

ANTIGUA AND BARBUDA
THE ELECTRONIC TRANSACTIONS BILL, 2006
ARRANGEMENT OF SECTIONS

Sections

Part 1 – Preliminary

1. Short title and commencement.
2. Interpretation.
3. Exclusions.
4. Variation by agreement.

Part II - Legal Requirements Respecting Electronic Records

5. Legal recognition of electronic records.
6. Writing.
7. Delivery.
8. Original form.
9. Retention of records.
10. Records available for inspection.
11. Admissibility of electronic records.
12. Other requirements.

Part III E-Government Services

13. State to be bound.
14. Acceptance of electronic filing and issuing of documents.
15. Requirements may be specified.

Part IV - Formation and Validity of Contracts

16. Formation and validity of contracts.

Part V - Communication of Electronic Records

17. Attribution of electronic records.
18. Effect of change or error.
19. Acknowledgement of receipt of electronic records.
20. Time and place.

Part VI - Electronic Signatures

21. Equal treatment of signatures.
22. Compliance with a requirement for a signature.
23. Determination of standards.
24. Conduct of a person relying on an electronic signature.
25. Recognition of foreign certificates and electronic signatures.

Part VII - Information Security Service Providers

26. Register of approved providers.
27. Arrangements for the grant of approvals.
28. Provision of information security services.
29. Conduct of the information security service provider.
30. Criteria for determining trustworthiness.
31. Contents of a certificate.
32. Conduct of the signature device holder.
33. Penalty for publishing Digital Signature Certificate false in certain particulars.
34. Publication for fraudulent purposes

Part VIII – Liability of Intermediaries and Service Providers

- 35. Mere conduit.
- 36. Caching.
- 37. Hosting.
- 38. Information location tools.
- 39. Take-down notification.
- 40. Monitoring and compliance.
- 41. Code of Practice

Part IX – Miscellaneous

- 42. Consumer Protection
- 43. Offences by bodies corporate
- 44. Appointment of e-Business Advisory Board
- 45. Regulations

ANTIGUA AND BARBUDA

NO. OF 2006

BILL FOR

AN ACT to establish the legal principles applicable to the conduct of electronic commerce and the processing, verification and attribution of electronic records; to provide for the approval, registration and liabilities of service providers and for incidental and connected purposes

| |

ENACTED by the Parliament of Antigua and Barbuda as follows—

**Short title and
Commencement**

1. This Act may be cited as the Electronic Transaction Act 2006.

Interpretation

2. In this Act unless the context requires otherwise –

“addressee”, in relation to an electronic record, means a person who is intended by the originator to receive the electronic record, but does not include a person acting as an intermediary with respect to that electronic record;

“Board” means the e-Business Advisory Board appointed under section 44;

“cache” means high speed memory that stores data for relatively short periods of time, under computer control, in order to speed up data transmission or processing;

“certificate” means an electronic record which purports to ascertain the identity of a person or entity who at the time of creation of that record controls a particular signature device;

“deliver” includes give, serve and file;

“electronic” means relating to technology having electrical, magnetic, optical, electromagnetic, or similar capabilities, whether digital, analogue or otherwise;

“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 an electronic record or event in whole or in part, without review by an individual;

"electronic commerce" means the type of business engaged in by e-commerce service providers;

“electronic record” means a record processed and maintained by electronic means;

“electronic signature” means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record;

“information” includes electronic records, data, text, images, sounds, codes, computer programs, software and databases;

“information processing system” means an electronic system for generating, sending, receiving, storing or otherwise processing information;

“information security service” and “information security procedure” includes a service or procedure which is provided to an originator, intermediary, or recipient of an electronic record, and which is designed to –

- (a) secure that the record can be accessed, or can be put into an intelligible form, only by certain persons; or
- (b) secure that –
 - (i) the authenticity;
 - (ii) the time of processing; or
 - (iii) the integrity, of such a record, is capable of being ascertained;

“intermediary”, with respect to an electronic record, means a person who sends, receives, stores, processes or provides other services with respect to that electronic record for another person;

“Minister” means the minister for the time being responsible for telecommunications;

“originator”, in relation to an electronic record, means a person who –

- (a) sends an electronic record;
- (b) instructs another to send an electronic record on his behalf; or
- (c) has an electronic record sent by his electronic agent, but does not include –
 - (i) a person who sends an electronic record on the instructions of another; or
 - (ii) a person acting as an intermediary with respect to that electronic record;

“prescribed” means prescribed in regulations made by the Minister;

“process”, in relation to an electronic record, means to create, generate, send, transmit, receive, store, communicate, modify or display the record;

"public body" means—

- (a) any department of state or administration in the national sphere of government or any municipality in the local sphere of government; or
- (b) any other functionary or institution when—
 - (i) exercising a power or performing a duty in terms of the Constitution; or
 - (ii) exercising a power or performing a function in terms of any legislation;

“record” means information that is inscribed, stored or otherwise maintained on a tangible medium or that is stored in an electronic or any other medium and is accessible in a perceivable form;

“transaction” means a transaction whether or not for consideration and whether or not of a commercial nature.

- Exclusions**
3. (1) Nothing in this Act shall apply to —
- (a) the grant of a Power-of-Attorney;
 - (b) a trust ;
 - (c) a will ;
 - (d) any contract for the sale or conveyance of immovable property or any interest in such property;
 - (e) the swearing of affidavits or statutory declarations before a Commissioner of oaths and notary public or
 - (f) the authentication of documents if specifically required to be done by law after a physical inspection and comparison with an original of such document where the original does not exist in electronic data format and has subsequently not be reduced into an electronic data format which integrity is not challenged by the originator of such document.
- (2) The Minister may provide by regulations subject to affirmative resolution that this Act, or such of its provisions as may be specified in the regulations-
- (a) shall not apply to any class of transactions, persons, matters or things; or
 - (b) shall apply to any class of transactions, persons, matters or things specified under paragraphs (a) to (g).
- Variation by agreement**
4. The Provisions of Part II, IV, V and VI (except sections 18 (b) and (c), 23 and 25 (2) to (6)) may be varied or excluded by agreement.

Part II - Legal Requirements Respecting Electronic Records

- | | | |
|--|----|--|
| Legal
recognition of
electronic
records | 5. | Information shall not be denied legal effect or validity solely on the ground that it is -
(a) in the form of an electronic record; or
(b) referred to but not contained in an electronic record. |
| Writing | 6. | (1) Where a document, record or information is required or permitted by any statutory provision or rule of law or by contract to be in writing, or is described in any statutory provision or contract as being written, that requirement, permission or description may be met by information in the form of an electronic record.

(2) Subsection (1) shall apply if the requirement for the document, record or information to be in writing is in the form of an obligation or if the statutory provision or rule of law or contract provides consequences if it is not in writing. |
| Delivery | 7. | (1) Where a document, record or information is required or permitted by any statutory provision or rule of law or by contract to be delivered or sent to a person, that requirement or permission may be met by delivery of it in the form of an electronic record if –
(a) the format of the electronic record and the means of delivery is acceptable to the parties; and
(b) where the originator of the electronic record states that the receipt of the electronic record is to be acknowledged, the addressee has knowingly acknowledged the receipt.

(2) Subsection (1) applies whether or not the requirement for delivery or sending is in the form of an obligation or whether or not the statutory provision, rule of law, contract provides consequences for the document, record or information not being delivered or sent. |
| Original
form | 8. | (1) (a) Where a statutory provision, rule of law, or contract requires conclusive evidence of the original form of a document, record or information to be presented or retained that requirement shall be met by the presentation or retention of an electronic record if the document, record or information is accurately represented therein.

(b) Paragraph (a) shall apply if the requirement for the presentation or retention of evidence of the original form of document, record or information is in the form of an obligation or if the statutory provision, rule of law, contract |

provides consequences if conclusive evidence of the original form of document, record or information is not provided.

- (2) (a) Where a statutory provision, rule of law, or contract requires a document, record or information to be presented or retained in its original form and such document, record or information was first generated in its final form as an electronic record, that requirement shall be met by the presentation or retention of an electronic record if the document, record or information is accurately represented therein.
- (b) Paragraph (a) shall apply if the requirement to present or retain the document, record or information in its original form is in the form of an obligation or if the statutory provision, rule of law or contract provides consequences if the original form of the document, record or information is not presented or retained.

- (3) For the purposes of subsections (1) and (2) the document, record or information is accurately represented where it has remained complete and unaltered from the time it was first generated in its final form, whether as an electronic record or on any other medium, apart from the application of an information security procedure, or apart from –
 - (a) the addition of an endorsement; or
 - (b) an immaterial change, which arises in the normal course of communication, translation, conversion, storage or display.

Retention of records

- 9. (1) Where documents, records or information are required by any statutory provision or rule of law or by contract [or by deed] to be retained, that requirement is met by retaining them in the form of electronic records if –
 - (a) the information contained in the electronic record is accessible and capable of retention for subsequent reference;

- (b) the electronic record is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the document, record or information when it was generated, sent or received;
- (c) any information that enables the identification of the origin and destination of an electronic record and the date and time when it was sent and received is retained; and
- (d) appropriate steps are taken to ensure the security of such electronic records in compliance with guidelines which may be prescribed in regulations made by the Minister.

- (2) An obligation to retain documents, records or information, in accordance with subsection (1) does not extend to information, the sole purpose of which is to enable the message to be sent or received.
- (3) A person may satisfy the requirement referred to in subsection (1) by using the services of another person, if the conditions set out in subsection (1)(a), (b), (c) and (d) are met.

Records available for inspection	10.	Where documents, records or information are required by any statutory provision or rule of law or by contract or by deed to be made available for inspection, that requirement shall be met by making such documents, records or information available for inspection in perceivable form as an electronic record.
Admissibility of electronic records	11.	In proceedings in a court, tribunal or arbitration, whether of a legal, judicial, quasi-judicial or administrative nature, the admissibility of an electronic record or an electronic signature in evidence shall not be denied solely on the grounds that it is an electronic record or an electronic signature.
Other requirements	12.	(1) A requirement in law for multiple copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single electronic record that is capable of being reproduced by that addressee.

- (2) An expression in a law, whether used as a noun or verb, including the terms "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to an electronic record unless otherwise provided for in this Act.
- (3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

Part III E-Government Services

State to be bound

- 13. (1) This Act binds the State.
- (2) Notwithstanding subsection (1), nothing in this Act shall require a ministry or public body to process an electronic record, but either the Minister or the appropriate minister or official member may, by notice published in the Gazette, indicate that a ministry or public body will process electronic records relating to such matters as may be specified in the notice.
- (3) Until a notice under subsection (2) has been published, no person dealing with such ministry or public body shall be entitled, by means of an electronic record, to satisfy a requirement to process a record.
- (4) The State, the Minister, or any employee of the State shall not be liable in respect of any act or omission in good faith and without gross negligence in performing a function in terms of this Act.

Acceptance of electronic filing and issuing of documents

- 14. Any public body that, pursuant to any law -
 - (a) accepts the filing of documents, or requires that documents be created or retained;
 - (b) issues any permit, licence or approval; or
 - (c) provides for a manner of payment; maynotwithstanding anything to the contrary in such law -

- (i) accept the filing of such documents, or the creation or retention of such documents in the form of electronic records;
- (ii) issue such permit, licence or approval in the form of an electronic record; or
- (iii) make or receive payment in electronic form or by electronic means.

**Requirements
may be
specified**

15. (1) In any case where a public body performs any of the functions referred to in section 14, such body may specify by notice in the *Gazette*-
- (a) the manner and format in which the electronic records must be filed, created, retained or issued;
 - (b) in cases where the electronic record has to be signed, the type of electronic signature required;
 - (c) the manner and format in which such electronic signature must be attached to, incorporated in or otherwise, associated with the electronic record;
 - (d) the identity of or criteria that must be met by any authentication service provider used by the person filing the electronic record or that such authentication service provider must be a preferred authentication service provider;
 - (e) the appropriate control processes and procedures to ensure adequate integrity, audit ability, security and confidentiality of electronic records or payments; and
 - (f) any other requirements for electronic records or payments.

Part IV - Formation and Validity of Contract

**Formation
and validity
of contracts**

16. (1) In the context of the information of a contract -
- (a) an offer;
 - (b) subject to any condition included in the offer

- (notwithstanding section 2), the acceptance of an offer; and
- (c) the method of payment of any consideration payable, may be expressed by an electronic record.
- (2) As between the originator and the addressee of an electronic record, a declaration of intention or other statement shall not be denied legal effect or validity solely on the ground that it is in the form of an electronic record.

Part V - Communication of Electronic Records

**Attribution of
electronic
records**

17. (1) An electronic record is that of an originator if it was sent by the originator himself.
- (2) As between the originator and the addressee, an electronic record shall be attributable to the originator if it was sent -
- (a) by a person who had been authorised by the originator to send the electronic record on his behalf; or
 - (b) by the originator's electronic agent.
- (3) As between the originator and the addressee, an addressee shall be entitled to attribute an electronic record to the originator, and to act on that assumption, if -
- (a) in order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
 - (b) the electronic record as received by the addressee resulted from the actions of a person whose relationship with the originator, or with any agent of the originator, enabled that person to gain access to a method used by the originator to identify electronic records as his own.
- (4) Subsection (3) shall not apply -
- (a) as of the time when the addressee has both received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly; or
 - (b) in a case to which subsection (3)(b) applies, at any time when the addressee knew or should have known, had he

exercised reasonable care or used any agreed procedure, that the electronic record was not that of the originator.

- (5) The addressee shall be entitled to regard each electronic record received as a separate electronic record and to act on that assumption, except to the extent that it duplicates another electronic record and the addressee knew or should have known, had he exercised reasonable care or used any agreed procedure, the electronic record was a duplicate.

**Effect of
change or
error**

18. If a change or error occurs in the transmission of an electronic record -

- (a) If the originator and the addressee have agreed to use an information security procedure in respect of the electronic record and one of them has conformed to the procedure, but the other has not, and the nonconforming person would have detected the change or error had he also conformed, the conforming person may avoid the effect of the changed or erroneous electronic record;
- (b) if an individual is either the originator or the addressee of an electronic record, he may avoid the effect of the electronic record if the error was made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual-
- (i) promptly notifies the other person of the error and that he did not intend to be bound by the electronic record received by the other person;
- (ii) takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and
- (iii) has not used or received any benefit or value from the consideration, if any, received from the other person; and
- (c) if neither paragraph (a) nor paragraph (b) applies, the change or error shall have the effect provided by any other law and any contract between the originator and the addressee;

**Acknowledge-
ment of receipt
of electronic**

19. (1) Subscriptions (2), (3) and (4) shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested, or agreed with, the addressee that

records

receipt of the electronic record be acknowledged by the addressee.

- (2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by –
 - (a) a communication by the addressee to the originator, automated or otherwise; or
 - (b) the conduct of the addressee,

that is reasonably sufficient to indicate to the originator, the electronic record has been received.

- (3) Where the originator has stated that an electronic record is conditional, on receipt by him of an acknowledgement, the record shall be presumed not to have been sent until an acknowledgment has been received by him.

- (4) Where the originator has not stated that the electronic record is conditional on receipt of the acknowledgement and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator -

- (a) may give notice to the addressee –
 - (i) stating that no acknowledgement has been received and that the electronic record is to be treated as though it had never been sent; or
 - (ii) specifying a reasonable time by which the acknowledgement must be received; and
- (b) if the acknowledgement is not received within the time specified in paragraph (a), may, upon notice to the addressee –
 - (i) treat the electronic record as though it had never been sent; and
 - (ii) exercise any other rights the originator may have.

- (5) Where the originator receives the addressee's acknowledgement of receipt it may be presumed that the related electronic record has

been received by the addressee but that presumption shall not imply that the electronic record received corresponds to the electronic record as sent.

- (6) Where the addressee's received acknowledgment states that the related electronic record met technical requirements that the originator and the addressee have agreed should be met, it shall be presumed that the requirements have been met.
- (7) Except in so far as it relates to the sending or receipt of an electronic record, this section shall not affect the legal or equitable consequences that may flow either from that electronic record or from the acknowledgement of its receipt.

Time and place 20.

- (1) Unless the originator and addressee agree otherwise, information or a record in electronic form is sent when it enters an information system outside the control of the originator or, if the originator and the addressee are in the same information system, if the information or record becomes capable of being retrieved and processed by the addressee.
- (2) If information or a record is capable of being retrieved and processed by an addressee, the information or record in electronic form is deemed, unless the contrary is proven, 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 records in electronic form of the type sent, or
 - (b) if the addressee has not designated or does not use an information system for the purpose of receiving information or records in electronic form of the type sent, on the addressee becoming aware of the information or record in the addressee's information system.

Part VI - Electronic Signatures

Equal treatment of

- 21. Except as provided in section 22, the provisions of this law shall not be applied so as to exclude, restrict, or deprive of legal effect, any method

signatures

of creating an electronic signature which -

- (a) satisfies the requirements of section 22 (1); or
- (b) otherwise, meets the requirements of an applicable statutory provision, rule of law, contract.

Compliance
with a require-
ment for a
signature

22.

- (1) Where the signature of a person is required by a statutory provision, rule of law or contract, that requirement shall be met in relation to an electronic record if an electronic signature is used that is as reliable and as appropriate for the purpose for which the electronic record was generated or communicated, in all the circumstances, including any relevant agreements.
- (2) Subsection (1) applies whether the requirement for a signature is in the form of an obligation or the statutory provision, rule of law, contract provides consequences for the absence of a signature.
- (3) An electronic signature shall be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if -
 - (a) the means of creating the electronic signature is, within the context in which it is used, linked to the signatory and to no other person;
 - (b) the means of creating the electronic signature was, at the time of signing, under the control of the signatory and of no other person;
 - (c) any alteration to the electronic signature, made after the time of signing, is detectable; and
 - (d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
- (4) Sub-section (3) does not limit the ability of any person -
 - (a) to establish in any other way, for the purpose of satisfying the requirement referred to in sub-section (1), the reliability of an electronic signature; or
 - (b) to adduce evidence of the non-reliability of an electronic signature.

- | | | |
|--|-----|---|
| Determination of standards | 23. | The Minister may make regulations prescribing methods which satisfy the requirements of Section 22. |
| Conduct of a person relying on an electronic signature | 24. | <p>A person relying on an electronic signature shall bear the legal consequences of his failure to -</p> <ul style="list-style-type: none">(a) take reasonable steps to verify the reliability of an electronic signature; or(b) where an electronic signature is supported by a certificate, take reasonable steps to –<ul style="list-style-type: none">(i) verify the validity, suspension or revocation of the certificate; or(ii) observe any limitation with respect to the certificate |
| Recognition of foreign certificates and electronic signatures | 25. | <ul style="list-style-type: none">(1) In determining whether, the extent to which, a certificate or an electronic signature is legally effective, no regard shall be had to the place where the certificate or the electronic signature was issued, nor to the jurisdiction in which the issuer had its place of business.(2) If the Minister considers that the practices of a foreign information security service provider provide a level of reliability at least equivalent to that required of information security service providers in order that they may be approved under Part VII, he may by notice published in the Gazette recognise certificates or classes of certificates issued by the foreign provider as legally equivalent to certificates issued by information security service providers approved under Part VII.(3) The Minister may, by notice published in the Gazette, recognise signatures complying with the laws of a foreign jurisdiction relating to electronic signatures as legally equivalent to signatures issued by information security service providers approved under [relevant law relating to information security service providers] if the laws of the other foreign jurisdiction require a level of reliability at least equivalent to that required for such signatures under this Act. |

- (4) The Minister may make regulations prescribing the matters to be taken into account by the Minister when deciding whether to exercise his powers under subsections (2) and (3).
- (5) Notwithstanding subsections (2) and (3), parties to commercial and other transactions may specify that a particular information security service provider, class of information security service providers or class of certificates shall be used in connection with messages or signatures submitted to them.
- (6) Where, notwithstanding subsections (2) and (3), the parties to a transaction agree to the use of particular types of electronic signatures and certificates, that agreement shall be recognised as sufficient for the purpose of cross-border recognition in respect of that transaction.

Part VII - Information Security Service Providers

- | | | |
|---------------------------------------|-----|---|
| Register of approved providers | 26. | <ul style="list-style-type: none">(1) The Minister may establish and maintain a register of approved information security services, and of providers of such services, which shall contain particulars of every person who, or service which, is for the time being approved under any arrangements in force under section 27.(2) The Minister may make regulations prescribing the particulars that are to be included in entries in the register maintained under subsection (1).(3) The Minister shall -<ul style="list-style-type: none">(a) allow public inspection at all times of an electronic copy of the register; and(b) publicise any withdrawal or modification of an approval under section 27, in accordance with arrangements prescribed by the Minister in regulations. |
| Arrangements for the grant | 27. | The Minister may make regulations enabling the Minister to grant approvals, whether subject to conditions or otherwise, on payment of a |

- (i) the identity of the information security service provider;
 - (ii) that the person who is identified in the certificate had control of the signature device at the time of signing;
 - (iii) that the signature device was operational on or before the date when the certificate was issued;
- (d) provide reasonably accessible means which enable a person who relies on the certificate to ascertain, where relevant, from the certificate or otherwise –
- (i) the method used to identify the signature device holder;
 - (ii) any limitation on the purpose or value for which the signature device or the certificate may be used;
 - (iii) that the signature device is operational and has not been compromised;
 - (iv) any limitation on the scope or extent of liability stipulated by the information security service provider;
 - (v) whether means exist for the signature device holder to give notice that a signature device has been compromised; and
 - (vi) whether a timely revocation service is offered;
- (e) provide a means for a signature device holder to give notice that a signature device has been compromised and ensure the availability of a timely revocation service; and
- (f) utilise trustworthy systems, procedures and human resources in performing its services.
- (2) An information security service provider shall be liable for its failure to satisfy the requirements of subsection (1).

Criteria for determining trustworthiness 30. The Minister may make regulations prescribing the factors to which regard shall be had in determining whether, and the extent to which, systems, procedures and human resources are trustworthy for the purposes of section 29 (1) (f).

- Contents of a certificate** 31. The Minister may make regulations prescribing the matters that shall be specified in a certificate.
- Contents of the signature device holder** 32. A signature device holder shall -
- (a) exercise reasonable care to avoid unauthorised use of its signature device;
 - (b) without undue delay, notify any person who may reasonably be expected by the signature device holder to rely on or to provide services in support of the electronic signature if –
 - (i) the signature device holder knows that the signature device has been compromised; or
 - (ii) the circumstances known to the signature device holder give rise to a substantial risk that the signature device may have been compromised; and
 - (c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signature device holder, which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.
- Penalty for Publishing Digital Signature Certificate false in certain particulars** 33. (1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with knowledge that -
- (a) the Certifying Authority listed in the certificate has not issued it with a license; or
 - (b) the subscriber listed in the certificate has not accepted it; or
 - (c) the license or issue of Digital Signatures or the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
- (2) Any person who contravenes the provisions of sub-section (1) commits an offence and shall upon conviction be liable to imprisonment for a term which not exceeding to three years, or with fine not exceedingor both.

- Publication for fraudulent purpose** 34. Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose commits an offence and shall upon conviction be liable to imprisonment for a term not exceeding five years, or with a fine not exceeding thirty thousand dollars or both.

Part VIII – Liability of Intermediaries and Service Providers

- Mere conduit** 35. (1) the intermediary or service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of electronic records via an information system under its control, as long as the intermediary or service provider—
- (a) does not initiate the transmission;
 - (b) does not select the addressee;
 - (c) performs the functions in an automatic, technical manner without selection of the electronic record; and
 - (d) does not modify the electronic record contained in the transmission.
- (2) The acts of transmission, routing and of provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place—
- (a) for the sole purpose of carrying out the transmission in the information system;
 - (b) in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and
 - (c) for a period no longer than is reasonably necessary for the transmission.
- Caching** 36. An intermediary or service provider that transmits an electronic record provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage

of that electronic record, where the purpose of storing such electronic record is to make the onward transmission of the electronic record more efficient to other recipients of the service upon their request, as long as the service provider—

- (a) does not modify the electronic record;
- (b) complies with conditions on access to the electronic record;
- (c) complies with rules regarding the updating of the electronic record, specified in a manner widely recognised and used by industry;
- (d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain information on the use of the electronic record; and
- (e) removes or disables access to the electronic record it has stored upon receiving a take-down notice referred to in section 39.

Hosting

37. (1) An intermediary or service provider that provides a service that consists of the storage of electronic records provided by a recipient of the service, is not liable for damages arising from information stored at the request of the recipient of the service, as long as the service provider—

- (a) does not have actual knowledge that the information or an activity relating to the information is infringing the rights of a third party; or
- (b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the information is apparent; and
- (c) upon receipt of a take-down notification referred to in section 39, acts expeditiously to remove or to disable access to the information.

(2) The limitations on liability established by this section do not apply to a service provider unless it has designated an agent to receive notifications of infringement and has provided through its services, including on its web sites in locations accessible to the public, the name, address, phone number and e-mail address of the agent.

(3) Subsection (1) does not apply when the recipient of the service is acting under the authority or the control of the service provider.

- Information location tools**
38. An intermediary or service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing electronic record or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the intermediary or service provider—
- (a) does not have actual knowledge that the electronic record or an activity relating to the electronic record is infringing the rights of that person;
 - (b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the electronic record is apparent;
 - (c) does not receive a financial benefit directly attributable to the infringing activity; and
 - (d) removes, or disables access to, the reference or link to the electronic record or activity within a reasonable time after being informed that the electronic record or the activity relating to such electronic record, infringes the rights of a person.
- Take-down notification**
39. (1) For the purposes of this Part, a notification of unlawful activity must be in writing, must be addressed by the complainant to the intermediary or service provider or its designated agent and must include—
- (a) the full names and address of the complainant;
 - (b) the written or electronic signature of the complainant;
 - (c) identification of the right that has allegedly been infringed;
 - (d) identification of the material or activity that is claimed to be the subject of unlawful activity;
 - (e) the remedial action required to be taken by the intermediary or service provider in respect of the complaint;
 - (f) telephonic and electronic contact details, if any, of the complainant;
 - (g) a statement that the complainant is acting in good faith;

- (h) a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct; and
 - (2) Any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts commits an offence and is liable for damages for wrongful take-down.
 - (3) An intermediary or service provider is not liable for wrongful take-down in response to a notification.
- Monitoring and compliance**
40. (1) An intermediary or service provider shall not be required to monitor any electronic record processed by means of his 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.
- (2) Except as provided by subsection (1), nothing in this section shall relieve an intermediary or service provider from -
- (a) any obligation to comply with an order or direction of a court or other competent authority; or
 - (b) any contractual obligation.
- Code of practice**
41. (1) The Minister may by regulations establish standards or conduct requirements with which service providers or intermediaries carrying on business in or from within Antigua and Barbuda must comply.
- (2) A standard established by regulations made under subsection (1) may relate to one or more of the following matters -
- (a) the types of services that are permitted to be provided by intermediaries;
 - (b) the types of customers to whom services may be provided by intermediaries;
 - (c) the types of information permitted to be contained in an electronic record for which services are provided by intermediaries;

- (d) the contractual application of relevant codes of conduct or standards to customers of intermediaries and service providers;
 - (e) the information to be disclosed by intermediaries and service providers including the name, address, e-mail address and contact and registration details;
 - (f) the actions to be taken in the event of customers of intermediaries or service providers sending bulk, unsolicited electronic records;
 - (g) the practical application of the relevant laws of Antigua and Barbuda to intermediaries and service providers;
 - (h) procedures for dealing with complaints;
 - (i) procedures for dispute resolution, including dispute resolution by electronic means; and
 - (j) such other matters as the Minister may require.
- (3) Regulations made under subsection (1) shall provide -
- (a) that an intermediary or service provider who fails to comply with a standard prescribed in the regulations shall in the first instance be given a written warning by the Minister;
 - (b) that the Minister may direct that person to cease or correct his practices; and
 - (c) that if that person fails to do so within such period as may be stated in the direction, he commits an offence and shall be liable to such penalties as may be prescribed.
- (4) If the Minister is satisfied that a person, body or organisation represents intermediaries or service providers carrying on business in Antigua and Barbuda, the Minister may, by notice given to the person, body or organisation, request that person, body or organisation to -
- (a) develop standards or conduct requirements that apply to intermediaries or service providers and that deal with one or more specified matters relating to the provision of services by those intermediaries or service providers; and

- (b) provide details relating to those standards or conduct requirements to the Minister within such time as may be specified in the request.
- (5) If the Minister is satisfied with the standards and conduct requirements provided under subsection (4), he shall approve such standards and conduct requirements by notice published in the Gazette and thereupon such standards and conduct requirements shall apply to such intermediaries or service providers as may be specified in the notice.
- (6) If the Minister has approved any standard or conduct requirement that applies to intermediaries or service providers, and
 - (a) he receives notice from a person, body or organisation representing intermediaries or service providers or proposals to amend the standard or conduct requirement; or
 - (b) he no longer considers that the standard or conduct requirement is appropriate, he may by notice published in the Gazette, revoke or amend any existing standard or conduct requirement.
- (7) References in this section to intermediaries and service providers include references to a particular class of intermediaries or to a particular class of service providers.

Part IX – Miscellaneous

- | | | |
|--------------------------------|-----|--|
| Consumer
Protection | 42. | <ul style="list-style-type: none">(1) A person using electronic communications to sell goods or services to consumers shall provide accurate, clear and accessible information about themselves, sufficient to allow:<ul style="list-style-type: none">(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;(c) service of legal process.(2) A person using electronic communications 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 records of the information.

- (3) A person using electronic communications to sell goods or services to consumers shall provide information about the terms, conditions and costs associated with a transaction, and notably:
 - (a) terms, conditions and methods of payment; and
 - (b) details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information.

**Offences by
bodies
corporate**

- 43. (1) Where an offence under this Act, which has been committed by a body corporate, is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the body corporate, or any person who was purporting to act in any such capacity, he, as well as the body corporate, shall be guilty of that offence and be liable to be proceeded against and punished accordingly.
- (2) Where the affairs of a body corporate are managed by its members, subsection (1) shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

**Appointment
of e-Business
Advisory
Board**

- 44. (1) The Minister shall appoint a Board, to be known as the e-Business Advisory Board.
- (2) The Board shall advise the Minister-
 - (a) on the discharge of their functions under this Act;
 - (b) on any matter connected with the functions referred to in paragraph (a);
 - (c) on any matter connected with the administration of this Act; and
 - (d) on any matter referred to it by the Minister that is connected or relates to the matters dealt with by this Act.
- (3) The members of the Board shall hold office at the pleasure of the Minister and notwithstanding any other enactment may provide their advice on a voluntary basis.
- (4) The Board shall consist of not less than seven, nor more than ten persons appearing to the Minister to be knowledgeable and

experienced about electronic business, the Internet, E-Commerce, technology law or electronic transactions.

- (5) The Board shall, at their first meeting, and at the first meeting in every calendar year thereafter, appoint one of their member to be the chairman of the Board until the date of the first meeting of the Board in the following calendar year.
- (6) The Board shall determine its own procedure.

- Regulations** 45. (1) Without derogating from the powers to make regulations conferred elsewhere in this Act, the Minister may make regulations -
- (a) prescribing matters required or permitted by this Act to be prescribed;
 - (b) authorising or facilitating -
 - (i) the investigation of; or
 - (ii) the bringing of, criminal proceedings in respect of, the processing of electronic records that may be, or is, an offence under this or any other Act; or
 - (c) for carrying the purpose and provisions of this Act into effect.
- (2) Regulations made under this Act may provide that the contravention of any provision constitutes an offence and may prescribe penalties for any such offence not exceeding the maximum fine and term of imprisonment prescribed in this Act for any offence under this Act.

Passed by the House of Representatives
this day of 2006.

Passed by the Senate
this day of 2006.

Speaker

President

THE ELECTRONIC TRANSACTIONS BILL, 2006

EXPLANATORY MEMORANDUM

The objects of this Bill are -

- (a) to facilitate modern business and commerce in Antigua and Barbuda;
- (b) to facilitate electronic transactions on a technology neutral basis by means of reliable electronic records;
- (c) to remove uncertainties in relation to conducting transactions electronically with respect to the requirements for documents and for signatures to be in writing;
- (d) to promote public confidence in the validity, integrity and reliability of conducting transactions electronically; and
- (e) to promote the development of the legal and business infrastructure necessary to implement electronic transactions securely.

The Bill will provide that transactions carried out by electronic means are regulated in a manner that –

- (a) permits and encourages the growth of business by electronic means through the operation of free market forces;
- (b) promotes the greatest possible use of industry self-regulation;
- (c) is flexible; and
- (d) is technologically neutral.

Clause 3 provides that the bill when passed shall not apply to powers of attorney, trusts, testamentary documents, contracts for sale or conveyance of land, the swearing of affidavits or statutory declarations, or the authentication of documents where required by law after a physical inspection and comparison, with an original, of such document where the original does not exist in electronic data format and has subsequently not be reduced into an electronic data format which integrity is not challenged by the originator of such document and for the passage of regulations that will be able to prescribe further exclusions. This clause also allows the Minister to provide by regulations that the Act applies to any of these specified documents and transactions and may not apply to any class of transaction, persons or things.

Clause 4 enables parties to transactions to agree that certain sections shall not apply or shall apply with amendments.

Clause 5 provides that the use of electronic communication shall not, by itself, invalidate a communication or its contents. This clarifies the legal recognition of electronic communication.

Clause 6 provides that any document, apart from those excepted in clause 1, which can be in writing, will be just as valid if it is in electronic form.

Clause 7 provides that a document that is required to be delivered to a person will be validly delivered if it is sent electronically. The format of the electronic record and the manner of delivery must be acceptable to both parties.

Clause 8 sets out the circumstances where a document that is required to be presented or retained in its original form, or where evidence of the original form of a document is required, those requirements can be satisfied by an electronic version of the document.

Clause 9 sets out the conditions to be complied with if a requirement to retain a document is to be satisfied by the retention of an electronic version.

Clause 10 provides that a requirement to make documents available for inspection shall be satisfied if a perceivable electronic version is produced.

Clause 11 ensures that courts, tribunals, etc. shall not be able to deny admissibility of documents solely on the grounds that they are presented in evidence in electronic form.

Clause 12 makes provision for where multiples copies are required by law, and allows for the use of electronic seals.

Clause 13 provides that the law shall apply to the State. It also provides that, in respect of government business, electronic communications may only be validly used by the public after notice to that effect has been published.

Clauses 14 and 15 set out the framework for E-Government services and self explanatory.

Clause 16 enables contracts to be concluded in electronic form.

Clause 17 deals with the attribution of electronic messages.

Clause 18 deals with the situation where there is a change or error in the transmission of an electronic record.

Clause 19 makes provision to govern the validity of acknowledgements of electronic messages and the circumstances where an electronic message may be presumed to have been received.

Clause 20 sets out the presumptions to be made about the time and place of sending and receipt of electronic messages.

Clause 21 ensures that preference is not given to any particular method of digitally signing an electronic message.

Clause 22 provides that where a document has to be signed, if the document is in electronic form it may be digitally signed. It then provides a number of conditions that have to be complied with if the electronic signature is to be reliable for the purposes of the Act.

Clause 23 enables regulations to be made prescribing methods which satisfy the requirements of clause 22.

Clause 24 prescribes the legal consequences of a person who fails to verify, in accordance with the procedures set out, an electronic signature.

Clause 25 makes provision for the conditions that have to be complied with before a foreign electronic signature, or the certificate attached thereto, shall be recognised.

Clause 26 creates an obligation for the keeping of a register of approved providers.

Clause 27 provides that the Minister may by regulations grant approvals to persons who are providing information security services in Antigua and Barbuda.

Clause 28 defines the provision of information security services.

Clause 29 sets out several provisions relating to the conduct of the information security service provider. An information security service provider must act in accordance with the representations it makes with respect to its policies and practices; exercise reasonable care to ensure the accuracy and completeness of all material representations made by it, provide reasonably accessible means which enable a person who relies on the certificate to ascertain, where relevant, from the certificate or otherwise, provide a means for a signature device holder to give notice that a signature device has been compromised and ensure the availability of a timely revocation service; and utilise trustworthy systems, procedures and human resources in

performing its services. An information security service provider shall be liable for its failure to satisfy these requirements.

Clause 30 provides that the Minister may make regulations regarding the criteria for determining trustworthiness, of the procedures and human resources of information security service provider in performing their services

Clause 31 specifies that the Minister may make regulations prescribing the matters that shall be specified in a certificate.

Clause 32 sets out the duties and responsibilities of a signature device holder in terms of conduct.

Clause 33 makes it an offence for anyone to publish a Digital Signature Certificate with the knowledge that the Certifying Authority listed in the certificate has not issued it with a license; the subscriber listed in the certificate has not accepted it; or the license or issue of Digital Signatures or the certificate has been revoked or suspended.

Clause 34 makes it an offence for anyone to knowingly create, publish or otherwise make available a Digital Signature Certificate for any fraudulent or unlawful purposes.

Clauses 35 to 40 set out matters that limit the liability of intermediaries and service providers as defined in the Bill.

Clause 41 enables the prescription of a Code of Practice to provide standards and other requirements that have to be complied by intermediaries and service providers.

Clause 42 makes basic provisions for consumer protection for online transactions. The provisions are adapted from the OECD Guidelines for Consumer Protection in the context of Electronic Commerce.

Clause 43 defines the situation, which arises when an offence is committed by a body corporate.

Clause 44 requires the appointment of an e-Business Advisory Board.

Clause 45 is a general power to make regulations.