

ANTIGUA AND BARBUDA



THE ELECTRONIC TRANSACTIONS ACT, 2013

No. 24 of 2013

*[Published in the Official Gazette Vol. XXXIV No. 37
dated 5th June, 2014]*

Printed at the Government Printing Office, Antigua and Barbuda,
by Ralph George, Government Printer
□ By Authority, 2014.

600 □ 06. 14

[Price \$10.65]

THE ELECTRONIC TRANSACTIONS ACT, 2013

ARRANGEMENT

PART I

PRELIMINARY

Sections

1. Short title.
2. Interpretation
3. Purposes and construction
4. Inapplicability of Act
5. Autonomy of parties

PART II

REQUIREMENTS FOR LEGAL RECOGNITION

6. Legal recognition of electronic communications
7. Legal recognition of electronic records
8. Requirement to provide access to information in paper form
9. Furnishing of information using prescribed forms
10. Delivery of information
11. Information in original form
12. Retention of documents, records or information in electronic form
13. Other requirements
14. Comparison of documents with original
15. Admissibility of electronic records

PART III

ELECTRONIC CONTRACTS

16. Formation and validity of contracts
17. Effectiveness between parties
18. Time and place of dispatch and receipt of electronic communications
19. Invitation to make offer
20. Use of automated message systems for contract formation
21. Error in electronic communications

PART IV

ELECTRONIC SIGNATURES

22. Requirements for signature
23. Equal treatment of signatures
24. Conduct of the signatory
25. Recognition of foreign certificates and electronic signatures

PART V

SECURE ELECTRONIC RECORDS AND SIGNATURES

26. Secure electronic record
27. Secure electronic signature
28. Presumptions relating to secure electronic records and signatures

PART VI

INFORMATION SECURITY PROCEDURE PROVIDERS

29. Specified security procedure providers
30. Regulation of specified security procedures and specified security procedure providers

PART VII

ELECTRONIC GOVERNANCE

31. Use of electronic records and electronic signatures in Government and its agencies
32. Records available for inspection

PART VIII

INTERMEDIARIES AND E-COMMERCE SERVICE PROVIDERS

33. Use of electronic records and electronic signatures in Government and its agencies
34. Procedure for dealing with unlawful, defamatory etc. information
35. Codes of conduct and standards for intermediaries and electronic-commerce service providers

PART IX

CONSUMER PROTECTION

36. Minimum information in e-commerce

37. Unwanted communications

PART X

CONTRAVENTION AND ENFORCEMENT

38. False or misleading information

39. Directors and officers

40. Penalties

PART XI

MISCELLANEOUS

41. Duties of directors

42. Regulations

43. Conflict of enactments

44. Repeal

[L.S.]



I Assent,

Louise Lake-Tack,
Governor-General.

27th May, 2014.

ANTIGUA AND BARBUDA
THE ELECTRONIC TRANSACTIONS ACT 2013
No. 24 of 2013

AN ACT to give legal effect to electronic documents, records and signatures and for incidental and connected purposes.

ENACTED by the Parliament of Antigua and Barbuda as follows:

1. Short title

This Act may be cited as the Electronic Transactions Act, 2013.

2. Interpretation

In this Act—

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

“authentication data” includes user name, password and license key;

“automated message system” means a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in

part, without review or intervention by a natural person each time an action is initiated or a response is generated by the program or electronic or other means;

certificate means a data message or other record confirming the link between a signatory and the signature creation data;

communication includes any statement, declaration, demand, notice, request, offer or the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract;

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;

electronic includes electrical, digital, magnetic, wireless, optical, electro-magnetic, biometric, photonic and similar capabilities;

e-commerce service provider means a person who uses electronic means in providing goods or services or both;

electronic communication means information which is communicated, processed, recorded, displayed, created, stored, generated, received or transmitted by electronic means;

electronic form, with reference to information, means any information generated, sent, received or stored in media, magnetic form, optical form, computer memory, microfilm, computer generated microfiche or similar device;

electronic record means a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another;

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

information includes data, text, documents, images, sounds, codes, computer programmes, software and databases;

information system means a system for generating, sending, receiving, storing or otherwise processing electronic records;

intermediary, with respect to an electronic communication, means a person including a host who on behalf of another person, sends, receives, transmits or stores either temporarily or permanently that electronic communication or provides related services with respect to that electronic communication, and includes telecommunication service providers, network service

providers, Internet service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafés;

Minister means the Minister to whom responsibility for information communication technology is assigned;

originator, in relation to an electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but does not include a party acting as an intermediary with respect to that electronic communication;

public authority means any Ministry, department, agency, board, commission, local democratic organ or other body of the Government and includes an entity or body established by law or by arrangement of the Government or a Minister for a non-commercial public service purpose;

record means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic, paper-based or other medium and is retrievable in visible form;

secure electronic record means an electronic record that is treated as a secure electronic record by virtue of section 27(1) or any other provision of this Act;

“secure electronic signature” means an electronic signature that is treated as a secure electronic signature by virtue of section 28 or any other provision of this Act;

security procedure means a procedure established by law or agreement or knowingly adopted by each party, that is employed for the purpose of verifying that an electronic signature, communication or performance is that of a particular person or for detecting changes or errors in content of an electronic communication;

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

signature, and its grammatical variations means a method (electronic or otherwise) used to identify a person and to indicate the intention of that person in respect of the information contained in a record;

signature creation data means unique data, including codes or private cryptographic keys or a uniquely configured physical device which is used by the signatory in creating an electronic signature;

“specified security procedure” means a security procedure which is specified by Order by the Minister;

“specified security procedure provider” means a person involved in the provision of a specified security procedure;

“transaction” means an action or set of actions relating to the conduct of business, consumer or commercial affairs between two or more persons including the sale, lease, exchange, licensing or other disposition of personal property, including goods and intangible interests in real property, services or any combination of any of these acts.

- (2) In this Act, “place of business” in relation to a party, means
- (a) any place where the party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location; or
 - (b) if the party is a natural person and he does not have a place of business, the person’s habitual residence.
- (3) For the purposes of subsection (2)
- (a) if a party has indicated his place of business, the location indicated by him is presumed to be his place of business unless another party proves that the party making the indication does not have a place of business at that location;
 - (b) if a party has not indicated a place of business and has more than one place of business, then the place of business is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract;
 - (c) a location is not a place of business merely because that location is where
 - (i) equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or
 - (ii) the information system may be accessed by other parties; and
 - (d) 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.

(4) Where an electronic communication does not relate to any contract, references to a contract in subsection (3) shall refer to the relevant transaction.

3. Purposes and construction

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

- (a) to facilitate electronic communications by means of reliable electronic records;
- (b) to 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) to facilitate electronic filing of documents with public authorities, and to promote efficient delivery by public agencies of services by means of reliable electronic records;
- (d) to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;
- (e) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records, and
- (f) to 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.

4. Inapplicability of Act

(1) This Act shall not apply to any written law requiring writing, signatures or original documents for

- (a) the making, execution or revocation of a will or testamentary instrument;
- (b) the conveyance of real or personal property or the transfer of any interest in real or personal property;
- (c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney;

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

(e) any other relevant matters that may be determined by the Minister by Order.

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

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

5. Autonomy of parties

Nothing in this Act shall

(a) require any person to use or accept electronic communications, electronic signatures or electronic contracts; or

(b) prohibit any person engaging in a transaction through the use of electronic means from

(i) varying by agreement any provision specified in Parts II, III and IV; or

(ii) establishing reasonable requirements about the manner in which electronic communications, electronic signatures or electronic forms of documents may be accepted.

PART II

REQUIREMENTS FOR LEGAL RECOGNITION

6. Legal recognition of electronic communications

An electronic communication shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is

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

(b) not contained in the electronic communication purporting to give rise to such legal effect, but is referred to in that electronic communication.

7. Legal recognition of electronic records

(1) Where any information or other matter is required by law to be given or rendered in writing or recorded in writing or in printed form or is described as being written, then, notwithstanding anything

contained in that law, such requirement or description shall be deemed to have been satisfied if such information or matter is—

- (a) rendered or recorded or made available in electronic form; and
- (b) accessible to, and is capable of retention by, the intended recipient so as to be usable or retrievable for a subsequent reference.

(2) Subsection (1) shall apply whether the requirement for the information to be in writing or recorded in writing is in the form of an obligation or the law provides consequences if it is not in writing.

(3) Where subsection (1) applies, a legal requirement to provide multiple copies of any information or other matter to the same person at the same time is met by providing a single electronic form of the information or other matter.

(4) Where any information is retained in electronic form in accordance with subsection (1) and is retrievable at any time during the specified period of retention, the paper or other non-electronic form of that information need not be retained.

8. Requirement to provide access to information in paper form

A legal requirement to provide access to information that is in paper or other non-electronic form is satisfied by providing access to the information in electronic form where the—

- (a) form and means of access to the information reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, access to the information is required to be provided; and
- (b) person to whom access is required to be provided consents to the access of the information in electronic form.

9. Furnishing of information using prescribed forms

Notwithstanding anything contained in any law, a legal requirement that a person provides information using a prescribed paper or other non-electronic form to another person is satisfied by providing the information in an electronic form that—

- (a) contains the same or substantially the same information as the prescribed paper or other non-electronic form;
- (b) is accessible to the other person so as to be usable or retrievable for subsequent reference; and

(c) is capable of being retained by the other person.

10. Delivery of information

(1) Where information is required by law to be delivered, dispatched, sent to, or to be served on, a person, that requirement is met by doing so in the form of an electronic record provided that the originator of the electronic record states that the receipt of the electronic record is to be acknowledged and the addressee has acknowledged its receipt.

(2) Subsection (1) applies whether the requirement for delivery, dispatch, sending or serving is in the form of an obligation or the law provides consequences for the information not being delivered, dispatched, sent or served.

11. Information in original form

(1) Where information is required by law to be presented or retained in its original form, that requirement is met by an electronic communication if

- (a) there exists a reliable assurance as to the integrity of the information from the time it was first generated in its final form as an electronic communication or otherwise; and
- (b) where it is required that information be presented, that information is capable of being accurately represented to the person to whom it is to be presented.

(2) Subsection (1) shall apply whether the requirement for the information to be presented or retained in its original form is in the form of an obligation or the law provides consequences if it is not presented or retained in its original form.

(3) For the purposes of subsection (1)(a), the

- (a) criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the additions of any endorsement and any change which arises in the normal course of communication, storage and display; and
- (b) standard of reliability required is to be assessed in the light of the purpose for which the information was generated and all the relevant circumstances.

12. Retention of documents, records or information in electronic form

(1) Where certain documents, records or information are required by law to be retained in paper or other non-electronic form, that requirement is met by retaining it in electronic form if the following conditions are satisfied :

- (a) the information contained in electronic form is accessible so as to be usable for subsequent reference;
- (b) the electronic communication 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 information generated, sent or received; and
- (c) any information that enables the identification of the origin and destination of an electronic communication and the date and time when it was sent or received is retained.

(2) An obligation to retain documents, records or information in accordance with subsection (1) shall not extend to any 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 any other person, if the conditions set out in subsection (1) are met.

(4) Nothing in this section shall preclude any public authority from specifying additional requirements for the retention of electronic communications that are subject to the jurisdiction of such public authority.

13. Other requirements

(1) 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.

(2) 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.

(3) 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, verified or made under oath, 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.

14. Comparison of documents with original

A legal requirement to compare a document with an original may be satisfied by comparing that document with an electronic form of the original document if the electronic form reliably assures the maintenance of the integrity of the document pursuant to the provisions of this Act.

15. Admissibility of electronic records

Subject to the Electronic Evidence Act, 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.

PART III

ELECTRONIC CONTRACTS

16. Formation and validity of contracts

(1) For the avoidance of doubt, it is declared that in the context of the formation of contracts, an offer and the acceptance of an offer may be given by means of electronic communications.

(2) Where an electronic communication is used in the formation of a contract, that contract shall not be denied validity or enforceability solely on the ground that an electronic communication was used for that purpose.

17. Effectiveness between parties

As between the originator and the addressee of an electronic communication, a declaration of intent or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic communication.

18. Time and place of dispatch and receipt of electronic communications

(1) The time of dispatch of an electronic communication is

- (a) the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator; or
- (b) if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

(2) The time of receipt of an electronic communication is the time when the electronic communication becomes capable of being retrieved by the addressee at an electronic address designated by the addressee

(3) The time of receipt of an electronic communication at an electronic address that has not been designated by the addressee is the time when the electronic communication becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address.

(4) For the purposes of subsection (3), an electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the electronic address of the addressee.

(5) An electronic communication is deemed to be dispatched at the place where the originator has his place of business and is deemed to be received at the place where the addressee has his place of business.

(6) Subsections (2), (3) and (4) shall apply notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under subsection (5).

19. Invitation to make offer

A proposal to conclude a contract, made through one or more electronic communications, which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including a proposal that makes use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

20. Use of automated message systems for contract formation

A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability solely on the ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

21. Error in electronic communications

(1) Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made.

(2) Subsection (1) shall not apply unless the person, or the party on whose behalf that person is acting

(a) notifies the other party of the error as soon as possible after learning of the error and indicates that he made an error in the electronic communication; and

(b) did not use or receive any material benefit or value from the goods or services, if any, from the other party.

(3) Nothing in this section shall affect the application of any rule of law that may govern the consequences of any error other than as provided for in subsections (1) and (2).

PART IV

ELECTRONIC SIGNATURES

22. Requirements for signature

Where a rule of law requires a signature, or provides for certain consequences if a document or a record is not signed, that requirement is satisfied in relation to an electronic record if:

(a) a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record; and

(b) the method used is either:

(i) as reliable as appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

(ii) proven in fact to have fulfilled the functions described in paragraph (a), by itself or together with further evidence.

23. Equal treatment of signatures

Unless otherwise provided by law, the parties to an electronic transaction may agree to the use of a particular method or form of electronic signature or security procedure.

24. Conduct of the signatory

Where signature creation data or authentication data can be used to create a signature or authenticate any electronic record that has legal effect, each signatory shall

- (a) exercise reasonable care to avoid unauthorised use of its signature creation data or authentication data;
- (b) without undue delay, notify any person who may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature where
 - (i) the signatory knows that the signature creation data or authentication data has been compromised; or
 - (ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data or authentication data may have been compromised; and
 - (iii) a certificate is used to support the electronic signature or authentication data, exercise reasonable care to ensure the accuracy and completeness of all material representation made by the signatory, which are relevant to the certificate throughout its lifecycle, or which are to be included in the certificate.

25. Recognition of foreign certificates and electronic signatures

(1) In determining whether, or 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 an issuer had its place of business.

(2) A party to a commercial or other type of transaction may specify that a particular information security procedure provider, class of information security procedure providers or class of certificates shall be used in connection with any message or signature submitted to them.

(3) Where, notwithstanding subsections (1) and (2), the parties to a transaction agree to the use of a particular type of electronic signature and certificate, that agreement shall be recognised as sufficient for the purpose of cross-border recognition in respect of that transaction.

PART V

SECURE ELECTRONIC RECORDS AND SIGNATURES

26. Secure electronic record

(1) If a specified security procedure, or a commercially reasonable security procedure agreed to by the parties involved, has been properly applied to an electronic record to verify that the electronic record has not been altered since a specific point in time, such record shall be treated as a secure electronic record from such specific point in time to the time of verification.

(2) For the purposes of this section and section 27, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including the

- (a) nature of the transaction;
- (b) level of technological modernity of the parties;
- (c) volume of similar transactions engaged in by either or all parties;
- (d) availability of alternatives offered to but rejected by any party;
- (e) cost of alternative procedures; and
- (f) procedures in general use for similar types of transactions.

27. Secure electronic signature

(1) If, through the application of a specified security procedure, or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made

- (a) unique to the person using it,
- (b) capable of identifying such person;
- (f) created in a manner or using a means under the sole control of the person using it; and
- (d) created in a manner or using a means under the sole control of the person using it, and such signature shall be treated as a secure electronic signature.

(2) Whether a security procedure is commercially reasonable shall be determined in accordance with section 26 (2).

28. Presumptions relating to secure electronic records and signatures

(1) In any proceedings involving a secure electronic record, it shall be presumed, unless evidence to the contrary is adduced, that the secure electronic record has not been altered since the specific point in time to which the secure status relates.

(2) In any proceedings involving a secure electronic signature, it shall be presumed, unless evidence to the contrary is adduced, that the secure electronic signature

- (a) is the signature of the person to whom it correlates; and
- (b) was affixed by that person with the intention of signing or approving the electronic record.

(3) In the absence of a secure electronic record or a secure electronic signature, nothing in this Part shall create any presumption relating to the authenticity and integrity of the electronic record or electronic signature.

PART VI

INFORMATION SECURITY PROCEDURES PROVIDERS

29. Specified security procedure providers

The Minister may by Order list the classes of specified security procedure providers to which this section applies.

30. Regulation of specified security procedures and specified security procedure providers

(1) The Minister may make regulations for the carrying out of this Part and, without prejudice to such general power, may make regulations for the following purposes □

- (a) the regulation, registration, licensing or accreditation of specified security procedure providers and their authorised representatives;
- (b) safeguarding or maintaining the effectiveness and efficiency of the common security infrastructure relating to the use of secure electronic signatures and the authentication of electronic records, including the imposition of requirements to ensure interoperability between specified security procedure providers or in relation to any security procedure;
- (c) ensuring that the common security infrastructure relating to the use of secure electronic signatures and the authentication of electronic records complies with Antigua and Barbuda's international obligations; and
- (d) prescribing the forms and fees applicable for the purposes of this Part.

(2) Without prejudice to the generality of subsection (1), the Minister may, in making regulations for the regulation, registration, licensing or accreditation of specified security procedure providers and their authorised representatives □

- (a) prescribe the accounts to be kept by specified security procedure providers;
- (b) provide for the appointment and remuneration of an auditor, and for the costs of an audit carried out under the regulations;
- (c) provide for the establishment and regulation of any electronic system by a specified security procedure provider, whether by itself or in conjunction with other specified

security procedure providers, and for the imposition and variation of requirements or conditions relating thereto as the Controller may think fit;

- (d) make provisions to ensure the quality of repositories and the services they provide, including provisions for the standards, registration, licensing or accreditation of repositories;
- (e) provide for the use of any accreditation mark in relation to the activities of specified security procedure providers and for controls over the use thereof;
- (f) prescribe the duties and liabilities of specified security procedure providers registered, licensed or accredited under this Act in respect of their customers; and
- (g) provide for the conduct of any inquiry into the conduct of specified security procedure providers and their authorised representatives and the recovery of the costs and expenses involved in such an inquiry.

(3) Regulations made under this section may provide that a contravention of a specified provision shall be a summary offence and may provide penalties consisting of a fine not exceeding two hundred thousand dollars or imprisonment for a term not exceeding two years, or to both.

PART VII

ELECTRONIC GOVERNANCE

31. Use of electronic records and electronic signatures in Government and its agencies

(1) Any public authority that, pursuant to any written law

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

requires that documents be created or retained;

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

issues any permit, licence or approval; or

requires payment of any fee, charge or other amount by any method and manner of payment, may, notwithstanding anything to the contrary in any written law, carry out that function by means of electronic records or in electronic form.

(2) In any case where a public authority decides to perform any of the functions in subsection (1) by means of electronic records or in electronic form, the public authority may specify

- (a) the manner and format in which such electronic records shall be filed, created, retained, issued or provided;
- (b) where such electronic records have to be signed, the type of electronic signature required, including, if applicable, a requirement that the sender use a particular type of secure electronic signature;
- (c) the manner and format in which such signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any specified security procedure provider used by the person filing the document;
- (d) such control processes and procedures as may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; or
- (e) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.

(3) 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 authority;
- (b) create or retain any document for a public authority;
- (c) use a prescribed form for an application or notification to, or other transaction with, a public authority;
- (d) provide to or retain for a public authority any document, record or information in its original form; or
- (e) hold a licence, permit or other approval from a public authority;
- (f) such a requirement is satisfied by an electronic record specified by the public authority for that purpose and
 - (i) in the case of a requirement referred to in paragraph (a), (c) or (d), transmitted or retained in the manner specified by the public authority;
 - (ii) in the case of a requirement referred to in paragraph (b), created or retained in the manner specified by the public authority; or

(iii) in the case of a requirement referred to in paragraph (e), issued by the public authority.

(4) Subject to sections 13 and 14, nothing in this Act shall by itself compel any public authority to accept or issue any document or information in the form of electronic records or to accept any payment in electronic form.

32. Records available for inspection

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.

PART VIII

INTERMEDIARIES AND E-COMMERCE SERVICE PROVIDERS

33. Liability of intermediaries

(1) An intermediary or e-commerce service provider may not be subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of which the intermediary provides services, if the intermediary was not the originator of the record and

- (a) he has no actual knowledge that the information gives rise to civil or criminal liability;
- (b) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known; or
- (c) follows the procedure set out in section 35 if the intermediary or e-commerce service provider
 - (i) acquires knowledge that the information gives rise to criminal liability; or
 - (ii) becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.

(2) An intermediary or e-commerce 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.

(3) Nothing in this section shall relieve an intermediary or e-commerce service provider from any

- (a) obligation to comply with an order or direction of a court or other competent authority; or
- (b) contractual obligation.

34. Procedure for dealing with unlawful, defamatory etc information

(1) If an intermediary or e-commerce service provider has actual knowledge that the information in an electronic record gives rise to civil or criminal liability, as soon as practicable the intermediary or e-commerce service provider shall □

- (a) remove the information from any information system within the intermediary's or e-commerce service provider's control and cease to provide or offer to provide services in respect of that information; and
- (b) notify the Minister or appropriate law enforcement authority of the relevant facts and of the identity of the person for whom the intermediary or e-commerce service provider was supplying services in respect of the information, if the identity of that person is known to the intermediary or e-commerce service provider.

(2) If an intermediary or e-commerce service provider is aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information in an electronic record ought reasonably to have been known, as soon as practicable the intermediary shall □

- (a) follow the relevant procedure set out in a code of conduct approved or standard appointed under this Act if such code or standard applies to the intermediary; or
- (b) notify the Minister.

(3) Where the Minister is notified in respect of any information under subsection (2), the Minister may direct the intermediary to □

- (a) remove the electronic record from any information processing system within the control of the intermediary;
- (b) cease to provide services to the person to whom the intermediary was supplying services in respect of that electronic record; or
- (c) cease to provide services in respect of that electronic record.

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

(5) Any person who lodges a notification of unlawful activity with an intermediary or e-commerce service provider, knowing that it materially misrepresents the facts, commits an offence and may be charged in a criminal or civil capacity for damages for wrongful removal of the information or electronic record under subsections (1) to (3).

(6) If a code of conduct is approved or a standard is specified by the Minister under this Act to apply to intermediaries or electronic-commerce service providers, those intermediaries or electronic-commerce service providers shall comply with such code of conduct or standards.

35. Codes of conduct and standards for intermediaries and electronic-commerce service providers

(1) If a code of conduct is approved or a standard is specified by the Minister under this section to apply to intermediaries or electronic-commerce service providers, those intermediaries or electronic-commerce service providers shall comply with such code of conduct or standards.

(2) An intermediary or electronic-commerce service provider who fails to comply with an approved code of conduct or specified standards, shall in the first instance be given a written warning by the Minister and the Minister may, by Order in writing, direct that intermediary or electronic-commerce service provider to cease and desist or otherwise to correct his practices and, if that person fails to do so within such period as may be specified in the direction, the intermediary or electronic-commerce service provider, commits an offence and shall be liable on summary conviction to a fine not exceeding fifty thousand dollars and if the offence is a continuing one to a further fine of one thousand dollars for each day the offence continues.

(3) If the Minister is satisfied that a body or organisation represents intermediaries or electronic-commerce service providers, the Minister may, by Notice given to the body or organisation, direct the body or organisation to

- (a) develop a code of conduct that applies to intermediaries or electronic-commerce service providers who deal with one or more specified matters relating to the provision of services by those intermediaries or electronic-commerce service providers; and
- (b) provide a copy of that code of conduct to the Minister within such time as may be specified in the direction.

(4) If the Minister is satisfied with the code of conduct provided under subsection (3), the Minister shall approve the code of conduct by Notice published in the Gazette and thereupon the code of conduct shall apply to intermediaries or electronic-commerce service providers, as may be specified in the notice.

(5) If the Minister is satisfied that

- (a) no body or organisation represents intermediaries or electronic-commerce service providers; or
 - (c) a body or organisation to which notice is given under subsection (3) has not complied with the direction of the Minister under subsection (3), the Minister may, by notice published in the *Gazette*, specify a standard that applies to the concerned intermediaries or electronic-commerce service providers or both.
- (6) If the Minister has approved a code of conduct or specified a standard that applies to intermediaries or electronic-commerce service providers or both and...
- (a) the Minister receives notification from a body or organisation representing intermediaries or electronic-commerce service providers of proposals to amend the code of conduct or standard; or
 - (b) the Minister no longer considers that the code of conduct or standard so approved or specified is appropriate, the Minister may, by notice published in the *Gazette*, revoke or amend the existing code of conduct or standard.
- (7) References in this section to intermediaries or electronic-commerce service providers include references to a particular class of intermediaries or electronic-commerce service providers.

PART IX

CONSUMER PROTECTION

36. Minimum information in e-commerce

(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

- (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 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 record 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 details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information;
- (b) details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information.

37. Unwanted communications

Any person who sends unsolicited commercial communications through electronic media to consumers based in Antigua and Barbuda or knowingly uses an intermediary or a telecommunications service provider based in Antigua and Barbuda to send, or who has a place of business in Antigua and Barbuda 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.

PART X

CONTRAVENTION AND ENFORCEMENT

38. False or misleading information

A person commits an offence under this Act where he—

- (a) files information required under this Act that contains false or misleading information; or
- (b) provides a consumer or a user of an electronic signature with false or misleading information.

39. Directors and officers

Where a corporation commits an offence under this Act, any officer, director or agent or the corporation who directed, authorised, assented to, acquiesced in or participated in the commission of the offence is a party to and commits an offence and is liable to the punishment provided for the offence, whether or not the corporation has been prosecuted and convicted.

40. Penalties

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

- (a) upon summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding three years; or
- (b) upon conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding six years.

(2) Where a corporation contravenes any of the provisions of this Act the Court may, in addition to any penalty it may impose for a criminal offence, impose a fine up to ten per cent of the last audited year of the enterprise.

(3) 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;
- (c) the estimate of the economic benefit of the contravention to the enterprise;
- (d) the time for which the contravention is in effect if continuing;
- (e) the number and seriousness of any other contraventions, if any, committed by the enterprise; and
- (f) any other matter the Court may consider appropriate in the circumstances.

PART XI

MISCELLANEOUS

41. Duties of directors

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

- (a) this Act and any regulations made thereunder; and
- (b) any Orders imposed by the Minister.

42. Regulations

(1) The Minister may make Regulations for the purpose of giving effect to this Act and to any matter that is required to be prescribed under this Act.

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

43. Conflict of enactments

Subject to section 5, where there is any conflict between the provisions of this Act and any other relevant enactment, the provisions of this Act shall prevail to the extent of the inconsistency.

44. Repeal

The Electronic Transactions Act No.8 of 2006 is hereby repealed.

Passed the House of Representatives on the
28th day of November, 2013.

Passed the Senate on the 11th day of
December, 2013.

D. Gisele Isaac-Arrindell,
Speaker.

Hazlyn M. Francis,
President.

Ramona Small,
Clerk to the House of Representatives.

Ramona Small,
Clerk to the Senate.

