment of regional offices in Thailand.

The IT 2010 Policy will also assist Thailand in moving toward an IT knowledge-based economy by focusing on five main issues: e-industry, e-commerce, e-government, e-education, and e-society.

### ELECTRONIC TRANSACTIONS ACT

The Electronic Transactions Act (ETA) shall govern both civil and commercial transactions made electronically with few exceptions, as shall be prescribed by a Royal Decree to be adopted pursuant to the ETA, and provided that it shall not override laws and regulations intended for consumer protection.

Before its adoption, electronic signatures were not yet recognized as valid and binding signatures. The ETA took care of that problem, in addition to providing the legal framework necessary to support electronic transactions and documents.

The ETA, which is based on the UN Model Law on Electronic Commerce (1996) and on Electronic Signatures (2001), is divided into six chapters.

### Chapters 1 and 2—Electronic Transactions and Electronic Signatures

Chapters 1 and 2 were mainly inspired by the UN Models with a few substantial changes. Chapter 1 embodies the fundamental principle whereby data messages (i.e., information generated, sent, received, stored, or processed electronically, such as EDI, e-mail, telegram, telex, or facsimile) shall be treated as paper documents. It also addresses the issues of electronic signatures and documents, and provides for their legal effectiveness, as well as their admissibility as evidence before Thai courts.

The ETA is “technology neutral” in that it does not require signatures to be made or documents to be retained through the use of a specific technology.

Under the ETA, a document shall be deemed signed if the method used can identify the originator and confirm that the originator approved the content of the document. The method used must be appropriately “reliable” with due regard for all circumstances, including any agreement between the originator and the addressee. Like the UN Model, the ETA states that an electronic signature shall be deemed reliable if “. . . (1) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person; (2) the signature creation data were, at the time of signing, under the control of the signatory and of no other person; (3) any alteration to the electronic signature made after the time of signing is detectable; and (4) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.”

Similarly, electronic documents may be presented or retained as originals, provided that a “reliable” method is used for assuring the integrity of the information and that such information can be subsequently displayed.

The ETA allows for different methods of electronic signatures or storage, provided that their reliability can be demonstrated. While such technological neutrality is important in order to keep the ETA from being outdated by new technologies, it does bring some uncertainty, as users must first assess the legal effectiveness of a specific method. With a view to bringing security, the Thai legislature added a provision whereby electronic transactions made in accordance with such security procedure, as shall be prescribed by a Royal Decree, shall be deemed reliable. At the time of this writing, the Royal Decree was still in the drafting stage.

Chapters 1 and 2 also contain sections on contract formation and validity; attribution of data messages; retention of documents; acknowledgment of receipt; time and place of dispatch/receipt of data messages; admissibility of data messages as evidence before Thai courts; rules of conduct for the signatory, the certification service provider, and the relying party; and the recognition of foreign signatures and certificates.

### Chapter 3—Businesses Providing Services Related to Electronic Transactions

Under the ETA, there are no licensing requirements for electronic transaction–related service providers. A person has the right to provide any such services without having to notify or obtain a specific license from the authority concerned. However, a Royal Decree may be issued requiring a service provider to notify, register, or obtain a license before providing electronic transaction–related services.

#### Chapter 4—Electronic Transactions with the Public Sector

Electronic transactions made with the public sector in accordance with such rules and procedures as shall be prescribed by a Royal Decree would fall under the application of the ETA.

#### Chapter 5—Electronic Transactions Commission

An Electronic Transactions Commission is to be established pursuant to Chapter 5 of the ETA with the duty, among others, to make recommendations to the Council of Ministers for the promotion and development of electronic transactions. The Commission shall also monitor the operations of businesses providing services related to electronic transactions and recommend the adoption of Royal Decrees under the ETA.

The Commission shall be composed of 12 members and chaired by the Minister of Science and Technology. The National Electronic and Computer Technology Center of the National Science and Technology Development Agency shall act as secretariat.

#### Chapter 6—Penalties

Businesses that provide services related to electronic transactions without notifying, registering, or obtaining the required license as shall be prescribed by a Royal Decree are subject to imprisonment for a term not exceeding one or two years and/or a fine not exceeding THB 100,000 or THB 200,000, depending on the offense. Administrative fines not exceeding THB 1 million or THB 2 million, depending on the offense, can also be imposed by the Commission for failure to comply with rules prescribed by Royal Decrees or by the Commission. Such penalties may be applied not only to the enterprises, but also to their managing directors, managing partners, or persons in charge of operations, unless the offense was committed without their knowledge or connivance.

The new Royal Decree Governing Control and Supervision of Electronic Payment Service Business went into effect on January 14, 2009. The general purpose of this new law is to introduce oversight of the electronic debit service business which, prior to this Decree, was not fully addressed by finance company, credit card, or banking regulations.

Thailand's government is pointed in the right direction to ensure that Thailand's e-commerce will be on a par with that of other countries. However, while other countries have charged forward in the protection and development of their e-commerce, Thailand has been plagued by one delay after another. Nevertheless, the next few years should witness significant changes with the new government's commitment to increasing Thailand's competitiveness in the IT sector.

#### ACT ON COMPUTER-RELATED OFFENSES

The Act on Computer-Related Offenses (ACRO) sets out various types of virtual criminal offenses. Provided below is a general overview of the new law and a commentary on significant issues which have been the subject of public questions and discussion.

In the past Thai prosecutors were forced to apply general rules of trespass and wrongful conduct to prosecute computer hackers, which oftentimes proved difficult. Now the ACRO broadly outlaws any kind of computer hacking, whether or not there is any resulting damage or modification caused to the system being hacked.

Sharing of passwords and dissemination of hacking tools/techniques can also potentially lead to criminal liability, even if the person who does so has not himself used such passwords or techniques

to effect an unlawful act.

Intercepting data without authorization is also a crime, regardless of whether such data is intercepted through hacking of protected systems or not.

An anti-spam section prohibits the transmission of data or e-mail (a) in such a manner that causes nuisance to others (b) by using a concealed or fabricated source. In other words, even transmissions which cause nuisance may not create criminal liability if their source is properly identified.

The ACRO makes it a criminal act to post information which is either (a) false, (b) threatens the national security of Thailand or causes a public panic, (c) constitutes an act of terrorism, or (d) contains pornography. This section is directed primarily at users of Internet services who post such information on public Web sites.

Service providers will be relieved to find that they are not liable for any of the above posted through their websites provided they themselves do not “willfully aid or allow” such false and/or unlawful data to be posted.

Posting altered images to defame or expose persons to public ridicule or embarrassment also incurs criminal liability. Service providers are not expressly excused from liability in these cases.

Penalties provided by the ACRO include fines up to THB 500,000 and/or jail time up to 20 years according to the severity of the crime.

Unlike other Thai laws, the ACRO is expressly given extraterritorial jurisdiction—applying not only to such unlawful acts conducted within Thailand but also to any act conducted outside Thailand which are either conducted by Thai citizens (regardless of effect within Thailand) or which affect the Thai government or any Thai entity.

The ACRO expressly provides powers of search and seizure to the competent officials enforcing the law and addresses the procedures for use of such powers. Officials may request computer traffic data and/or user identification data from service providers without the need to obtain a prior court order provided they have “reasonable grounds” to suspect the commission of a crime.

For broader data searches and equipment seizures, reasonable grounds must be presented to the courts as part of an application for a search/seizure warrant. The courts must consider the application on an expedited basis and issue an appropriate search and seizure warrant before the officials can effect same. This creates a check on government searches and seizures similar to that of Western nations which require some level of proof before such searches and seizures can be conducted. Whether the Thai courts will be strict or lax in requiring “reasonable grounds” before authorizing a search is something to be seen.

Section 238 of the 1997 Constitution of Thailand provided that “[i]n a criminal case, a search in a private place shall not be made except where an order or a warrant of the Court is obtained or there is a reasonable ground to search without an order or a warrant of the Court as provided by law.” Contrary to some public criticisms, searches mandated by the ACRO do not create any new power that goes beyond what was provided in the 1997 Constitution.

The ACRO provides that failure to comply with an official’s inquiries would result in a fine of up to THB 200,000 per offense, plus a fine of up to THB 5,000 for each day of noncompliance. However, if a party can show that the officials did not have reasonable grounds to make an inquiry and/or obtain a warrant, such penalties would also necessarily fail.

Moreover, notwithstanding the said penalties, the enforcement provisions of the new law cannot

supersede a person's right against self-incrimination as provided under the 2007 Constitution. Still, third parties such as ISPs who are asked to provide data on their subscriber's identification and usage may be obliged to comply with inquiries supported by reasonable grounds.