ELECTRONIC TRANSACTIONS ACT

CHAPTER 22:05

Act
6 of 2011

Current Authorised Pages

Pages (inclusive)	*Authorised by L.R.O.*
1–32	..

UNOFFICIAL VERSION

L.R.O.

UPDATED TO DECEMBER 31ST 2012

Note on Subsidiary Legislation

This Chapter contains no subsidiary legislation.

Note on Proclamation

At the date of the Revision of this Act, Parts V, VI, VIII, IX and X had not yet been brought into operation. [*See* Section 1(2)].

CHAPTER 22:05

ELECTRONIC TRANSACTIONS ACT

ARRANGEMENT OF SECTIONS

SECTION

ARRANGEMENT OF SECTIONS—*Continued*

SECTION

PART III

CONTRACT FORMATION AND DEFAULT PROVISION

PART IV

ELECTRONIC SIGNATURE

PART V

ELECTRONIC AUTHENTICATION SERVICE PROVIDERS

SECTION

ARRANGEMENT OF SECTIONS—*Continued*

SECTION

PART IX

CONTRAVENTION AND ENFORCEMENT

PART X

MISCELLANEOUS

CHAPTER 22:05

ELECTRONIC TRANSACTIONS ACT

An Act to give legal effect to electronic documents, electronic records, electronic signatures and electronic transactions. 6 of 2011.

*[ASSENTED TO 28TH APRIL 2011]

PART I

PRELIMINARY

Short title and commencement. 1/2012. 8/2012.

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

*(2) Parts I, II, III and IV of this Act came into operation on 6th January 2012.

Part VII of this Act came into operation on 18th January 2012.

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;

"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;

"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;

See Section 1(2) for commencement dates of this Act. Also *see* Note on page 2.

"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;

"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;

"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; Ch. 1:01.

(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; Ch. 25:04.

(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 or controlled by the State;

(h) a Service Commission established under the Constitution or other written law; or Ch. 1:01.

(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. Ch. 47:31.

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 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 bodies, and to promote efficient delivery by public bodies 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—

(a) documents;

(b) records; or

(c) information,

to use, provide, accept or retain these in electronic form.

(2) Notwithstanding subsection (1), with regard to parties to 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.

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

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.

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

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.

Copies.

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.

Electronically signed message deemed to be original document.

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

Admissibility and evidential weight of electronic records.

17. Information or record in electronic form or a data message 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.

Electronic notarisation.

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 notarised, 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 authorised to perform those acts, together with all other information required to be included by other applicable 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 legal effect, validity or 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.

Error that occurs while dealing with an electronic agent.

22. (1) A contract concluded or a transaction undertaken in an electronic environment through the interaction of a person and an electronic agent of another person is void where—

(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.

Attribution of data messages or records.

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.

Time of sending of data message.

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

(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 data message.

26. Unless the originator and addressee agree otherwise, a data message is deemed to be sent from the originator's place of business and to be received at the addressee's place of business.

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 conforms with the standard which the parties have agreed to by contract.

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;

(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; and

(e) such other criteria as may be prescribed by Regulations.

(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.

(3) The electronic authentication products referred to in the Schedule are the products which can be used to validate an electronic signature under subsection (1).

(4) The Minister may by Order amend the Schedule.

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 an

authority as designated by the Minister by Order (hereinafter referred to as "the designated authority") and has provided the information prescribed under this Act.

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

(3) An Order under subsection (1) shall prescribe—

(a) the powers and functions of the designated authority; and

(b) any other matter relating to the designated authority which the Minister deems necessary for the purposes of this Part.

Application for registration.

34. (1) A person wishing to be registered as an accredited Electronic Authentication Service Provider (hereinafter referred to as "the applicant") shall apply to 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) proof of accreditation of its operations.

(3) Where an applicant has valid prior accreditation from another recognised jurisdiction, proof of accreditation shall be information relating to—

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

(b) the period of validity of the accreditation; and

(c) any other information required by Regulations as may be prescribed.

(4) Where an applicant has no valid prior accreditation, he shall indicate same to the designated authority who shall require the applicant to submit to an audit of his operations and systems to ensure compliance with the requirements of section 35 and any other standards which the Minister may prescribe by Regulations.

(5) Where the designated authority is satisfied that the applicant has met the requirements of this Act the designated authority may issue a notice of accreditation to the applicant.

(6) The Minister may make Regulations specifying the procedures for registration and accreditation.

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 recognised 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 designated authority is satisfied that an applicant has valid prior accreditation and has met the requirements of section 34, the designated authority may grant the registration.

(2) Where the designated authority is satisfied that an applicant who has no valid prior accreditation has met the requirements of sections 34 and 35, 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 recognise a qualified electronic authentication product or classes of qualified electronic authentication products 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 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 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 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 designated authority may employ whatever experts it 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 designated authority while conducting an audit and shall make available information necessary to satisfy 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 the designated authority to deal with failure to meet requirements.

43. Where 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 accreditation 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 35; or

(e) make any other order that 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 designated authority may require an Electronic Authentication Service Provider to pay the costs reasonably incurred in the performance of an audit pursuant to section 40.

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, 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.

(4) An intermediary or a telecommunications service provider, during an audit, shall not be liable under the Copyright Act in respect of— Ch. 82:80.

(a) the infringement of copyright in any work or other subject matter in which copyright subsist; or

(b) the unauthorised use of any public performance, the duration of which the copyright period has not expired.

(5) For the purposes of this section, "public performance" has the same meaning as in the Copyright Act.

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 and secure 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 authorised by written law or in accordance with the established code of conduct; and

(b) in the case of criminal liability, notify 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) 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, this section.

(3) 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 subsection (1).

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

52. (1) The Minister may develop codes of conduct and standards for intermediaries and telecommunications service providers for the purposes of this Act.

(2) 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.

(3) 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 authorisation.

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 body 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 body 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 in Trinidad and Tobago or knowingly uses an intermediary or a telecommunications service provider 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; or

(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.

Liability of directors and officers.

62. Where a body corporate commits an offence under this Act, any officer, director or agent of the body corporate who directed, authorised, assented to 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.

Penalties.

63. (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; 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 not exceeding 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 for any Order which the Court considers appropriate to facilitate the enforcement of any provisions of this Act; or

(b) upon an application 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.

Section 31.

SCHEDULE

ELECTRONIC AUTHENTICATION PRODUCTS USED TO VALIDATE ELECTRONIC SIGNATURES

Electronic certificates.
