ELECTRONIC TRANSACTIONS BILL, 2009

EXPLANATORY NOTES
(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-seven sections.

Part I of the Bill would comprise the preliminary clauses and would contain eight 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 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. Subclause (4) also provides that this Act shall not apply to electronic funds transfers.

Clause 5 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.

Clause 6 of the Bill would provide that the Data Commissioner who is appointed under the Data Protection act would be responsible for the administration of Part V of this Act.

Clause 7 of the Bill would provide that the Act does not limit the authorisation, prohibition or regulation of information or records in electronic form under any other law.

Part II of the Bill would set out the requirements for recognition and would contain ten 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 a record or information 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 or a record be provide or sent in writing, that requirement is met where the information is provided or sent in electronic form.

Clause 11 of the Bill would provide that where there is a legal requirement that information or a record be in a specific non-electronic form, that requirement is met where the information or record when put in electronic form is organized in substantially the same way, accessible and capable of retention 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 the there is a reliable assurance as to the integrity of the information, data messages or records. 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 the original message.

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 eleven clauses.

Clause 18 of the Bill would provide that the fact that a transaction is conducted, negotiated or formulated in electronic form does not affect its validity

Clause 19 of the Bill would set out the manner of offer and acceptance of an offer is satisfied electronically.

Clause 20 of the Bill would provide for the involvement of electronic agents in the formation of a contract.

Clause 21 of the Bill would provide that an electronic contract is void where a material error is made, no opportunity is given to prevent or correct the error, notification of the error takes place, reasonable steps are taken to correct the error and material benefit or value is not received. This section does not apply to electronic auctions.

Clause 22 of the Bill would provide for the attribution of an electronic record

Clause 23 of the Bill would provide for the effect of the acknowledgement of receipt of an electronic data message or information.

Clause 24 of the Bill would set out what period is deemed to be the period when information or a record in electronic form is sent.

Clause 25 of the Bill would set out what is the period when information or a record in electronic form is received.

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 five clauses.

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

Clause 30 of the Bill would set the minimum standards 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 empower the Minister to make regulations by Order, setting out a particular form of electronic signature to meet a specified legal requirement.

Clause 33 of the Bill would provide that an electronic signature that is associated with an accredited certificate satisfies the requirements for reliability and integrity.

PART V of the Bill would deal with certification service providers and would contain sixteen clauses.

Clause 34 of the Bill would prohibit the offer of certification services unless the service provider is registered by the Data Commissioner for such purpose.

Clause 35 of the Bill would require a person wishing to be registered as a certification service provider to apply to the Data Commissioner. The clause also goes on to provide that a statement of compliance must accompany the application and the procedure thereafter where an application is received. The requirement to be registered under this Act is subject however to the holding of a certificate form another jurisdiction as provided for in section 44.

Clause 36 of the Bill would set out the requirements for a certification service provider that issues accredited certificates.

Clause 37 of the Bill would require the maintenance of a public registry of certification service providers by the Data Commissioner under section 34.

Clause 38 of the Bill would provide for the annual renewal of the notification of compliance.

Clause 39 of the Bill would empower the Data Commissioner to conduct the audit to substantiate that the certification service provider has been or remains in compliance with the Act.

Clause 40 of the Bill would require a certification service provider to co-operate with any person or body conducting an audit.

Clause 41 of the Bill would restrict the communication of information by a person which was obtained during the course of performance of his duties or functions under the Act.

Clause 42 of the Bill would empower the Data Commissioner to deal with the failure of a certification service provider to meet the requirements to issue accredited certificates by either cancelling registration, ordering the certification service provider to cease all of its activities, ordering the certification service provider be struck from the registry, taking such action as is deemed reasonable to ensure compliance with section 37 and making any other order deemed reasonable.

Clause 43 of the Bill would empower the Minister to recognize the certificates or classes of certificates as accredited certificates issued by certification service providers by Order. Where the Minister publishes an Order under this clause the certification service providers so named in the Order shall be deemed to be registered and his name shall be entered in the Registry.

Clause 44 of the Bill would permit certification service providers to request that a particular signatory indicate the relevant certificate pseudonym instead of the signatory's name.

Clause 45 of the Bill would require a certification service provider to ensure the operation of a prompt and secure directory of certificate holders and to secure an immediate revocation service that make it possible to check whether an accredited certificate is revoked

Clause 46 of the Bill would provide for the revocation of a certificate by a certification service provider when a request is made for such revocation by the signatory or if other circumstances warrant a revocation.

Clause 47 of the Bill would set out the liability of a certification service provider for damages or loss to anyone relying on a certificate where the damage or loss is due to the service provider not meeting the requirements of section 32 or 37. This section also applies to a certification service provider who guarantees that the certificates of another service provider are accredited.

Clause 48 of the Bill would provide that a certification service provider who issues an accredited certificate may be exempted from liability if the provider can show that the injury or loss arising was not caused by its own negligence.

Clause 49 of the Bill would empower a certification service provider to pay the costs reasonably incurred in the performance of an audit.

Part VI of the Bill would provide for intermediaries and internet service providers and would contain four clauses.

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

Clause 51 of the Bill would set out the procedure for dealing with unlawful or defamatory information.

Clause 52 of the Bill would set out the role of the Telecommunications Authority of Trinidad and Tobago.

Clause 53 of the Bill would require intermediaries and telecommunications service providers to comply with codes of conduct developed by the Telecommunications Authority of Trinidad and Tobago.

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

Clause 54 of the Bill would allow the Government of Trinidad and Tobago, unless specifically prohibited by law, to use electronic means to create, collect, receive, store, transfer etc., records or information.

Clause 55 of the Bill would provide that where a written law authorizes the issue, prescription or establishment of a form of or manner of filing a document or submitting information such authorization includes the power to do so electronically.

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

Clause 56 of the Bill would require the provision of certain minimum information to consumers, by persons with a place of business in Trinidad and Tobago who use an internet service provider.

Clause 57 of the Bill would entitle a consumer who is not provided with the information required under section 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 that before entering into a contract requiring the issuance of an accredited certificate that the certificate service provider provide the party seeking the certificate with certain information.

Clause 59 of the Bill would require persons who send unsolicited e-mails to provide the receivers of such e-mail with the option to opt out of receiving future communications.

Part IX of the Bill would deal with offences and would contain six clauses.

Clause 60 of the Bill would make it an offence to fail to provide information to consumers under section 56 or the information and technical capacity required by section 58.

Clause 61 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 signature with false or misleading information.

Clause 62 of the Bill would make it an offence of a person to make false or misleading statements during an audit or who obstructs or other wise hinders the conduct of an audit.

Clause 63 of the Bill would make it an offence to breach the confidentiality obligations under section 41.

Clause 64 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 65 of the Bill would set out the penalties for offences under this Act ranging from fifty thousand dollars to five hundred thousand dollars.

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

Clause 66 of the Bill would impose duties in directors and officers of a corporation.

Clause 67 of the Bill would set out the jurisdiction of the Court under this Act.

Clause 68 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.

THE ELECTRONIC TRANSACTIONS BILL, 2009

Arrangement of Clauses

Clause

PART I
PRELIMINARY

1. Short title and commencement.
2. Interpretation.
3. Act binds the State.
4. Inapplicability of Act.
5. Voluntary use of electronic transactions.
6. Role of Data Commissioner under this Act.
7. Certain legal requirements continue.

PART II
REQUIREMENTS FOR LEGAL RECOGNITION

8. Legal recognition of electronic transactions.
9. Writing.
10. Provision of information.
11. Specified non-electronic form.
12. Original form.
13. Retention of information, data messages or records in electronic form.
14. Whether information, a data message or a record is capable of being retained.
15. Copies.
16. Electronically signed message deemed to be original document.
17. Admissibility and evidential weight of electronic records.

PART III
CONTRACT FORMATION AND DEFAULT PROVISIONS

18. Formation and validity of contracts.
19. Electronic expression of offer and acceptance.
20. Involvement of electronic agents.
21. Error that occur while dealing with an electronic agent.
22. Attribution of electronic data messages or records.
23. Acknowledgement of receipt of electronic data message.
24. Time of sending of electronic data message.
25. Time of receipt of electronic records.
26. Place of sending and receipt of information or record.
27. Place of business.
28. Habitual residence.

PART IV
ELECTRONIC SIGNATURE

29. Electronic signature.
30. Minimum standards for legally required signatures.
31. Reliability and integrity of electronic signatures.
32. Regulations regarding electronic signatures.
33. Electronic signature associated with an accredited certificate .

PART V
CERTIFICATION SERVICE PROVIDERS

34. Registration of certification service providers.
35. Application for and grant of registration.
36. Requirements for a certification service provider that issues accredited certificate.
37. Registry of certification service providers.
38. Annual renewal of notification of compliance.
39. Audit by the Data Commissioner.
40. Responsibility to co-operate with an audit.
41. Confidentiality.
42. Power of Data Commissioner to deal with failure to meet requirements.
43. Recognition of external certification service provider.
44. Pseudonyms.
45. Additional responsibilities of a certification service provider.
46. Immediate revocation upon request.
47. Liability of certification service provider issuing an accredited certificate.
48. Release from liability.
49. Cost of audit.

PART VI
INTERMEDIARIES AND INTERNET SERVICE PROVIDERS

50. Liability of intermediaries and internet service providers.
51. Procedure for dealing with unlawful, defamatory etc,. information.
52. Role of the Telecommunications Authority of Trinidad and Tobago.
53. Codes of conduct and service standards for intermediaries and internal service providers.

PART VII
GOVERNMENT AND OTHER PUBLIC AUTHORITIES

54. General authorization.
55. Forms and filings.

PART VIII
CONSUMER PROTECTION

56. Minimum information in e-commerce.
57. Right of rescission.
58. Minimum information regarding electronic signatures.
59. Unwanted communications.

PART IX
ENFORCEMENT

60. Failure to provide required information to consumers.
61. False or misleading information.
62. Obstruction of an audit.
63. Breach of obligations of confidentiality.
64. Directors and officers.
65. Penalties.

PART X
MISCELLANEOUS

66. Duties of directors.
67. Jurisdiction of the Court.
68. Regulations.

A BILL

An Act to give legal effect to electronic documents, records and signatures

Enactment.

ENACTED by the Parliament of Trinidad and Tobago as follows:

PART I

PRELIMINARY

Short title and commencement.

1.(1) This Act may be cited as the Electronic Transactions Act, 2009.

(2) This Act shall come into operation on such day as is fixed by the President by Proclamation and different days may be fixed for different provisions of this Act.

Interpretation.

2. In this Act-

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

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

"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 or stored by any electronic means by or on behalf of the person it represents;

"electronic" means information created, recorded, transmitted or stored in digital or other intangible forms by electronic, magnetic, optical or any other means that has capabilities for creation, transmission or storage similar to those means;

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

"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 an electronic data message which may be used to-

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

(b) indicate the signatory's approval of the information contained within that electronic 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 an electronic data message means a person who on behalf of another person, sends, transports, receives or stores that electronic data message or provides other services with respect to that electronic data message;

"Minister" means the Minster to whom responsibility for e-government and e-commerce is assigned;

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

"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.

Chap. 47:31

Act binds State.

3. This Act binds the State.

Inapplicability of Act.

4.(1) 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) any other matters that may be determined by the Minister by Order.

(2) Notwithstanding subsection (1), the Minister may by Order make this Act applicable to any of the legal requirements set out in subsection (1).

(3) An Order made under subsection (2) shall be subject to affirmative resolution of Parliament.

(4) Unless otherwise provided by any other written law, this Act shall not apply to electronic funds transfers.

Comment [i1]: Suggestion from Ministry of Finance and Central Bank

Voluntary use of electronic transactions.

5. This Act does not require a person who uses, provides, accepts or retains a document record or information, to use, provide, accept or retain it in an electronic form.

Role of Data Commissioner under this Act.

6. The Data Commissioner appointed under the Data Protection Act, 2008 is responsible for the administration of Part V of this Act.

Certain legal requirements continue.

7. Notwithstanding Parts II, III and IV, this Act does not limit the operation of any written law that expressly authorizes, prohibits or regulates the use of information, data messages, records, payments or signatures in electronic form or requires that information, a data message, a record or a payment be posted or displayed in a specific manner.

PART II
REQUIREMENTS FOR LEGAL RECOGNITION

Legal recognition of electronic transactions.

8. An electronic data message, record or information to which this Act applies shall not be denied legal effect or enforceability merely because it is in electronic form.

Writing.

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

Provision of information.

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

or sending the information, data message or record by electronic means.

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

Specified non-electronic form.

11. Where a written law requires information, a data message or a record to be presented in a specified non-electronic form, that requirement is satisfied if the information, data message or record in electronic form-

(a) is organized in substantially the same way;

(b) is accessible; and

(c) is capable of retention for subsequent reference.

Original form.

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

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

(b) it is presented to a person; and

(c) the information, data message or record 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, data message or record 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, data message or record was created.

Retention of information, data messages or records in electronic form.

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

Whether information, a data message or a record is capable of being retained.

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

Copies.

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

Electronically signed message deemed to be original document.

16. A copy of an electronic data message containing an electronic signature shall be as valid, enforceable and effective as a message containing a non-electronic signature.

Admissibility and evidential weight of electronic records.

17. An electronic data message or record will not be deemed inadmissible as evidence-

(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.

PART III
CONTRACT FORMATION AND DEFAULT PROVISIONS

Formation and validity of contracts.

18. In the context of contract formation, 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.

19. 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 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.

Involvement of electronic agents.

20. A contract may be formed between persons through the interaction of an electronic agent and a person or by the interaction of electronic agents.

Error that occur while dealing with an electronic agent.

21.(1) A contract concluded in an electronic environment through the interaction of a person and an electronic agent of another person is voidable where- -

(a) the first person referred 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) 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 received or used any material benefit or value from the other person..

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

Attribution of electronic data

22. An electronic data message or record is attributed to a

messages or records.

particular person if it resulted from an action of that person or through an agent or electronic agent of that person.

Acknowledgement of receipt of electronic data message or information.

23. Where a person issues an acknowledgement of receipt of an electronic data message or information, that acknowledgement of receipt validates an electronic transaction if, before sending the electronic data message or information or by means of that electronic data message or information, the originator has requested or has agreed with the addressee that receipt of the electronic data message or information be acknowledged.

Time of sending of electronic data message.

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

(a) when it enters an information system outside 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 or data message becomes capable of being retrieved and processed by the addressee.

Time of receipt of electronic records.

25. Unless the originator and address**ee** agree otherwise, if information or a data message in electronic form 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 or data messages in electronic form of the type sent; or

(b) upon the addressee becoming aware of the information 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 or data message in electronic form of the type sent.

Place of sending and receipt of information or record.

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

Place of business.

27. Unless the originator and addressee of a communication 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.

Habitual residence.

28. If the originator or addressee of a communication 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 communication.

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

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

signatures.

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

(b) it 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.

Regulations regarding electronic signatures.

32. The Minister may make regulations setting out a particular form of electronic signature to meet a specific legal requirement.

Electronic signature associated with an accredited certificate.

33. An electronic signature that is associated with a certificate issued by a certification service provider registered under Part V, (hereinafter referred to as an accredited certificate) is deemed to satisfy the requirements set out in section 31 for reliability and integrity.

PART V
CERTIFICATION SERVICE PROVIDERS

Registration of certification service providers.

34. No person shall issue accredited certificates to the public unless he is registered with the Data Commissioner as a certification service provider and has provided the information required by the Minister by Order.

Application for and grant of registration.

35.(1) Subject to section 43, a person wishing to be registered as a certification service provider in order to issue accredited certificates to the public, shall apply to the Data Commissioner in the manner prescribed and pay the prescribed fee.

(2) The application under subsection (1) shall include at a minimum a statement of compliance with the requirements set out in section 36.

(3) On receipt of an application, the Data Commissioner shall cause to be published in the *Gazette* and in at least one daily newspaper in circulation in Trinidad and Tobago, a notice stating that he has received and is reviewing the application.

(4) A notice under subsection (3) shall state the time, which shall not be less than fourteen days but no more than twenty-eight days from the date of publication of the notice, within which any comment on or objection to the application may be submitted to the Data Commissioner and the Data Commissioner shall consider the comments and objections prior to making a determination.

(5) The Data Commissioner shall make a determination in writing of the person's application for registration within thirty days of-

(a) receiving all relevant information pertinent to the application; or
(b) the period prescribed in subsection (4),

whichever is later, and shall cause that determination to be published in the *Gazette* and at least one daily newspaper.

(6) Where the Data Commissioner rejects the application, the person so affected may apply in writing for the reasons therefor within thirty days of publication of the decision, and the Data Commissioner shall respond in writing giving reasons no later than sixty days after receipt of such written request.

(7) If on the expiration of the period referred to in subsection (5), the Data Commissioner has not made a written determination in respect of the application, the application shall be deemed to be approved.

Requirements for a certification service provider that issues accredited

36. A certification service provider that issues accredited certificates to the public shall conduct his or its operations in a

certificates.

reliable manner and shall-

(a) employ personnel who possess the expert knowledge and experience required for these operations, especially with regard to management, technology 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 accredited certificates are issued;

(f) maintain a prompt and secure system for registration and immediate revocation of accredited certificates;

(g) take measures against forgery of accredited certificates and**,** where applicable**,** guarantee full confidentiality during the process of generating signature creation data;

(h) comply with section 57; and

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

Registry of certification service providers.

37. The Data Commissioner shall maintain a public registry of certification service providers that includes the information required by the Minister by Order.

Annual renewal of notification of compliance.

38. A registered certification service provider that issues accredited certificates shall annually provide the Data Commissioner with an updated notification of compliance with the requirements of

section 36 and pay the prescribed fee.

Audit by the Data Commissioner.

39.(1) The Data Commissioner may conduct an audit to verify that the certification service provider has been or remains in compliance with the requirements of this Act.

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

Responsibility to co-operate with an audit.

40. A certification service provider shall co-operate with and offer all reasonable assistance to the Data Commissioner while conducting an audit and shall make available information necessary to satisfy the Data Commissioner regarding compliance with the requirements of this Act.

Confidentiality.

41. 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 39, 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 Data Commissioner to deal with failure to meet requirements.

42. Where the Data Commissioner is satisfied that a certification service provider no longer meets the requirements to issue accredited certificates, he may-

(a) cancel the registration of the certification service provider;

(b) order the certification service provider to cease any or all of its activities, including the provision of accredited certificates;

(c) order the certification service provider to be removed from the registry;

(d) take any action that he deems reasonable to ensure that the certification service provider is in compliance with the requirements set out in section 36; or

(e) make any other order that the Data Commissioner deems reasonable in the circumstances including, but not limited to reimbursement of fees and charges to users of the certification service providers services or public notification of cessation of business.

Recognition of external certification service providers.

43.(1) The Minister may by Order recognize certificates or classes of certificates as accredited certificates issued by certification service providers or classes of certification service providers established in any other jurisdiction, as accredited certificates.

(2) Where the Minister makes an Order under subsection (1) the certification service providers named in the Order shall be deemed to be registered for the purposes of this Part and the Data Commissioner shall enter the names of such service providers in accordance with section 37.

Pseudonyms.

44. Certification service providers may**,** at the request of a particular signatory, indicate in the relevant certificate a pseudonym instead of the signatory's name.

Additional responsibilities of a certification service provider.

45. A certification service provider shall ensure the operation of a prompt and secure directory of certificate holders and a secure an immediate revocation service that make it possible to-

(a) check whether an accredited certificate is revoked;

(b) the validity period of the certificate; or

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

Immediate revocation upon

46.(1) A certification service provider shall revoke a

request.

certificate immediately upon the receipt of a request to do so by the signatory or if otherwise warranted in the circumstances.

(2) The certification service provider shall ensure that the date and time when a certificate is revoked can be determined precisely.

Liability of certification service provider issuing an accredited certificate.

47.(1) A certification service provider issuing an accredited certificate to the public is *prima facie* liable for any damages or loss caused to anyone relying on such a certificate due to the certificate provider not having met the requirements set forth in section 31 or section 36 or the certificate, when issued, having contained incorrect information.

(2) This section also applies to a certification service provider who guarantees that the certificates of another service provider are accredited.

Release from liability.

48.(1) A certification service provider issuing an accredited certificate may be exempted from liability if the provider can show that the injury or loss was not caused by its own negligence.

(2) The certification service provider is also not liable for damages for an injury or loss arising from the use of an accredited certificate in violation of any limitations of use or scope of transaction clearly stated in the certificate.

(3) This section also applies to a certification service provider who guarantees that the certificates of another service provider are accredited.

Costs of audit.

49. The Minister may order a certification service provider to pay the costs reasonably incurred in the performance of an audit pursuant to section 39 and may prescribe fees for the registration pursuant to section 34 and notification of compliance pursuant to section 38.

PART VI
INTERMEDIARIES AND TELECOMMUNICATIONS SERVICE PROVIDERS

Liability of intermediaries and telecommunications service providers.

50. An intermediary or telecommunications service provider who merely provides a conduit for the transmission of electronic data messages shall not be liable for the content of electronic data messages 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 intermediary network or who**,** upon acquiring actual knowledge or becoming aware of such facts, follows the procedures required by section 51 as soon as practicable.

Procedure for dealing with unlawful, defamatory etc information.

51. If an intermediary or telecommunications service provider has actual knowledge that the information in an electronic record or data message gives rise to criminal liability or liability for a tort may be reasonably believed to give rise to criminal liability or liability for a tort, the intermediary or telecommunications service provider shall as soon as practicable-

(a) notify the Telecommunications Authority of Trinidad and Tobago and if it considers it appropriate, notify the appropriate law enforcement authorities of the relevant information;

(b) where authorized by written law, disclose the Identity of the person for whom the intermediary was supplying services in respect of the information, if the identity of that person is known to the intermediary; and

(c) where authorized by written law, remove the information or data message from any information processing system within the intermediary's control and cease to provide or offer to provide services in respect of that information or take any other action authorized by law.

Role of the Telecommunications Authority of Trinidad and Tobago.

52. Where pursuant to section 51 the Telecommunications Authority of Trinidad and Tobago has been notified by an intermediary or telecommunications service provider of information in an electronic data message that gives rise to criminal liability or liability for a tort or that may be reasonably believed to give rise to criminal liability or liability for a tort, the Telecommunications Authority may take such action as it consider reasonable, including:

(a) notifying the appropriate law enforcement authorities;

(b) seeking an *ex parte* order of the Court to require removal of the information from the information processing system, disclosure of the identity of the person for whom the intermediary or telecommunications service provider was supplying services or any other action that the Court considers reasonable in the circumstances;

(c) requiring the disclosure of any and all records of the transfer or movement of the data message within the information processing systems under the control of the intermediary or telecommunications service provider or between such information and any other information systems.

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

53.(1) Where the Telecommunications Authority of Trinidad and Tobago or other designated agency 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 AUTHORITIES

General authorization.

54. In the absence of a specific legal provision that electronic means may not be used or that electronic means shall be used in a specific way, the Government of Trinidad and Tobago and other public authorities may use electronic means to create, collect, receive, store, transfer, distribute, publish or otherwise deal with records or information.

Forms and filings.

55. Subject to section 54**,** the authority under any law or regulation to issue, prescribe or in any other manner establish a form or to establish the manner of filing a document or submitting information, includes the authority to issue, prescribe or establish an electronic form or to establish an electronic manner of filing the document or submitting the information.

PART VIII
CONSUMER PROTECTION

Minimum information in e-commerce.

56.(1) Suppliers with a place of business in Trinidad and Tobago who knowingly use an intermediary or a telecommunications service provider based in Trinidad and Tobago for effecting an electronic transaction shall, before the conclusion of the electronic contract based on such transaction, provide certain information to consumers in respect of such electronic contract.

(2) The information shall include but not be limited to-

(a) the identity, address and telephone number of the supplier;

(b) a detailed description of the characteristics of the goods or services including any system or technical requirements;

(c) the amount to be paid including taxes, the currency in which the amount must be paid, the method of payment and the security arrangement for performance;

(d) the cancellation, refund or exchange policy;

(e) the expected date of delivery, where applicable;

(f) the privacy policy;

(g) a copy of the contract for the consumer in a format that can be retained;

(h) the arrangements for payment, delivery or performance; and

(i) the existence of a right of withdrawal.

(3) This section shall not apply to contracts concluded at an electronic auction.

Right of rescission.

57. A consumer who is not provided with the information required by section 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 .

Minimum information regarding electronic signatures.

58. Before entering into a contract requiring the issuance of an accredited certificate, a certification service provider shall inform the party seeking the certificate in writing of the following:

(a) the terms and conditions concerning the use of the certificate, 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 certificate and of using the other services of the certification authority;

(d) whether the certification authority is accredited under a voluntary accreditation scheme or by an accreditation body in another jurisdiction; and

(e) procedures for settlement of complaints.

Unwanted communications.

59. 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 consume**r** with a clearly specified and easily activated option to opt out of receiving future communications.

PART IX

CONTRAVENTION AND ENFORCEMENT

Failure to provide required information to consumers.

60. A person who fails to provide-

(a) the information to a consumer required by section 56;

(b) the information required by section 58,

commits an offence.

False or misleading information.

61. 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 signature with false or misleading information,

commits an offence.

Obstruction of an audit.

62. A person who with respect to an audit carried out pursuant to section 39 -

(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

63. A person who breaches the confidentiality obligations

obligations of confidentiality.

established by section 41 commits an offence.

Directors and officers.

64. Where a corporation commits an offence under this Act, any officer, director or agent of the corporation 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, whether or not the corporation has been prosecuted and convicted.

Penalties.

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

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

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

(3) Where a corporation 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 enterprise.

(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.

66. Every director and officer of a corporation shall take all reasonable care to ensure that the corporation 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.

67.(1) The Court shall have jurisdiction to hear and determine-

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

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

Regulations.

68.(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, 2009

Clerk of the House

I confirm the above.

Speaker

Passed in the Senate this day of , 2009

Clerk of the Senate

I confirm the above.

President.