Legal Supplement Part C to the "Trinidad and Tobago Gazette", Vol. 50, No.55, 21st April, 2011

No. 5 of 2011

First Session Tenth Parliament Republic of Trinidad and Tobago

HOUSE OF REPRESENTATIVES

BILL

AN ACT to give legal effect to electronic documents, electronic records, electronic signatures and electronic transactions

PRINTED BY THE GOVERNMENT PRINTER, PORT-OF-SPAIN
REPUBLIC OF TRINIDAD AND TOBAGO—2011

THE ELECTRONIC TRANSACTIONS BILL, 2011

Arrangement of Clauses

PART I

PRELIMINARY

Clause

PART II

REQUIREMENT FOR LEGAL RECOGNITION

PART III

CONTRACT FORMATION AND DEFAULT PROVISION

PART IV

ELECTRONIC SIGNATURE

PART V

ELECTRONIC AUTHENTICATION SERVICE PROVIDERS

PART IX

CONTRAVENTION AND ENFORCEMENT

PART X

MISCELLANEOUS

THE ELECTRONIC TRANSACTIONS BILL, 2011

Explanatory Note

(These notes form no part of the Bill but are intended only to indicate its general purport)

The Bill seeks to provide for the transfer of information and records by electronic means.

The Bill would contain ten Parts and sixty-six sections.

Part I of the Bill would comprise the preliminary clauses and would contain seven clauses.

Clause 1 of the Bill would contain the short title.

Clause 2 of the Bill would provide for the interpretation of certain words and phrases.

Clause 3 of the Bill would bind the State.

Clause 4 of the Bill would provide that a public body is not required to accept or issue any document.

Clause 5 of the Bill seeks to set out the purposes and construction of the Act.

Clause 6 of the Bill would make the Act inapplicable where the law requires the writing, signatures or original documents in certain circumstances. These include the making, execution or revocation of a will, the conveyance or transfer of any interest in real property, the creation, performance or enforcement of an indenture of trust or power of attorney, the production of documents relating to immigration, citizenship or passport matters; or the issuance, recognition and endorsement of negotiable instruments.

Clause 7 of the Bill would provide that a person who uses, provides, accepts or retains information or a document is not required to do so in electronic form. Subclause (2) would provide that the past conduct of the parties to a transaction may infer consent to the use, provision, acceptance or retention of information, data messages or records in electronic form.

Part II of the Bill would set out the requirements for legal recognition and would contain eleven clauses.

Clause 8 of the Bill would provide that an electronic record or information under this Act shall not be denied legal effect simply because it is in electronic form.

Clause 9 of the Bill provides that where there is a legal requirement that information, a data message or a record be in writing, the requirement is satisfied by an electronic record if the electronic record data is accessible and capable of being retained for subsequent reference.

Clause 10 of the Bill would provide that where there is a legal requirement that information, a data message or a record be provided or sent in writing, that requirement is met where the information is provided or sent in electronic form and is capable of being retained.

Clause 11 of the Bill would provide that where there is a legal requirement that information, a data message or a record be in a specific non-electronic form, that requirement is met where the information, a data message or record when transferred in electronic form contains substantially the same information and is accessible so as to be used for subsequent reference.

Clause 12 of the Bill would provide that where there is a legal requirement that information, data messages or records be presented in its original form, that requirement is satisfied where the information, data messages or records are in electronic form if there is a reliable assurance as to the integrity of the information, data messages or records and where information, data messages or records are accessible and capable of retention for subsequent reference. It would also provide that the criteria for assessing integrity shall be whether the information, data messages or records have remained complete and unaltered apart from the introduction of any change that arise in the normal course of communication, storage and display.

.

Clause 13 of the Bill would provide that where there is a legal requirement that certain information, data messages or records be retained, that requirement is met by retaining such information, data messages or records in electronic form.

Clause 14 of the Bill sets out the circumstances under which information, data messages or records in electronic form are not capable of being retained.

Clause 15 of the Bill would provide that where there is a legal requirement that one or more copies of information, a data message or record be provided to a single addressee at the same time, that requirement is satisfied by providing a single copy in electronic form.

Clause 16 of the Bill would provide that an electronically signed data message is as valid, enforceable and effective as a non-electronic signature.

Clause 17 of the Bill would set out the evidential weight that is to be attached to an electronic record.

Part III of the Bill would set out the requirements for contract formation and default provisions and would contain ten clauses.

Clause 18 of the Bill would provide for the recognition of the notarization of documents electronically.

Clause 19 of the Bill would provide for contract formation in an electronic environment and the mere fact that the contract is formed electronically does not affect its enforceability.

Clause 20 of the Bill would provide for an offer or the acceptance of an offer or any other matter that is material to the operation or formation of a contract to be expressed by means of information or a record in electronic form.

Clause 21 of the Bill would provide for the legal validity and enforceability of contracts formed through the involvements of electronic agents.

Clause 22 of the Bill would provide that an electronic contract is voidable where a material error is made, no opportunity is given to prevent or correct the error, notification of the error takes place, no reasonable steps are taken to correct the error, material benefit or value is not received and where consideration is received and returned or disposed of. This section does not apply to electronic auctions.

Clause 23 of the Bill would provide for an electronic data message or record to be attributed to a particular person.

Clause 24 of the Bill would set out the time when an electronic data message or record is considered to be sent.

Clause 25 of the Bill would set out the time of receipt of information or data message in electronic form.

Clause 26 of the Bill would provide for the place of sending and receipt of information or a record in electronic form.

Clause 27 of the Bill would provide where the place of business governing the electronic transaction is located.

Clause 28 of the Bill would provide that where there is no place of business of the originator or addressee of a communication, the habitual residence of the originator or addressee is the relevant address for sending and receipt of communications.

Part IV of the Bill would set out the requirements in respect of electronic signatures and would contain four clauses.

Clause 29 of the Bill would provide that parties may agree as to the particular method or form of electronic signature to be used.

Clause 30 of the Bill would set the minimum standards of reliability and integrity for legally required signatures when an electronic signature is used.

Clause 31 of the Bill would set out the criteria for the reliability and integrity of electronic signatures.

Clause 32 of the Bill would provide that an electronic signature that is associated with an accredited electronic authentication product is deemed to satisfy the requirements for reliability and integrity.

PART V of the Bill would deal with electronic authentication service providers and would contain seventeen clauses.

Clause 33 of the Bill provides for the prohibition of a person to issue an accredited electronic authentication product to the public unless he is registered as an Electronic Authentication Service Provider under this Act.

Clause 34 of the Bill would set out the application requirements for registration as an accredited Electronic Authentication Service Provider. This clause will also empower the Minister to make regulations with respect to registration.

Clause 35 of the Bill would set out the requirements for an Electronic Authentication Service Provider that issues accredited electronic authentication products.

Clause 36 of the Bill would empower the Minister or designated authority to grant registration to applicants who have previously been accredited and who have also met the requirements set out in clause 35 or who having no prior accreditation has met the requirements of clauses 34 and 35.

Clause 37 of the bill would empower the Minister to recognize accredited electronic authentication products which are issued outside Trinidad and Tobago.

Clause 38 of the Bill would require the Minister to maintain a public registry of Electronic Authentication Service Providers.

Clause 39 of the Bill would require the Electronic Authentication Service Provider to annually provide an updated notification of compliance.

Clause 40 of the Bill would empower the Minister to conduct audits on Electronic Authentication Service Providers.

Clause 41 of the Bill would require the Electronic Authentication Service Provider to co-operate or offer reasonable assistance during an audit.

Clause 42 of the Bill would provide for the confidentiality by any person performing duties or functions in the administration or enforcement of this Act.

Clause 43 of the Bill would empower the Minister to deal with an Electronic Authentication Service Provider who no longer meets the requirements to issue accredited electronic authentication products.

Clause 44 of the Bill would permit an Electronic Authentication Service Provider to request a particular signatory to indicate in the relevant electronic authentication product a pseudonym instead of the signatory's name.

Clause 45 of the Bill would require an Electronic Authentication Service Provider to ensure the operation of a prompt and secure directory of holders of electronic authentication products and to secure an immediate revocation service that makes it possible to check whether an accredited electronic authentication product was revoked, the validity period of the accredited electronic authentication product and whether the accredited electronic authentication product contains any limitations.

Clause 46 of the Bill would provide for the revocation of an electronic authentication product by an Electronic Authentication Service Provider when a request is made for such revocation by the signatory or if other circumstances warrant a revocation. It also requires that the date and time of the revocation of an electronic authentication product be determined precisely.

Clause 47 of the Bill would set out the liability of an Electronic Authentication Service Provider for damages or loss caused to anyone relying on an accredited electronic authentication product where the damage or loss is due to the Electronic Authentication Service Provider not meeting the requirements of section 31 or 35. This clause also applies to an Electronic Authentication Service Provider who guarantees that the electronic authentication product of another service provider is accredited.

Clause 48 of the Bill would provide that an Electronic Authentication Service Provider who issues an accredited electronic authentication product may be exempted from liability if the provider can show that the injury or loss arising was not caused by its own negligence. Subclause (2) also exempts the Electronic Authentication Service Provider from liability where the accredited electronic authentication product is in violation of any limitations of use of transaction. Subclause (3) applies to an accredited electronic authentication product of another service provider.

Clause 49 of the Bill would require an Electronic Authentication Service Provider to pay the costs reasonably incurred in the performance of an audit, for registration and for notification of compliance.

Part VI of the Bill would provide for intermediaries and telecommunications service providers and would contain three clauses.

Clause 50 of the Bill would set out the liability of intermediaries and telecommunications service providers.

Clause 51 of the Bill would set out the procedure for an intermediary or telecommunications service provider in dealing with unlawful or defamatory information.

Clause 52 of the Bill would require intermediaries and telecommunications service providers to comply with codes of conduct developed by the Minister.

Part VII of the Bill would set out the requirements for the Government and other public authorities and would contain two clauses.

Clause 53 of the Bill would set out the functions of a public body. Subclause (2) provides that when the public authority decides to perform any of its functions in an electronic environment, it may

specify the manner and format in which such information, documents or records in electronic form shall be filed, created, retained, issued or provided, the manner and format in which such signature shall be affixed to documents, records or information, such control processes and procedures as may be appropriate, and other required attributes for documents, record or information. Subclause (3) provides for the Minister to specify the type of signature required when information, data message or record in electronic form is required to be signed. Subclause (4) provides that where any person is required to file, create or retain any document, use a prescribed form for an application, provide to or retain for a public body any document or hold a licence, such a requirement is satisfied by information, data message or record in electronic form.

Clause 54 of the Bill would require documents, records or information to be made available for inspection in an electronic record.

Part VIII of the Bill would deal with consumer protection and would contain four clauses.

Clause 55 of the Bill would require the provision of certain minimum information to consumers by a person using electronic means to sell goods or services.

Clause 56 of the Bill would require that before entering into a contract requiring the issuance of an accredited electronic authentication product that the Electronic Authentication Service Provider provides the party seeking the electronic authentication product with certain information.

Clause 57 of the Bill would entitle a consumer who is not provided with the information required under clauses 55 and 56 to cancel the transaction within thirty days if the consumer has not received any material benefit from the transaction.

Clause 58 of the Bill would require persons who send unsolicited e-mails to provide the receivers of such e-mails with the option to opt out of receiving future communications.

Part IX of the Bill would deal with contravention and enforcement and would contain five clauses.

Clause 59 of the Bill would make it an offence for a person who in providing information under this Act submits false or misleading information or if he provides a consumer or a user of an electronic authentication product with false or misleading information.

Clause 60 of the Bill would make it an offence for a person to make false or misleading statements to persons carrying out an audit or who obstructs or otherwise hinders the persons carrying out the audit in compliance with clause 40.

Clause 61 of the Bill would make it an offence to breach the confidentiality obligations under clause 42.

Clause 62 of the Bill would provide that where a corporation commits an offence under this Act, its officers, directors or agents who directed, authorized, assented to, acquiesced in or participated in the commission of the offence is party to and commits an offence and would be liable to the punishment provided for the offence whether or not the corporation has been prosecuted or convicted.

Clause 63 of the Bill would set out the penalties for offences committed by a person or a body corporate.

Part X of the Bill would contain Miscellaneous provisions and would contain three clauses.

Clause 64 of the Bill would impose duties on directors and officers of a corporation.

Clause 65 of the Bill would set out the jurisdiction of the Court under this Act.

Clause 66 of the Bill would empower the Minister to make regulations for the purpose of giving effect to the requirements of this Act and such regulations are subject to negative resolution of Parliament.

BILL

AN ACT to give legal effect to electronic documents, electronic records, electronic signatures and electronic transactions

[, 2011]

ENACTED by the Parliament of Trinidad and Tobago as follows: Enactment

PART I

PRELIMINARY

1. (1) This Act may be cited as the Electronic Transactions Act, 2011. Short title and commencement

(2) This Act shall come into operation on such day as is fixed by the President by Proclamation.

Interpretation

2. In this Act—

"addressee" in relation to a data message, means a person who is intended by the originator to receive the data message but does not include a person acting as an intermediary or telecommunications service provider with respect to that data message;

"certificate" means an electronic attestation that links certain signature verification information to the signatory and confirms his or its identity;

"certification service provider" means a person who issues electronic certificates or provides other services related to electronic signatures;

"consumer" means any person who enters or intends to enter into an electronic transaction with a supplier as the end user of the goods or services offered by the supplier;

"Court" means the High Court of Trinidad and Tobago;

"computer-mediated networks" means the networks established by the logical or physical interconnection of multiple information systems, whether belonging to the same or multiple persons, facilitated by public or private telecommunications networks;

"data" means the content including but not limited to the text, images or sound which make up a data message;

"data message" means any document, correspondence, memorandum, book, plans, map, drawing, diagram, pictorial or graphic work, photograph, audio or video recording, machine-readable symbols generated, sent, received or stored by any electronic means by or on behalf of the person it represents; his official duties

"electronic" means being in digital or intangible forms with the capability of creation, storage, transmission or receipt by electronic, magnetic, wireless, optical, biometric or any other similar means;

"electronic agent" means a program or other electronic or automated means configured and enabled by a person that is used to initiate or respond to data messages or performance in whole or in part without review or intervention by a person at the time of the initiation or response;

"electronic authentication product" means a product designed to identify the holder of an electronic signature to another person;

"Electronic Authentication Service provider" means a person who issues electronic authentication products and services related thereto and includes Certification Service Providers;

"electronic record" means a record created, stored, generated, received or communicated by electronic means;

"electronic signature" means information in electronic form affixed to, or logically associated with a data message which may be used to—

(a) identify the signatory in relation to that data message; or

(b) indicate the signatory's approval of the information contained within that data message;

"electronic transaction" includes the single communication or outcome of multiple communications involved in the sale or purchase of goods and services conducted over computer-mediated networks or information systems, where the goods and services may be ordered through such networks or systems but the payment and ultimate delivery of the goods and services may occur without the use of such networks or systems;

"enterprise" means a partnership or body, whether corporate or unincorporated, engaged in business;

"individual" means a natural person;

"information" includes data, codes, computer programs, software and databases;

"information system" means a device or combination of devices including input and output devices capable of being used in conjunction with external files which contain computer programs, electronic instructions, input data and output data that perform logic, arithmetic, data

storage and retrieval, communication control and other functions but does not include a calculator;

"intermediary" with respect to a data message means a person who on behalf of another person, sends, transports, receives or stores that data message or provides other services with respect to that data message including the provision of content, e-mail, caching and hosting services;

"Minister" means the Minister to whom responsibility for Information and Communication Technology is assigned;

"originator" in relation to a data message means a person by whom or on whose behalf the data message purports to have been sent or generated prior to storage, but does not include a person acting as an intermediary or telecommunications service provider with respect to that data message;

"products" includes services;

"public body" means—

(a) Parliament, a Joint Select Committee of Parliament or a committee of either House of Parliament;

(b) the Court of Appeal, the High Court, the Industrial Court, the Tax Appeal Board or any court of summary jurisdiction;

(c) the Cabinet as constituted under

the Constitution, a Ministry or Department, Division or Agency of a Ministry;

(d) the Tobago House of Assembly, the Executive Council of the Tobago House of Assembly or a division of the Tobago House of Assembly;

(e) a municipal corporation established under the Municipal Corporations Act;

(f) a statutory body, responsibility for which is assigned to a Minister of Government;

(g) a company incorporated under the laws of Trinidad and Tobago that is owned and controlled by the State;

(h) a Service Commission established under the Constitution or other written law; or

(i) a body corporate or an unincorporated entity in relation to any function that it exercises on behalf of the State, or which is supported, directly or indirectly by Government funds and over which Government is in a position to exercise control;

"record" means recorded information collected, created or received in the initiation, conduct or completion of an activity and that comprises sufficient content, context

and structure to provide evidence or proof of that activity or transaction;

"signatory" means a person who may or may not hold a signature-creation device and acts either on his or its own behalf or on behalf of another person to create an electronic signature; and

"telecommunications service provider" means a provider of telecommunications services within the meaning of the Telecommunications Act.

Act binds the State

3. This Act binds the State.

No requirement to accept or issue document or information in electronic form

4. Notwithstanding section 3, nothing in this Act shall by itself compel any public body to accept or issue any document or information in the form of electronic records.

Purposes and construction

5. This Act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes to:

(a) facilitate the appropriate use of electronic transactions;

(b) facilitate electronic commerce, to eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(c) facilitate electronic filing of documents with public authorities, and to promote efficient delivery by public agencies of services by means of reliable electronic records;

(d) help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and

(e) promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

Inapplicability of Act

6. Parts II, III and IV of this Act shall not apply to any written law requiring writing, signatures or original documents for—

(a) the making, execution or revocation of a will or testamentary instrument;

(b) the conveyance of real or personal property or the transfer of any interest in real or personal property;

(c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney;

(d) the production of documents relating to immigration, citizenship or passport matters; or

(e) the recognition or endorsement of negotiable instruments.

Voluntary use of electronic transactions

7. (1) This Act does not require a person who uses, provides, accepts or retains documents, records or information, to use, provide, accept or retain it in an electronic form.

(2) Notwithstanding subsection (1), with regard to parties in a transaction, either party's consent to use, provide, accept or retain documents, records or information in electronic form in the course of that transaction may be inferred by past conduct.

PART II

REQUIREMENT FOR LEGAL RECOGNITION

Legal recognition of electronic transactions

8. Information or a record in electronic form or a data message shall not be denied legal effect, admissibility or enforceability solely on the grounds that it is—

(a) rendered or made available in electronic form; or

(b) not contained in the information, data message, or record in electronic form purporting to give rise to such legal effect but is referred to in that information, data message or record.

Writing

9. The legal requirement that information, a record or a data message be in writing is satisfied where that information, record or data message is presented in electronic form, if the information, record or data message is accessible and capable of retention for subsequent reference.

Provision of information

10. (1) The legal requirement that information, a record or a data message be provided or sent to a person may be met by providing or sending the information, record or data message by electronic means.

(2) For the purpose of this Act, information or a record in electronic form or a data message is not provided or sent to a person if it is merely made available for access by the person and is not capable of being retained.

Specified non-electronic form

11. Where a written law requires information, a record or a data message to be presented in a specified

non-electronic form, that requirement is satisfied if the information or record in electronic form or the data message—

(a) contains substantially the same information; and

(b) is accessible and retainable so as to be usable for subsequent reference.

Original form

12. (1) Where a written law requires information, a record or a data message to be presented or retained in its original form, that requirement is satisfied by the information, record or data message being presented in electronic form if—

(a) there exists a reliable assurance as to the maintenance of the integrity of the information or record in electronic form or the data message by the person who presented the information; and

(b) it is to be presented to a person, the information or record in electronic form or the data message in electronic form is accessible and capable of retention for subsequent reference.

(2) The criterion for assessing integrity under subsection (1) shall be whether the information or record in electronic form or a data message has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display.

(3) Reliability under subsection (1) shall be determined in light of all the circumstances, including the purpose for which the information or record in electronic form or the data message was created.

13. Where a written law requires that certain information, records or data messages be retained, that requirement is satisfied by retaining the information, data messages or records in electronic form. Rention of information, data messages or records in electronic form

14. Information or record in electronic form or a data message is not capable of being retained if the person providing the information, record or data message prevents or does anything to hinder its printing, audio or video playback or storage by the recipient. Whether information, a data message or a record is capable of being retained

15. Where information, a record or a data message is provided in electronic form, a requirement under any written law for one or more copies of the information, record or data message to be provided to a single addressee at the same time is satisfied by providing a single copy in electronic form. Copies

16. A copy of a data message containing an electronic signature shall be as valid, enforceable and effective as a message containing a non-electronic signature. Electronically signed message deemed to be original document

17. Information or record in electronic form or a data message will not be deemed inadmissible as evidence— Admissibility and evidental weight of electronic records

(a) solely on the ground that it is in electronic form; or

(b) on the ground that it is not in the original non-electronic form, if it is the best evidence.

18. Where information or a signature, document or record is required by a statutory provision or rule of law, or by contract or deed to be notarized, acknowledged or verified, the requirement shall be satisfied if, in relation to an electronic signature, electronic document or electronic record, the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable Electronic Notarization

law, is attached to or logically associated with the electronic signature, electronic document or electronic record to be notarized, acknowledged or verified.

PART III

CONTRACT FORMATION AND DEFAULT PROVISION

Formation and validity of contracts

19. In the context of contract formation—

(a) an offer or the acceptance of an offer or any other matter that is material in the operation or formation of a contract may be expressed by means of information or record in electronic form or a data message; and

(b) the fact that a transaction is conducted in electronic form or that information or a record of the negotiation or formation of a contract is in electronic form does not affect its enforceability.

Electronic expression of offer and acceptance

20. Unless parties agree otherwise, an offer or the acceptance of an offer or any other matter that is material to the operation or formation of a contract may be expressed by means of information, a data message or a record in electronic form, including by an activity in electronic form such as touching or clicking on an appropriately designated icon or place on the computer screen or otherwise communicating electronically in a manner that is intended to express the offer, acceptance or other matter.

Use of electronic agents for contract formation

21. A contract formed through the interaction of an electronic agent and a person or by the interaction of electronic agents shall not be denied legal validity and enforceability solely on the ground that no person reviewed or intervened in each of the individual actions carried out by the electronic agent.

22. (1) A contract concluded in an electronic environment through the interaction of a person and an electronic agent of another person is void where— Error that occurs while dealing with an electronic agent

(a) the first referred person made a material error in the information or data message;

(b) the electronic agent of the second referred person did not provide an opportunity to prevent or correct the error;

(c) on becoming aware of the error, the first referred person notifies the second referred person of the error;

(d) the second referred person has taken no reasonable steps to correct the error; and

(e) the first referred person has not received or used any material benefit or value from the second referred person.

(2) Subsection (1) shall not apply to electronic auctions.

23. A data message or record in electronic form is attributed to a particular person if it resulted from an action of that person or through an agent or electronic agent of that person. Attribution of data messages or records

24. Unless the originator and addressee agree otherwise, information in electronic form or a data message is sent— Time of sending of data message

(a) when it leaves the information system under the control of the originator; or

(b) in the case where the originator and the addressee are in the same information system, when the information in electronic form or data message becomes capable of being retrieved and processed by the addressee.

Time of receipt of data message

25. (1) Unless the originator and addressee agree otherwise, if information in electronic form or a data message is capable of being retrieved by an addressee, it is deemed to be received by the addressee-

(a) when it enters an information system designated or used by the addressee for the purpose of receiving information in electronic form or data messages of the type sent; or

(b) upon the addressee becoming aware of the information in electronic form or data message in the addressee's information system, if the addressee has not designated or does not use an information system for the purpose of receiving information in electronic form or data messages of the type sent.

(2) Subsection (1) shall apply notwithstanding the fact that the place where the information system supporting an electronic address is located may be different from the place where information in electronic form or the data message is deemed to be received under section 26.

Place of sending and receipt of information or record

26. Unless the originator and addressee agree otherwise, information or a record in electronic form or a data message is deemed to be sent from the originator's address and to be received at the addressee's address.

Place of business

27. (1) Subject to subsection (2) and unless the originator and addressee of a data message agree otherwise, the place of business of either party is deemed to be—

(*a*) the place of business that has the closest relationship to the underlying electronic transaction if a party has more than one place of business; or

(*b*) if there is no underlying electronic transaction, the principal place of business of the originator or addressee of the communication.

(2) A location is not a place of business merely because that location is—

(*a*) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or

(*b*) where the information system may be accessed by other parties.

(3) The sole fact that a party makes use of a domain name or an electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

Habitual residence

28. If the originator or addressee of a data message has no place of business, then the habitual residence of the originator or addressee is the relevant criterion for the place of sending and receipt of the data message.

PART IV

ELECTRONIC SIGNATURE

Electronic signature

29. Parties to an electronic transaction may agree to the use of a particular method or form of electronic signature, unless otherwise provided by written law.

Minimum standards for legally required signatures

30. Where a written law requires the signature of a person, that requirement is met in relation to an electronic record or data message by the use of an electronic signature that meets the minimum standards of reliability and integrity or is as reliable as appropriate, given the purpose for which and the circumstances in which the signature is required.

Reliability and integrity of electronic signatures

31. (1) The criteria that shall be used to determine the reliability and integrity of an electronic signature include whether—

(a) the authentication technology uniquely links the user to the signature;

(b) the signature is capable of identifying the user;

(c) the signature is created using a means that can be maintained under the sole control of the user; and

(d) the signature will be linked to the information to which it relates in such a manner that any subsequent change in the information is detectable.

(2) Information or a record in electronic form or a data message that is signed with an electronic signature that meets the reliability criteria set out in subsection (1) is deemed to be unaltered since the time of its signing.

Electronic signature associated with an accredited electronic authentication product

32. An electronic signature that is associated with an electronic authentication product issued by an Electronic Authentication Service Provider accredited under Part V (hereinafter referred to as a "qualified electronic authentication product"), is deemed to satisfy the requirements set out in section 31 for reliability and integrity.

PART V

ELECTRONIC AUTHENTICATION SERVICE PROVIDERS

Registration of Electronic Authentication Service Provider

33. (1) No person shall issue a qualified electronic authentication product to the public unless he is registered as an accredited Electronic Authentication Service Provider by the Minister or such authority as designated by the Minister by Order (hereinafter

referred to as "the designated authority") and has provided the information prescribed by the Minister.

(2) A person who contravenes subsection (1) commits an offence.

Application for registration

34. (1) A person wishing to be registered as an accredited Electronic Authentication Service Provider shall apply to the Minister or the designated authority in the manner prescribed and pay the prescribed fee.

(2) The application under subsection (1) shall include at a minimum the following information:

(a) the name and business address of the person; and

(b) where the person is previously accredited in another jurisdiction, information relating to—

(i) the name and address of the accreditation authority; and

(ii) the period of validity of the accreditation.

(3) The Minister may make Regulations specifying the procedure for registration and the information required for that purpose.

(4) Where an applicant under this section has no prior accreditation, the Minister or the designated authority shall require the applicant to submit to an audit of its operations and systems to ensure compliance with the requirements of section 35, and any other international standards which the Minister may prescribe.

(5) Where the Minister or the designated authority is satisfied that the person has met the requirements outlined in subsection (3), the Minister or the

designated authority may issue a notice of accreditation to that person, and complete their registration as outlined in subsection (1).

Requirements for an Electronic Authentication Service Provider that issues qualified electronic authentication products

35. An Electronic Authentication Service Provider that issues qualified electronic authentication products to the public shall conduct his or its operations in a reliable manner and shall—

(a) employ personnel who possess the expert knowledge and experience required for these operations, especially with regard to management, technology, electronic authentication and security procedures;

(b) apply such administrative and management routines that conform to recognized standards;

(c) use trustworthy systems and products that are protected against modification and that ensure technical and cryptographic security;

(d) maintain sufficient financial resources to conduct his or its operations in accordance with these requirements and any other provisions set forth in the Act and bear the risk of liability for damages;

(e) have secure routines to verify the identity of those signatories to whom qualified electronic authentication products are issued;

(f) maintain a prompt and secure system for registration and immediate revocation of a qualified electronic authentication product;

(g) take measures against forgery of a qualified electronic authentication product and, where applicable, guarantee full confidentiality during the process of generating signature creation data;

(h) comply with section 56; and

(i) comply with any other requirements established by the Minister by Order.

Grant of registration

36. (1) Where the Minister or the designated authority is satisfied that an applicant has previously been accredited and has met the requirements of section 35, the Minister or the designated authority may grant the registration.

(2) Where the Minister or the designated authority is satisfied that an applicant who has no prior accreditation has met the requirements of sections 34 and 35, the Minister or the designated authority may issue a notice of accreditation to that applicant, and grant the registration.

Recognition of the qualified external Electronic Authentication products

37. The Minister may by Order recognize a qualified electronic authentication product or classes of qualified electronic authentication products as a qualified electronic authentication product issued by Electronic Authentication Service Providers or classes of Electronic Authentication Service Providers established in any other jurisdiction, as qualified electronic authentication products in Trinidad and Tobago.

Registry of Electronic Authentication Service Providers

38. The Minister or the designated authority shall maintain a public registry of accredited Electronic Authentication Service Providers that includes the information required by the Minister by Order.

Updated notification of compliance

39. A registered Electronic Authentication Service Provider that issues qualified electronic authentication products shall annually provide the Minister or the designated authority with an updated notification of compliance with the requirements of section 35 and pay the prescribed fee.

Audit by the Minister

40. (1) The Minister or the designated authority may conduct an audit to verify that the Electronic Authentication Service Provider has been or remains in compliance with the requirements of this Act.

(2) In the performance of an audit, the Minister may employ whatever experts he considers may be required.

Responsibility to co-operate with an audit

41. An Electronic Authentication Service Provider shall co-operate with and offer all reasonable assistance to the Minister or the designated authority while conducting an audit and shall make available information necessary to satisfy the Minister or the designated authority regarding compliance with the requirements of this Act.

Confidentiality

42. Notwithstanding any law to the contrary, no person who performs or has performed duties or functions in the administration or enforcement of this Act, including performing an audit pursuant to section 40, shall communicate or allow to be communicated information obtained in the course of performance of duties or functions under the Act to any other person except—

(a) to law enforcement authorities of the Republic of Trinidad and Tobago on the basis of a warrant; or

(b) by Order of the Court.

Power of Minister to deal with failure to meet requirements

43. Where the Minister or the designated authority is satisfied that an Electronic Authentication Service Provider no longer meets the requirements to issue qualified electronic authentication products, he may—

(a) cancel the registration of the Electronic Authentication Service Provider;

(b) order the Electronic Authentication Service Provider to cease any or all of its activities, including the provision of qualified electronic authentication products;

(c) order the Electronic Authentication Service Provider to be removed from the registry;

(d) take any action that he deems reasonable to ensure that the Electronic Authentication

Service Provider is in compliance with the requirements set out in section 36; or

(e) make any other order that the Minister or the designated authority deems reasonable in the circumstances including, but not limited to reimbursement of fees and charges to users of the services of the Electronic Authentication Service Provider or public notification of cessation of business.

Pseudonyms

44. An Electronic Authentication Service Provider may, at the request of a particular signatory, indicate in the relevant electronic authentication product a pseudonym instead of the signatory's name.

Additional responsibilities of an Electronic Authentication Service Provider

45. An Electronic Authentication Service Provider shall ensure the operation of a prompt and secure directory of holders of electronic authentication products and secure an immediate revocation service that makes it possible to ascertain—

(a) whether a qualified electronic authentication product was revoked;

(b) the validity period of the qualified electronic authentication product; or

(c) whether the qualified electronic authentication product contains any limitations on the scope or value of the electronic transactions for which the signature can be used.

Immediate revocation upon request

46. (1) An Electronic Authentication Service Provider shall revoke an electronic authentication product immediately upon the receipt of a request to do so by the signatory or if otherwise warranted in the circumstances.

(2) An Electronic Authentication Service Provider shall ensure that the date and time when an electronic

authentication product is revoked can be determined precisely.

Liability of Electronic Authentication Service Provider issuing a qualified electronic authentication product

47. (1) An Electronic Authentication Service Provider issuing a qualified electronic authentication product to the public is *prima facie* liable for any damages or loss caused to anyone relying on the qualified electronic authentication product due to—

(a) the Electronic Authentication Service Provider not continuing to meet the requirements set forth in section 31 or 35 at the time of the issuance of the qualified electronic authentication product; or

(b) the qualified electronic authentication product, when issued, having contained incorrect information.

(2) This section also applies to an Electronic Authentication Service Provider who guarantees that the electronic authentication product of another service provider is qualified.

Release from liability

48. (1) An Electronic Authentication Service Provider issuing a qualified electronic authentication product may be exempted from liability if the provider can show that the injury or loss was not caused by its own negligence.

(2) The Electronic Authentication Service Provider is also not liable for damages for an injury or loss arising from the use of a qualified electronic authentication product in violation of any limitations of use or scope of transaction clearly stated in the qualified electronic authentication product.

(3) This section also applies to an Electronic Authentication Service Provider who guarantees that the electronic authentication product of another service provider is qualified.

Costs of audit

49. The Minister or the designated authority may order an Electronic Authentication Service Provider to pay

the costs reasonably incurred in the performance of an audit pursuant to section 40 and may prescribe fees for the registration pursuant to section 33 and notification of compliance pursuant to section 39.

PART VI

INTERMEDIARIES AND TELECOMMUNICATIONS SERVICE PROVIDERS

Liability of intermediaries and telecommunications service providers

50. (1) An intermediary or telecommunications service provider who merely provides a conduit for the transmission of data messages, records or information in electronic form shall not be liable for the content of data messages, records or information in electronic form if the intermediary or telecommunications service provider has no actual knowledge or is not aware of facts that would to a reasonable person, indicate a likelihood of criminal liability or liability for a tort in respect of material on the network of an intermediary or telecommunications service provider or who, upon acquiring actual knowledge or becoming aware of such facts, follows the procedures required by section 51.

(2) Nothing in this section relieves an intermediary or telecommunications service provider from complying with any court order, injunction, writ, ministerial direction, regulatory requirement or contractual obligation in respect of data messages, records or information in electronic form.

(3) An intermediary or telecommunications service provider shall not be required to monitor any data message processed by means of its system in order to ascertain whether its processing would, apart from this section, constitute or give rise to an offence or give rise to civil liability.

Procedure for dealing with unlawful, defamatory, etc., information

51. (1) If an intermediary or telecommunications service provider has actual knowledge that the information in a data message or an electronic record

gives rise to civil or criminal liability then, as soon as is practicable after acquiring such knowledge, the intermediary or telecommunications service provider shall—

(a) remove the information from any information system within the control of the intermediary or telecommunications service provider and cease to provide or offer to provide services in respect of that information or take any other action authorized by written law; and

(b) notify the Minister or such person designated by the Minister ("the designated person") and the appropriate law enforcement authority of the relevant facts and of the identity of the person for whom the intermediary or telecommunications service provider was supplying services in respect of the information, if the identity of that person is known to the intermediary or telecommunications service provider.

(2) If an intermediary or telecommunications service provider is aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information in a data message or an electronic record ought reasonably to have been known, then as soon as is practicable after becoming aware, the intermediary or telecommunications service provider shall—

(a) follow the relevant procedure set out in a code of conduct approved or standard appointed under this Act if such code or standard applies to the intermediary or telecommunications service provider; or

(b) notify the Minister or the designated person.

(3) If the Minister or the designated person is notified in respect of any information under subsection (2), the Minister or the designated person may direct the intermediary or telecommunications service provider to—

(a) remove the information from any information processing system within the control of the intermediary or telecommunications service provider;

(b) cease to provide services to the person to whom the intermediary or telecommunications service provider was supplying services in respect of that information; or

(c) cease to provide services in respect of that information.

(4) An intermediary or telecommunications service provider is not liable, whether in contract, tort, under statute or otherwise to any person, including any person on whose behalf the intermediary or telecommunications service provider provides services in respect of information in a data message or an electronic record for any action, the intermediary or telecommunications service provider takes in good faith in exercise of the powers conferred by, or as directed by, the Minister or the designated person, under this section.

(5) Any person who lodges a notification of unlawful activity with an intermediary or telecommunications service provider, knowing that it materially misrepresents the facts, commits an offence and is liable for damages for wrongful removal of the information in a data message or electronic record under subsections (1) to (3).

Codes of conduct and service standards for intermediaries and telecommunications service providers

52. (1) Where the Minister has developed a code of conduct or service standards for intermediaries and telecommunications service providers, the intermediaries and telecommunications service providers shall comply with the code of conduct or service standards.

(2) Compliance with relevant codes of conduct and service standards may be taken into account by the courts in determining liability.

PART VII

GOVERNMENT AND OTHER PUBLIC BODIES

General authorization

53. (1) A public body that, pursuant to any written law—

(a) accepts the filing of documents, or obtains information in any form;

(b) requires that documents be created or retained;

(c) requires documents, records or information to be provided or retained in their original form; or

(d) issues any permit, licence or approval,

may, notwithstanding anything to the contrary in such written law, carry out those functions by electronic means.

(2) Where a public body decides to perform any of the functions in subsection (1) by electronic means, the public authority may specify—

(a) the manner and format in which such documents, records or information in electronic form shall be filed, created, retained, issued or provided;

(b) the manner and format in which such signature shall be affixed to the

documents, record or information in electronic form, and the identity of or criteria that shall be met by any Electronic Authentication Service Provider used by the person filing the document;

(c) such control processes and procedures as may be appropriate to ensure adequate integrity, security and confidentiality of documents, record or information in electronic form; or

(d) any other required attributes for documents, record or information in electronic form that are currently specified for corresponding paper documents.

(3) Where a document, record or information in electronic form under subsection (2) is required to be signed, the Minister may by Regulations specify the type of signature required, including, where applicable, the requirement that the sender use a particular type of encrypted electronic signature.

(4) For the avoidance of doubt, notwithstanding anything to the contrary in any written law but subject to any specification made under subsection (2), where any person is required by any written law to—

(a) file any document with or provide information in any form to a public body;

(b) create or retain any document for a public body;

(c) use a prescribed form for an application or notification to, or other transaction with, a public body;

(d) provide to or retain for a public body any document, record or information in its original form; or

(e) hold a licence, permit or other approval from a public body,

such a requirement is satisfied by a document, record or information in electronic form specified by the public authority for that purpose.

Documents for inspection

54. Where documents, records or information are required by any written law to be made available for inspection, that requirement is met by making such documents, records or information available for inspection in electronic form.

PART VIII

CONSUMER PROTECTION

Minimum information in e-commerce

55. (1) A person using electronic means to sell goods or services to consumers shall provide accurate, clear and accessible information about themselves, sufficient to allow—

(a) the legal name of the person, its principal geographic address, and an electronic means of contact or telephone number;

(b) prompt, easy and effective consumer communication with the seller; and

(c) service of legal process.

(2) A person using electronic means to sell goods or services to consumers shall provide accurate and accessible information describing the goods or services offered, sufficient to enable consumers to make an informed decision about the proposed transaction and to maintain an adequate record of the information.

(3) A person using electronic means to sell goods or services to consumers shall, before the conclusion of the electronic contract based on such transaction, provide the following information to consumers in respect of such electronic contract:

(a) the terms, conditions and methods of payment;

(b) the details of, and conditions and policies related to, privacy, withdrawal, termination, return, exchange, cancellation and refunds;

(c) the arrangements for delivery or performance; and

(d) a copy of the contract for the consumer in a format that can be retained.

Minimum information regarding authentication products

56. Before entering into an electronic contract requiring the issuance of a qualified electronic authentication product, an Electronic Authentication Service Provider shall inform the party seeking the electronic authentication product in writing of the following:

(a) the terms and conditions concerning the use of the electronic authentication product, including any limitations on its scope or amounts;

(b) any requirements concerning storage and protection of the signature-creation data by the signatory;

(c) the cost of obtaining and using the electronic authentication product and of using the other services of the Electronic Authentication Service Provider;

(d) whether the Electronic Authentication Service Provider is accredited; and

(e) procedures for settlement of complaints.

Right of rescission

57. A consumer who is not provided with the information required by sections 55 and 56 has the right to rescind the contract within thirty calendar days provided that the consumer has not received any material benefit from the transaction.

Unwanted communications

58. (1) Any person who sends unsolicited commercial communications through electronic media to consumers based in Trinidad and Tobago or knowingly uses an intermediary or a telecommunications service provider based in Trinidad and Tobago to send, or who has a place of business in Trinidad and Tobago and sends unsolicited electronic correspondence to consumers, shall provide the consumer with a clearly specified and easily activated option to opt out of receiving future communications.

(2) A person who contravenes subsection (1) commits an offence.

PART IX

CONTRAVENTION AND ENFORCEMENT

False or misleading information

59. A person who—

(a) files information required under this Act that contains false or misleading information;

(b) provides a consumer or a user of an electronic authentication product with false or misleading information,

commits an offence.

Obstruction of an audit

60. A person who, with respect to an audit carried out pursuant to section 40—

(a) knowingly makes any false or misleading statement, either orally or in writing to persons carrying out the audit; or

(b) otherwise obstructs or hinders the persons carrying out the audit in the conduct of their duties and functions,

commits an offence.

Breach of obligations of confidentiality

61. A person who breaches the confidentiality obligations established by section 42 commits an offence.

62. Where a body corporate commits an offence under this Act, any officer, director or agent of the body corporate who directed, authorized, assented to, acquiesced in or participated in the commission of the offence is a party to and commits an offence and is liable to the punishment provided for the offence. Liability of directors and officers

63. (1) A person who commits an offence under this Act for which no penalty is provided is liable upon— Penalties

(a) summary conviction to a fine of two hundred thousand dollars or to imprisonment for a term of three years; or

(*b)* conviction on indictment to a fine of two hundred and fifty thousand dollars or to imprisonment for a term of five years.

(2) Where the offence under this Act is committed by a body corporate for which no penalty is provided, the body corporate shall be liable upon—

(a) summary conviction to a fine of two hundred and fifty thousand dollars; or

(b) conviction on indictment to a fine of five hundred thousand dollars.

(3) Where a body corporate contravenes any of the provisions of this Act, the Court may, in addition to any penalty it may impose for a criminal offence, impose a fine up to ten per cent of the annual turnover of the body corporate.

(4) In imposing a fine under subsection (3) the Court shall take into account—

(a) the estimate of the economic cost of the contravention to the consumers, users of the services in question or any other person affected by the contravention;

(b) the estimate of the economic benefit of the contravention to the enterprise;

(c) the time for which the contravention is in effect if continuing;

(d) the number and seriousness of any other contraventions, if any, committed by the enterprise; and

(e) any other matter the Court may consider appropriate in the circumstances.

PART X

MISCELLANEOUS

Duties of directors

64. Every director and officer of a body corporate shall take all reasonable care to ensure that the body corporate complies with—

(a) this Act and the regulations made under this Act; and

(b) any orders imposed by the Minister or his delegate.

Jurisdiction of the Court

65. The Court shall have jurisdiction to hear and determine—

(a) applications by the Minister for any Order which the Court considers appropriate to facilitate the enforcement of any provisions of this Act;and

(b) upon application by the Minister pursuant to this Act, cases involving any contravention of the provisions of this Act and make such appropriate Orders in relation thereto.

Regulations

66. (1) The Minister may make Regulations for the purpose of giving effect to this Act.

(2) Notwithstanding the generality of the foregoing, the Minister may make Regulations with respect to any matter that is required to be prescribed under this Act.

(3) Regulations made under this section shall be subject to negative resolution of Parliament.

Passed in the House of Representatives this day of , 2011.

Clerk of the House

I confirm the above.

Speaker

Passed in the Senate this day of , 2011.

Clerk of the Senate

I confirm the above.

President of the Senate

No. 5 of 2011

FIRST SESSION

TENTH PARLIAMENT

REPUBLIC OF

TRINIDAD AND TOBAGO

BILL

AN ACT to give legal effect to electronic documents, electronic records, electronic signatures and electronic transactions

Received and read the

First time .....

Second time .....

Third time .....