S. No. 1902 H. No. 9971 / 96 OG No. 48, 7675 (Nov. 27, 2000) ; 12 VLD 2d 1

[REPUBLIC ACT NO. 8792, June 14, 2000]

AN ACT PROVIDING FOR THE RECOGNITION AND USE OF ELECTRONIC COMMERCIAL AND NON-COMMERCIAL TRANSACTIONS, PENALTIES FOR UNLAWFUL USE THEREOF, AND OTHER PURPOSES

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

PART I

SHORT TITLE AND DECLARATION OF POLICY

Section 1. *Short Title.* - This Act shall be known and cited as the "Electronic Commerce Act."

Sec. 2. *Declaration of Policy*. - The State recognizes the vital role of information and communications technology (ICT) in nation-building; the need to create an information-friendly environment which supports and ensures the availability, diversity and affordability of ICT products and services; the primary responsibility of the private sector in contributing investments and services in ICT; the need to develop, with appropriate training programs and institutional policy changes, human resources for the information age, a labor force skilled in the use of ICT and a population capable of operating and utilizing electronic appliances and computers; its obligation to facilitate the transfer and promotion of technology; to ensure network security, connectivity and neutrality of technology for the national benefit; and the need to marshal, organize and deploy national information infrastructures, comprising in both communications network and strategic information services, including their interconnection to the global information networks, with the necessary and appropriate legal, financial, diplomatic and technical framework, systems and facilities.

PART II

ELECTRONIC COMMERCE IN GENERAL

Chapter I — GENERAL PROVISIONS

SEC. 3. *Objective.* - This Act aims to facilitate domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information through the utilization of electronic, optical and similar medium, mode, instrumentality and technology to recognize the authenticity and reliability of electronic data messages or electronic documents related to such activities and to promote the universal use of electronic transactions in the government and by the general public.

SEC. 4. *Sphere of Application*. - This Act shall apply to any kind of electronic data message and electronic document used in the context of commercial and non-commercial activities to include domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information.

SEC. 5. *Definition of Terms.* - For the purposes of this Act, the following terms are defined, as follows:

a. "Addressee" refers to a person who is intended by the originator to receive the electronic data message or electronic document, but does not include a person acting as an intermediary with respect to that electronic data message or electronic document.
b. "Computer" refers to any device or apparatus singly or interconnected which, by electronic, electro-mechanical, optical and/or magnetic impulse, or other means with the same function, can receive, record, transmit, store, process, correlate, analyze, project, retrieve and/or produce information, data, text, graphics, figures, voice, video, symbols or other modes of expression or perform any one or more of these functions.
c. "Electronic data message" refers to information generated, sent, received or stored by electronic, optical or similar means.
d. "Information and Communications System" refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic data message or electronic document.
e. "Electronic signature" refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document.
f. "Electronic document" refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.
g. "Electronic key" refers to a secret code which secures and defends sensitive information that crosses over public channels into a form decipherable only with a matching electronic key.
h. "Intermediary" refers to a person who in behalf of another person and with respect to a particular electronic data message or electronic document sends, receives and/or stores or provides other services in respect of that electronic data message or electronic document.
i. "Originator" refers to a person by whom, or on whose behalf, the electronic document purports to have been created, generated and/or sent. The term does not include a person acting as an intermediary with respect to that electronic document.
j. "Service provider" refers to a provider of-

i. Online services or network access, or the operator of facilities therefor, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among points specified by a user, of electronic documents of the user's choosing; or
ii. The necessary technical means by which electronic documents of an originator may be stored and made accessible to a designated or undesignated third party.

Such service providers shall have no authority to modify or alter the content of the electronic document received or to make any entry therein on behalf of the originator, addressee or any third party unless specifically authorized to do so, and who shall retain the electronic document in accordance with the specific request or as necessary for the purpose of performing the services it was engaged to perform.

CHAPTER II

Legal Recognition of Electronic Data Messages and Electronic Documents

SEC. 6. *Legal Recognition of Electronic Data Message.* -Information shall not be denied validity or enforceability solely on the ground that it is in the form of an electronic data message purporting to give rise to such legal effect, or that it is merely incorporated by reference in that electronic data message.

SEC. 7. *Legal Recognition of Electronic Documents*. - Electronic documents shall have the legal effect, validity or enforceability as any other document or legal writing, and -

a. Where the law requires a document to be in writing, that requirement is met by an electronic document if the said electronic document maintains its integrity and reliability and can be authenticated so as to be usable for subsequent reference, in that -
    i. The electronic document has remained complete and unaltered, apart from the addition of any endorsement and any authorized change, or any change which arises in the normal course of communication, storage and display; and
    ii. The electronic document is reliable in the light of the purpose for which it was generated and in the light of all relevant circumstances.
b. Paragraph (a) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the document not being presented or retained in its original form.
c. Where the law requires that a document be presented or retained in its original form, that requirement is met by an electronic document if-
    i. There exists a reliable assurance as to the integrity of the document from the time when it was first generated in its final form; and
    ii. That document is capable of being displayed to the person to whom it is to be presented: *Provided,* That no provision of this Act shall apply to vary any and all requirements of existing laws on formalities required in the execution of documents for their validity.

For evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws.

This Act does not modify any statutory rule relating to the admissibility of electronic data messages or electronic documents, except the rules relating to authentication and best evidence.

SEC. 8. *Legal Recognition of Electronic Signatures.* - An electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if the signature is an electronic signature and proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, existed under which -

a. A method is used to identify the party sought to be bound and to indicate said party's access to the electronic document necessary for his consent or approval through the electronic signature;
b. Said method is reliable and appropriate for the purpose for which the electronic document was generated or communicated, in the light of all circumstances, including any relevant agreement;
c. It is necessary for the party sought to be bound, in order to proceed further with the transaction, to have executed or provided the electronic signature; and
d. The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.

SEC. 9. *Presumption Relating to Electronic Signatures.* - In any proceedings involving an electronic signature, it shall be presumed that,

a. The electronic signature is the signature of the person to whom it correlates; and
b. The electronic signature was affixed by that person with the intention of signing or approving the electronic document unless the person relying on the electronically signed electronic document knows or has notice of defects in or unreliability of the signature or reliance on the electronic signature is not reasonable under the circumstances.

SEC. 10. *Original Documents.* -

1. Where the law requires information to be presented or retained in its original form, that requirement is met by an electronic data message or electronic document if:
    a. the integrity of the information from the time when it was first generated in its final form, as an electronic data message or electronic document is shown by evidence *aliunde* or otherwise; and
    b. where it is required that information be presented, that the information is capable of being displayed to the person to whom it is to be presented.
2. Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.
3. For the purposes of subparagraph (a) of paragraph (1):
    a. the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

b. the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

SEC. 11. *Authentication of Electronic Data Messages and Electronic Documents.* - Until the Supreme Court by appropriate rules shall have so provided, electronic documents, electronic data messages and electronic signatures, shall be authenticated by demonstrating, substantiating and validating a claimed identity of a user, device, or another entity in an information or communication system, among other ways, as follows:

a. The electronic signature shall be authenticated by proof that a letter, character, number or other symbol in electronic form representing the persons named in and attached to or logically associated with an electronic data message, electronic document, or that the appropriate methodology or security procedures, when applicable, were employed or adopted by a person and executed or adopted by such person, with the intention of authenticating or approving an electronic data message or electronic document;
b. The electronic data message or electronic document shall be authenticated by proof that an appropriate security procedure, when applicable was adopted and employed for the purpose of verifying the originator of an electronic data message or electronic document, or detecting error or alteration in the communication, content or storage of an electronic document or electronic data message from a specific point, which, using algorithm or codes, identifying words or numbers, encryptions, answers back or acknowledgement procedures, or similar security devices.

The Supreme Court may adopt such other authentication procedures, including the use of electronic notarization systems as necessary and advisable, as well as the certificate of authentication on printed or hard copies of the electronic documents or electronic data messages by electronic notaries, service providers and other duly recognized or appointed certification authorities.

The person seeking to introduce an electronic data message or electronic document in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic data message or electronic document is what the person claims it to be.

In the absence of evidence to the contrary, the integrity of the information and communication system in which an electronic data message or electronic document is recorded or stored may be established in any legal proceeding-

a. By evidence that at all material times the information and communication system or other similar device was operating in a manner that did not affect the integrity of the electronic data message or electronic document, and there are no other reasonable grounds to doubt the integrity of the information and communication system;
b. By showing that the electronic data message or electronic document was recorded or stored by a party to the proceedings who is adverse in interest to the party using it; or
c. By showing that the electronic data message or electronic document was recorded or stored in the usual and ordinary course of business by a person