



ST. CHRISTOPHER AND NEVIS

CHAPTER 18.44

ELECTRONIC TRANSACTIONS ACT

Revised Edition

showing the law as at 31 December 2017

This is a revised edition of the law, prepared by the Law Commission under the authority of the Law Commission Act, Cap. 1.03.

This edition contains a consolidation of the following laws—

ELECTRONIC TRANSACTIONS ACT

Act 9 of 2011 ... in force 14th April 2011

Page
3

Published in
2019
Consolidated, Revised and Prepared under the Authority of the Law Commission Act,
on behalf of the Government of Saint Christopher and Nevis
by
The Regional Law Revision Centre Inc.,
P.O. Box 1626, 5 Mar Building,
The Valley, AI-2640, Anguilla,
West Indies.

Available for purchase from—

Attorney General's Chambers,
Government Headquarters, P.O. Box 164,
Church Street, Basseterre, St. Kitts,
West Indies

Tel: (869) 465-2521

Ext. 1013

Tel: (869) 465-2127

Fax: (869) 465-5040

Email: attorneygeneral@gov.kn

© Government of Saint Christopher and Nevis
All rights reserved. No part of this publication may be reproduced in any form or by any means
without the written permission of the Government of Saint Christopher and Nevis except as
permitted by the Copyright Act or under the terms of a licence from
the Government of Saint Christopher and Nevis.

CHAPTER 18.44
ELECTRONIC TRANSACTIONS ACT

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

1. Short title
2. Interpretation
3. Exclusions
4. Variation of Terms

PART II

LEGAL REQUIREMENTS RESPECTING ELECTRONIC RECORDS

5. Legal Recognition of Electronic Records
6. Requirement for Information to be in Writing
7. Delivery
8. Original Records
9. Retention of Records
10. Availability of Records for Inspection
11. Admissibility of Electronic Records
12. Other Requirements

PART III

E-GOVERNMENT SERVICES

13. Government Services
14. Acceptance of Electronic Filing and Issuing of Documents
15. Requirements May be Specified

PART IV

ELECTRONIC RECORDS

16. Formation and validity of contracts
17. Attribution of Electronic Records
18. Acknowledgement of Receipt of Electronic Records
19. Time and Place of Electronic Communication and Electronic Records

PART V

ELECTRONIC SIGNATURES

20. Equal Treatment of Signatures
21. Compliance with a Requirement for a Signature
22. Reliance on an Electronic Signature
23. Unlawful Publication of Digital Signature Certificate
24. Publication for a Fraudulent Purpose

PART VI

CERTIFICATION SERVICE PROVIDERS

25. Register of Approved Providers
26. Arrangements for the Grant of Approvals
27. Provision of Certification Services
28. Conduct of the Certification Service Provider
29. Recognition of External Certification and Electronic Signatures
30. Conduct of the Signatory
31. Effectiveness of Electronic Signature or Certificate

PART VII

LIABILITY OF INTERMEDIARIES AND SERVICE PROVIDERS

32. Third Party Liability
33. Information Location Tools
34. Notification of Unlawful Activity
35. Monitoring and Compliance

PART VIII

MISCELLANEOUS PROVISIONS

36. Offences by Bodies Corporate
37. Appointment of E-Commerce Advisory Board
38. Regulations
39. Act Binds Crown

CHAPTER 18.44**ELECTRONIC TRANSACTIONS ACT**

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.

PART I**PRELIMINARY****Short title.**

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

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-Commerce Advisory Board appointed under section 37;

“certificate” means an electronic attestation issued by an approved certification service provider that—

- (a) links signature-verification data to a person and confirms the identity of that person; or
- (b) links time-verification data to an electronic record or to an electronic communication and confirms the associated date and time of that electronic record or electronic communication;

“certification procedure” includes a procedure which is provided to an originator, intermediary, or recipient of an electronic record which is designed to—

- (a) ensure that the electronic record can be accessed, or put into an intelligible form, only by certain persons; or
- (b) ensure that the—
 - (i) authenticity;
 - (ii) time of processing; or
 - (iii) integrity,

of such electronic record is capable of being ascertained;

and “certification service” shall be construed accordingly;

“certification service provider” means a person who issues electronic certificates or provides other services related to electronic signatures, which have been accredited by the accreditation authority;

“data” means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable to cause an information system to perform a function;

“deliver” includes give, serve and file;

“electronic” means any medium that is created, recorded, transmitted or stored in a digital or other intangible form by electronic, magnetic, optical or by another means that has capabilities for creation, recording, transmission or storage similar to those means;

“electronic agent” means a program, or other electronic or automated means, configured and enabled by a person, that is used to initiate or respond to an electronic record or event in whole or in part, without review by an individual;

“electronic commerce” means the ability to conduct commerce which deals with the exchange of anything of economic value, goods, services, information or money from producer to final consumer to satisfy their needs using electronic communications and digital information processing technologies;

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

“electronic signature” means data in electronic form which is attached to, incorporated in or logically associated with other electronic data and which serves as a method of authentication;

“electronic transaction” means the single communication or outcome of multiple communications involved in the sale or purchase of goods and services;

“information” includes documents, 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;

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

“Minister” means the Minister responsible for Information Technology;

“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;

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

“record” means information that is—

- (a) captured, created, collected, or received in the initiation, conduct or completion of an activity; and

- (b) in such a format as to provide evidence or proof of that activity or transaction being inscribed, stored or otherwise maintained on a tangible medium;
- (c) stored in an electronic or any other medium and is accessible in visible and audible form;

“signature” includes any symbol executed or adopted, or any methodology or procedure employed or adopted by a person with the intention of authenticating a record, including electronic or digital methods;

“transaction” includes—

- (a) a transaction of a non-commercial nature;
- (b) a single communication; or
- (c) the outcome of multiple related communications.

Exclusions.

3. (1) Nothing in this Act shall apply to—

- (a) the grant of a Power-of-Attorney;
- (b) a trust;
- (c) the making, execution or revocation of a will or other testamentary instrument;
- (d) any contract for the sale or conveyance of immoveable property or any interest in such property;
- (e) the swearing of affidavits or statutory declarations before a Commissioner of oaths or 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 been reduced into an electronic data format the integrity of which 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 (f).

Variation of Terms.

4. As between parties involved in generating, sending, receiving, storing or otherwise processing records, any provision of Part II or Part IV may be varied or excluded by agreement of the parties.

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.

Requirement for Information to be in Writing.

6. (1) Where information is required by law to be in writing, or is described in any statutory provision as being written, that requirement is satisfied by provision of an electronic record, if the information contained in the electronic record is accessible and is capable of retention for subsequent reference.

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

Delivery.

7. (1) Where information is required or permitted by law 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) the originator of the electronic record states that the receipt of the electronic record is to be acknowledged, and 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 law provides consequences for the information not being delivered or sent.

Original Records.

8. (1) Where there is a legal requirement that information be presented or retained in its original form, that requirement is satisfied by presenting or keeping an electronic record—
- (a) if 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 record or otherwise; or
 - (b) if that information is capable of being accurately represented in an electronic format.

(2) Paragraph (a) shall apply if the requirement for the presentation or retention of evidence of the original form of the information is in the form of an obligation or if the law provides consequences if conclusive evidence of the original form of the information is not provided.

(3) For the purpose of subsection (1) the 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 the law requires that certain information is to be retained that requirement is satisfied 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 information 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.

Availability of Records for Inspection.

10. Where information is required by any law to be made available for inspection, that requirement shall be satisfied by making such information available for inspection in perceivable form as an electronic record.

Admissibility of Electronic Records.

11. (1) In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility of—

- (a) an electronic record in evidence solely on the ground that it is an electronic record; or
- (b) an electronic signature in evidence shall not be denied solely on the grounds that it is an electronic signature.

(2) Information in the form of an electronic record shall be given due evidential weight and in assessing the evidential weight of an electronic record, regard shall be had to—

- (a) the reliability of the manner in which the electronic record was generated, stored or communicated;

- (b) the reliability of the manner in which the integrity of the information was maintained;
- (c) the manner in which the originator was identified; and
- (d) any other relevant factor.

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, shall 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 satisfied 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

Government Services.

13. (1) Notwithstanding section 39, nothing in this Act shall require a ministry or public body to process an electronic record, but the relevant Minister for the ministry in question may, by notice published in the *Gazette*, indicate that a ministry or public body shall process electronic records relating to such matters as may be specified in the notice.

(2) Until a notice under subsection (1) has been published, no person dealing with such ministry or public body shall be entitled to use an electronic record, to meet a requirement to process a record.

(3) The State, the Minister, or any employee of the State in performing a function in terms of this Act shall not be liable in respect of any act or omission in good faith and without gross negligence.

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,

may, notwithstanding 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 criteria that must be satisfied by any authorised certification service provider used by the person filing the electronic record;
- (e) the appropriate control processes and procedures to ensure adequate integrity, auditability, security and confidentiality of electronic records or payments; and
- (f) any other requirements for electronic records or payments.

PART IV

ELECTRONIC RECORDS

Formation and validity of contracts.

16. (1) Unless otherwise agreed by the parties, an offer, and the acceptance of an offer, in relation to a contract may be expressed—

- (a) by means of electronic records; or
- (b) by an act that is intended to result in an electronic communication such as touching or clicking an appropriate icon or other place on a computer screen, by speaking or accessing an electronic page or site subject to prior expressed conditions.

(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.

(3) An electronic contract may be formed through the interaction of a computer program or other electronic means used to initiate an act or to respond to an electronic communication, in whole or in part, without review by an individual at the time of the response or act.

(4) Where an electronic contract is formed in accordance with subsection (3) it shall be valid and binding on the condition that—

- (a) the contracting party knows or has reason to believe that by taking a particular action he or she will cause the transaction to be completed electronically;
- (b) the contract terms were capable of being reviewed by all the contracting parties prior to the formation of the contract;
- (c) in a case where a person receives moneys or other benefit from or through an electronic agent as a result of an error, the person returns or disposes of the consideration.

(5) An electronic transaction between a person and an electronic agent has no legal effect if the person makes a material error in the electronic communication or electronic record used in the transaction and where—

- (a) the electronic agent does not give the person an opportunity to prevent or correct the error;
- (b) on becoming aware of the error, the person promptly notifies the person that owns or is in charge of the electronic agent;
- (c) in a case where the person receives moneys or other benefit from or through the electronic agent as a result of the error, the person returns or disposes of the consideration.

Attribution of Electronic Records.

17. (1) An electronic record is that of an originator if it was sent by the electronic 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, that the electronic record was a duplicate.

Acknowledgement of Receipt of Electronic Records.

18. (1) Subsections (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 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, that 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 of Electronic Communication and Electronic Records.

19. (1) Unless the originator and addressee otherwise agree, an electronic record is sent as an electronic communication when it enters an information processing system outside the control of the originator or, if the originator and the addressee are in the same information system, at the point when the information or record becomes capable of being retrieved and processed by the addressee.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record is determined as follows—

- (a) where the addressee has designated an information-processing system for the purpose of receiving electronic records, receipt occurs—
 - (i) when it enters the designated information processing system; or
 - (ii) if the electronic record is sent to an information processing system of the addressee that is not the designated information processing system, at the time when the electronic record is retrieved by or comes to the attention of the addressee;
- (b) if the addressee has not designated or does not use an information processing system, receipt occurs when the electronic record enters the information processing system of the addressee or otherwise is retrieved by or comes to the attention of the addressee.

(3) Subsection (2) applies notwithstanding that the place where the information processing system is located may be different from the place where the electronic record is deemed to be received under subsection (4).

(4) Unless otherwise agreed between the originator and the addressee, an electronic record is deemed to be sent from 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.

(5) For the purposes of subsection (4) if the originator or the addressee—

- (a) has more than one place of business, the place of business is that which has the closest relationship to the transaction to which the electronic record relates or, where there is no transaction, the place of business is presumed to be the principle place of business; or
- (b) does not have a place of business, it is presumed to be where the originator or the addressee originally resides.

PART V**ELECTRONIC SIGNATURES****Equal Treatment of Signatures.**

20. (1) Except as provided in section 21, the provisions of this Act shall not be applied so as to exclude, restrict, or deprive of legal effect, any method of creating an electronic signature which—

- (a) satisfies the requirements of section 21 (1); or
- (b) otherwise meets the requirements of an applicable law.

(2) An electronic signature that is associated with a certificate issued by a certification service provider under section 27 is deemed to satisfy the requirements of section 6.

Compliance with a Requirement for a Signature.

21. (1) Where there is a legal requirement for the signature of a person, that requirement shall be satisfied in relation to an electronic record if an electronic signature is used that—

- (a) adequately identifies the signatory and his or her approval of the information to which the signature relates;
- (b) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required.

(2) A legal requirement for a signature is not satisfied by use of an electronic signature unless, the person requiring that person to present a signature consents to receiving the electronic signature.

(3) Subsection (1) applies whether the requirement for a signature is in the form of an obligation or the law provides consequences for the absence of a signature.

(4) The Minister may prescribe methods for satisfying the requirements referred to in this section.

Reliance on an Electronic Signature.

22. Where an electronic signature is supported by a certificate, due diligence should be conducted to—

- (a) verify the validity, suspension or revocation of the certificate; or
- (b) observe any limitation with respect to the certificate.

Unlawful Publication of Digital Signature Certificate.

23. (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 the person with a licence;
- (b) the subscriber listed in the certificate has not accepted it; or
- (c) the licence 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 subsection (1) commits an offence and shall upon conviction be liable to imprisonment for a term not exceeding three years, or to a fine not exceeding twenty thousand dollars or both such fine and imprisonment.

Publication for Fraudulent Purpose.

24. 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 to a fine not exceeding thirty thousand dollars or both such fine and imprisonment.

PART VI

CERTIFICATION SERVICE PROVIDERS

Register of Approved Provider.

25. (1) The Minister may establish and maintain a register of approved certification 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—

- (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 26, in accordance with arrangements prescribed by the Minister in regulations.

Arrangements for the Grant of Approvals.

26. The Minister may make regulations on the granting of approvals, subject to the payment of a prescribed fee, to persons who—

- (a) are providing certification services in Saint Christopher and Nevis or are proposing to do so; and
- (b) seek approval in respect of any such services that they are providing, or are proposing to provide, whether in Saint Christopher and Nevis or elsewhere.

Provision of Certification Services.

27. (1) References in this part to the provision of a certification service do not include references to the supply of, or of any right to use computer software or computer hardware unless the right to use the supply or services is integral to the provision of certification services which do not consist of such a supply or right to use.

(2) For the purposes of this Part certification services are provided in Saint Christopher and Nevis if they are provided from premises in Saint Christopher and Nevis and—

- (a) they are provided to a person who is in Saint Christopher and Nevis when he makes use of the services; or
- (b) they are provided to a person who makes use of the services for the purposes of a business carried on in Saint Christopher and Nevis or from premises in Saint Christopher and Nevis.

Conduct of the Certification Service Provider.

- 28.** (1) A certification service provider shall—
- (a) be authorised to provide certification services for electronic signatures;
 - (b) act in accordance with the representations it makes with respect to its policies and practices;
 - (c) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it—
 - (i) that are relevant to the certificate throughout its life cycle; or
 - (ii) which are included in the certificate;
 - (d) provide reasonably accessible means which enable a person who relies on a certificate to ascertain from that certificate—
 - (i) the identity of certification 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;
 - (e) 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 signatory;
 - (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 certification service provider;
 - (v) whether means exist for the signatory holder to give notice that a signature device has been compromised; and
 - (vi) whether a timely revocation service is offered;
 - (f) provide a means for a signatory to give notice that a signature device has been compromised and ensure the availability of a timely revocation service; and
 - (g) utilise reliable systems, procedures and human resources in performing its services.
- (2) A certification service provider shall be liable for its failure to satisfy the requirements of subsection (1).
- (3) The Minister may prescribe factors to which regard might be had in determining whether, and the extent to which, systems, procedures and human resources are reliable for the purposes of this section.

Recognition of External Certification and Electronic Signatures.

- 29.** (1) The Minister may, by notice published in the *Gazette*, recognize signatures or certification complying with the laws of another jurisdiction relating to electronic

signatures, certificates, classes of certificates issued in, or certification service providers or classes of certification service providers established in another jurisdiction and, upon such recognition and on payment of such fee as may be prescribed, those—

- (a) electronic signatures shall be deemed to be authentic;
- (b) certificates or classes of certificates shall be deemed to be accredited certificates; and
- (c) those certification service providers or classes of certification service providers shall be deemed to be authorized under section 28(1).

(2) In the determination to accord recognition under subsection (1) the Minister shall have regard to whether—

- (a) the electronic signatures are legally equivalent to signatures issued by certification service providers approved under this Act or regulations issued pursuant to this Act and whether the laws of the other jurisdiction require a level of reliability at least equivalent to that required for such signatures under this Act;
- (b) the certificates or classes of certificates are required to, and do in fact, meet obligations equivalent to those required for a certificate under this Act; or
- (c) the certification service providers or classes of certification service providers are required to, and do in fact, meet criteria equivalent to those required for an authorised certification service provider.

(3) The Minister may, by notice published in the *Gazette*, revoke any recognition accorded under subsection (1), but, before doing so, the Minister shall—

- (a) advise the person affected of his intention to do so;
- (b) indicate his reasons for the proposed revocation; and
- (c) invite that person, within fourteen days of the notice, to submit representations in writing as to why the recognition should not be revoked, and shall consider those representations.

(4) Notwithstanding subsections (2) and (3)—

- (a) parties to a commercial and other transactions may specify that a particular certification service provider, class of certification service provider or class of certificates shall be used in connection with messages or signatures submitted to them;
- (b) where 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.

Conduct of the Signatory.

30. A signatory 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 signatory to rely on or to provide services in support of the electronic signature if—

- (i) the signatory knows that the signature device has been compromised; or
- (ii) the circumstances known to the signatory 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 signatory which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

Effectiveness of Electronic Signature or Certificate.

31. (1) In determining whether, or to what extent, an electronic certificate or an electronic signature issued within Saint Christopher and Nevis is legally effective, no regard shall be had to the geographic locations—

- (a) where an electronic certificate is issued and used; or
- (b) of the place of business of the certificate service provider or signatory.

(2) Subsection (1) shall only be applicable where the national or regional authority in charge of administering the electronic signature system accredited the certification service provider.

PART VII

LIABILITY OF INTERMEDIARIES AND SERVICE PROVIDERS

Third Party Liability.

32. (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.

Information Location Tools.

33. 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.

Notification of Unlawful Activity.

34. (1) For the purposes of this Part, a notification of unlawful activity shall be in writing, addressed by the complainant to the intermediary or service provider or its designated agent and shall 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 notification is to his or her knowledge true and correct.

(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 on conviction to two years imprisonment or ten thousand dollars or to both such fine and imprisonment.

(3) An intermediary or service provider is not liable for a wrongful notification.

Monitoring and Compliance.

35. (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 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.

PART VIII

MISCELLANEOUS PROVISIONS

Offences by Bodies Corporate.

36. (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-Commerce Advisory Board.

37. (1) The Minister may appoint a Board, to be known as the E-Commerce Business Advisory Board.

(2) Where appointed, 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 terms of appointment of a Board appointed pursuant to subsection (1) may be prescribed by the Minister.

Regulations.

38. (1) The Minister may make regulations for the purpose of giving effect to provisions of this Act.

(2) Notwithstanding the generality of subsection (1), the Minister may provide in regulations for the establishment of standards or practice requirements with which service providers or intermediaries carrying on business in or from within St. Christopher and Nevis must comply.

(3) Standards established by regulations made under subsection (2) 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 Saint Christopher and Nevis to intermediaries and service providers;
- (h) procedures for dealing with complaints;
- (i) procedures for dispute resolution, including dispute.

Act Binds Crown.

39. This Act binds the Crown.
