

**SAINT VINCENT AND THE GRENADINES
ELECTRONIC TRANSACTIONS ACT 2015
ARRANGEMENT OF SECTIONS**

SECTION

PART I

PRELIMINARY

1. Short title and commencement
2. Interpretation
3. Objects
4. Act binds Crown
5. Inapplicability of Act
6. Autonomy of parties

PART II

REQUIREMENTS FOR LEGAL RECOGNITION

7. Legal recognition of electronic communications
8. Legal recognition of electronic records
9. Requirement to provide access to information in paper form
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. Requirement 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 PROCEDURES PROVIDERS

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

PART VII

ELECTRONIC GOVERNANCE

31. Records available for inspection
32. Furnishing of information in prescribed forms

PART VIII

INTERMEDIARIES AND ELECTRONIC COMMERCE SERVICE PROVIDERS

33. Liability of intermediaries

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 PROVIDER**

36. Minimum information in electronic commerce
37. Cool-off period
38. Unwanted communications

**PART X
CONTRAVENTION AND ENFORCEMENT**

39. False or misleading information
40. Penalties

**PART XI
MISCELLANEOUS**

41. Regulations
42. Repeal



SAINT VINCENT AND THE GRENADINES

ACT NO. 6 OF 2015

I ASSENT

[L.S.]

DR. FREDERICK BALLANTYNE

Governor-General

12th May, 2015

AN ACT to repeal and replace the Electronic Transactions Act, Chapter 145, to give legal effect to electronic documents, records and signatures and for related matters.

[By Proclamation]

BE IT ENACTED by the Queen's Most Excellent Majesty, by and with the advice and consent of the House of Assembly of Saint Vincent and the Grenadines and by the authority of the same, as follows:

PART I

PRELIMINARY

1. (1) This Act may be cited as the Electronic Transactions Act, 2015. Short title and commencement

(2) This Act comes into operation on a day to be appointed by the Governor General by Proclamation published in the *Gazette* and different days may be fixed for different provisions of this Act.

2. (1) In this Act – Interpretation

“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, electromagnetic, biometric, photonic and similar capabilities;
- “electronic commerce service provider” means a person who uses electronic means in providing goods or services;
- “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;

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

“electronic transaction” means the single communication or outcome of multiple communications involved in the sale or purchase of goods or services conducted over computer mediated networks or information systems, where the goods or services may be ordered through the networks or systems but the payment and ultimate delivery of the goods or services may occur without the use of the networks or systems;

“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 record, means a person, who sends, receives, stores, processes or provides other services with respect to the electronic record for another person, including the provision of content, email, caching and hosting services;

“Minister” means the Minister to whom responsibility for e-government and electronic commerce 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 a 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 recorded information created, collected, or received in the initiation, conduct or completion of an activity and that comprises content, context and structure to provide evidence or proof of that activity or transaction, being inscribed, stored or otherwise maintained on a tangible medium or that is stored in an electronic or any other medium and is accessible in visible or audible form or both;

“secure electronic record” means an electronic record that is treated as a secure electronic record by virtue of section 26(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 27 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;

“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;

“signed” or “signature” and its grammatical variations means –

(a) 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; and

(b) 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;

“specified security procedure” means a security procedure which is specified by the Minister in an order made under section 29 (b);

“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 –

(i) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or

(ii) where 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 a contract, references to a contract in subsection (3) shall refer to the relevant transaction.

Objects

3. The objects of this Act are to –

(a) facilitate electronic communications by means of reliable electronic records;

(b) facilitate electronic commerce, to eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(c) minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;

(d) help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records;

(e) promote public confidence in the integrity and reliability of electronic records and electronic commerce, and foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium; and

- (f) promote the harmonisation of legal rules on electronic transactions across national or international boundaries.

4. This Act binds the Crown.

Act binds Crown

5. (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 matters that may be determined by the Minister by order published in the *Gazette*.

(2) Notwithstanding subsection (1); the Minister may by order published in the *Gazette* make this Act applicable to any of the legal requirements set out in subsection (1).

(3) An order made under subsection (2) is subject to affirmative resolution of the House of Assembly.

6. (1) Nothing in this Act shall –

Autonomy of parties

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

(2) A transaction which has been conducted using electronic means shall not be denied legal effect, validity or enforceability solely for

the reason of the type or method of electronic communication, electronic signature or electronic authentication selected by the parties.

(3) The fact as to whether or not a party agrees to conduct a transaction electronically shall be determined by the context and surrounding circumstances including the party's conduct.

(4) A party that agrees to conduct a particular transaction electronically may refuse to conduct other transactions electronically.

PART II

REQUIREMENTS FOR LEGAL RECOGNITION

Legal recognition
of electronic
communications

7. Information and transactions shall not be denied legal effect, validity or enforcement solely on the ground that they are represented in electronic form, provided the requirements established in this Act are met.

Legal recognition
of electronic
records

8. (1) Where any law requires a person to provide information or to enter into a transaction in a prescribed non-electronic form the requirement is satisfied by the provision of the information or the entering into the transaction in an electronic form that is –

- (a) organized in the same or substantially the same way as the prescribed non-electronic form;
- (b) accessible to the other person (or to third parties, as the case may be) so as to be usable for subsequent reference; and
- (c) capable of being retained by the other person (or by third parties, as the case may be).

(2) In subsection (1), providing information includes, but is not limited to, the following –

- (a) making an application;
- (b) making, filing or lodging a claim;
- (c) giving, sending or serving a notification;
- (d) filing or lodging a return;
- (e) making a request;
- (f) making a declaration;

(g) filing, lodging or issuing a certificate; and

(h) making, varying or canceling electronic voting.

(3) Where any law referred to in subsection (1) requires more than one copy of the information or transaction to be submitted to a person, that requirement is satisfied by providing the information or transaction record to the person electronically in accordance with the provisions of this section.

9. (1) Any law that requires information or transactions to be in writing is satisfied by electronic records if the requirements set out in section 8 (1) (b) and (c) are met.

Requirement to provide access to information in paper form

(2) Subsection (1) does not apply where the interested party consents to waive the requirements.

10. (1) Where information is required by law to be delivered, dispatched, given or 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.

Delivery of information

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

11. (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 –

Information in original form

(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) –

- (a) the 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) the 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.

Retention of documents, records or information in electronic form

12. (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) (c) 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 the public authority.

Other requirements

13. (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 the 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 the law does not prescribe the method or form by which the 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 secure 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. 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.

Comparison of documents with original

15. (1) 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.

Admissibility of electronic records

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

- (a) the reliability of the manner in which the electronic communication was generated, stored or transmitted;
- (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.

(3) This section shall not affect the application of the Evidence Act.

Cap. 220

PART III
ELECTRONIC CONTRACTS

Formation and validity of contracts 16. (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.

Effectiveness between parties 17. 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.

Time and place of dispatch and receipt of electronic communications 18. (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 its place of business and is deemed to be received at the place where the addressee has its 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. 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.

Invitation to
make offer

20. 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.

Use of automated
message systems
for contract
formation

21. (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.

Error in
electronic
communications

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

- (a) notifies the other party of the error as soon as possible after having learned of the error and indicates that he made an error in the electronic communication; and
- (b) has not used or received any material benefit or value from the goods or services, if any, received 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**

- Requirement for signature
22. 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.
- Equal treatment of signatures
23. 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.
- Conduct of the signatory
24. Where signature creation data or authentication data can be used to create an electronic 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 if –
 - (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
 - (c) where 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. (1) The Minister may by order published in the *Gazette* declare certain classes of certificates or electronic signatures originating in other specified jurisdictions to be legally effective and the order shall create no presumption as to the legal effectiveness of certificates or electronic signatures originating in any jurisdiction that is not specified.

Recognition of
f o r e i g n
c e r t i f i c a t e s
a n d
e l e c t r o n i c
s i g n a t u r e s

(2) Notwithstanding subsection (1), parties to commercial and other transactions 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 messages or signatures submitted to them.

(3) Where, notwithstanding subsection (1), the parties to a transaction agree to the use of particular types of electronic signatures or certificates, 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. (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, the record shall be treated as a secure electronic record from that specific point in time to the time of verification.

Secure electronic
record

(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 –

- (a) the nature of the transaction;
- (b) the sophistication of the parties;
- (c) the volume of similar transactions engaged in by either or all parties;
- (d) the availability of alternatives offered to but rejected by any party;
- (e) the cost of alternative procedures; and

- (f) the procedures in general use for similar types of transactions.

Secure electronic signature

27. (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 the person;
- (c) created in a manner or using a means under the sole control of the person using it; and
- (d) linked to the electronic record to which it relates in such a manner that if the record was changed the electronic signature would be invalidated, the 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).

Presumptions relating to secure electronic records and signatures

28. (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 –

- (a) the secure electronic signature is the signature of the person to whom it correlates; and
- (b) the secure electronic signature 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.

INFORMATION SECURITY PROCEDURES PROVIDERS

29. The Minister may by order published in the *Gazette* –
- (a) list the classes of specified security procedure providers to which this Part applies; or
 - (b) specify security procedure.
30. (1) The Minister may make regulations for the carrying out of this Part and, without prejudice to that general power, may make regulations for all or any of the following purposes –
- (a) the regulating, registering, 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 Saint Vincent and the Grenadines 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;

Specified security
p r o c e d u r e
p r o v i d e r s a n d
p r o c e d u r e

Regulation of
s p e c i f i e d s e c u r i t y
p r o c e d u r e s a n d
s p e c i f i e d s e c u r i t y
p r o c e d u r e
p r o v i d e r s

- (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 Minister 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 the inquiry.

(3) Regulations made under this section may provide that a contravention of a specified provision shall be an offence and may provide penalties of a fine not exceeding fifty thousand dollars or imprisonment for a term not exceeding twelve months or both.

PART VII

ELECTRONIC GOVERNANCE

Records available
for inspection

31. Where documents, records or information are required by any statutory provision or 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.

Furnishing of
information in
prescribed forms

32. Notwithstanding anything contained in any law, a legal requirement that a person provides information in 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.

PART VIII

INTERMEDIARIES AND ELECTRONIC COMMERCE SERVICE PROVIDERS

33. (1) An intermediary or electronic 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 or electronic commerce service provider provides services, if the intermediary or electronic commerce service provider was not the originator of the record and he –

Liability of
intermediaries

- (a) 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 34 if the intermediary or electronic 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 electronic 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 electronic commerce 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.

Procedure for dealing with unlawful, defamatory etc. information

34. (1) If an intermediary or electronic commerce service provider has actual knowledge that the information in an electronic record or electronic communication gives rise to criminal liability or liability for a tort or that may be reasonably believed to give rise to criminal liability or liability for a tort, and has obtained from the user of its services information that cannot reasonably indicate otherwise, the intermediary or electronic commerce service provider shall as soon as practicable –

- (a) notify appropriate law enforcement authorities of the relevant information, where required by criminal laws in effect;
- (b) where authorized by written law, disclose the identity of the person for whom the intermediary or electronic commerce service provider was supplying services in respect of the information, if the identity of that person is known to the intermediary; and
- (c) where authorized by written law, remove the information or data message from any information processing system within the intermediary's or electronic commerce service provider's control and cease to provide or offer to provide services in respect of that information or take any other action authorized by law.

(2) Failure to disclose knowledge of unlawful content under subsection (1) constitutes an offence.

(3) A person who lodges a notification of unlawful activity with an intermediary or electronic commerce service provider, knowing that it materially misrepresents the facts, commits an offence and, in addition to any criminal penalty that a court may impose, is liable for damages for wrongful removal of the information or electronic record under subsections (1) to (2).

Codes of conduct and standards for intermediaries and electronic commerce service providers

35. (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 the code of conduct or standards, as the case may be.

(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 the period specified in the direction, the intermediary or electronic commerce service provider, as the case may be, commits an offence and is liable on summary conviction to a fine of 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 the time 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 the code of conduct shall apply to intermediaries or electronic commerce service providers, as the case may be, 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
- (b) 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) A standard specified by the Minister under subsection (5) 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 electronic commerce service providers.
- (e) the information to be disclosed by intermediaries and electronic commerce 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 electronic commerce service providers sending bulk, unsolicited electronic records;
- (g) the practical application of the relevant laws of Saint Vincent and the Grenadines to intermediaries and electronic commerce service providers;
- (h) procedures for dealing with complaints;
- (i) procedures for dispute resolution, including dispute resolution by electronic means;
- (j) such other matters as the Minister may require.

(7) 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 notice 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, as the case may be.

(8) 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. (1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction shall make the following data available to consumers in a clear and comprehensible manner –

Minimum
information in
electronic
commerce

- (a) its full name and legal status;
- (b) its physical address and telephone number;
- (c) its web site address and e-mail address;
- (d) the physical address where the supplier will receive legal service of documents;
- (e) a sufficient description of the main characteristics of the goods or services offered by the supplier to enable a consumer to make an informed decision on the proposed electronic transaction;
- (f) the full price of the goods or services, including transport costs, taxes and any other fees or costs;
- (g) the method of payment;
- (h) any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;
- (i) the time within which the goods will be dispatched or delivered or within which the services will be rendered;
- (j) the manner and period within which consumers can access and maintain a full record of the transaction;
- (k) the return, exchange, insurance and refund policy of the supplier;
- (l) the security procedures and privacy policy of the supplier in respect of payment, payment information and personal information;

- (m) a channel for receipt of notices from the consumer, in the same area of the electronic communication originally used by the supplier to display the offering or to promote the transaction.
- (2) The supplier shall provide a consumer with the opportunity to –
- (a) review the entire electronic transaction;
 - (b) correct any mistakes; and
 - (c) withdraw from the transaction before finally placing any order.
- (3) If the supplier fails to comply with the provisions of subsection (1) or (2) –
- (a) the supplier commits an offence; and
 - (b) the consumer may cancel the transaction within fourteen days of receiving the goods or services under the transaction.
- (4) If a transaction is cancelled as provided by subsection (3) –
- (a) the consumer shall return the goods of the supplier or, where applicable, cease using the services performed; and
 - (b) the supplier shall refund all payments made by the consumer including the cost of returning the goods within thirty days of the return of the goods.
- (5) The supplier shall utilize a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned.
- (6) The supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).
- (7) The supplier shall ensure the availability of an automated response system to acknowledge receipt of electronic communications sent by the consumer.
- (8) A consumer electronic transaction shall be deemed concluded upon receipt by the consumer of the electronic communication

om the supplier confirming receipt of consumer's acceptance of the offering.

37. (1) A consumer is entitled to cancel without reason and without penalty any transaction and any related credit agreement for the supply Cool-off period

- (a) of goods within seven business days after the date of receipt of the goods; or
- (b) of services within seven business days after the date of conclusion of the agreement.

(2) The only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) If payment for the goods or services has been effected prior to a consumer exercising a right referred to in subsection (1), the consumer is entitled to a full refund of such payment, which refund shall be made within thirty days of the date of cancellation.

(4) This section does not apply to an electronic transaction

- (a) for financial services, including investment services, insurance and reinsurance operations, and banking services;
- (b) conducted as an auction;
- (c) for services which began, with the consumer's consent, before the applicable cooling-off period specified in subsection (1);
- (d) where the price for the supply of the goods, services or facilities in question is dependent on fluctuations in the financial markets and cannot be controlled by the supplier;
- (e) where the goods in question –
 - (i) are made to the consumer's specifications;
 - (ii) are clearly personalized;
 - (iii) by reason of their nature cannot be returned; or
 - (iv) are likely to deteriorate or expire rapidly;

- (f) where audio or video recordings or consumer software are unsealed by the consumer;
- (g) for the sale of newspapers, periodicals, magazines or books;
- (h) for the provision of gaming or lottery services; or
- (i) for the provision of accommodation, transport, catering or leisure services or facilities, which the supplier undertakes to provide (when the transaction is concluded) on a specific date or within a specific period.

U n w a n t e d
communications

38. (1) A person who sends unsolicited commercial communications through electronic media to consumers based in Saint Vincent and the Grenadines or knowingly uses an intermediary or a telecommunications service provider based in Saint Vincent and the Grenadines to send, or who has a place of business in Saint Vincent and the Grenadines and sends, unsolicited electronic correspondence to consumers shall –

- (a) provide the consumer with a clearly specified and easily activated option to opt out of receiving future communications; and
- (b) give to a consumer to whom any communications is sent upon request by the consumer, the identifying particulars of the source from which that person obtained the consumer's information or other personal information.

(2) A person who fails to comply with subsection (1) commits an offence and is liable on summary conviction to a fine of twenty thousand dollars for the first conviction and of forty thousand dollars for any subsequent conviction.

PART X

CONTRAVENTION AND ENFORCEMENT

False or
misleading
information

39. A person who –

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

commits an offence.

40. (1) A person who commits an offence under this Act for which no penalty is provided is liable – Penalties

- (a) upon summary conviction to a fine of two hundred thousand dollars or to imprisonment for a term of three years or to both; or
- (b) upon conviction on indictment to a fine of two hundred and fifty thousand dollars or to imprisonment for a term of five years or to both.

(2) Where the offence under this Act is committed by an enterprise for which no penalty is provided, the enterprise shall be liable –

- (a) on summary conviction to a fine of two hundred and fifty thousand dollars; and
- (b) on conviction on indictment to a fine of five hundred thousand dollars.

(3) Where an enterprise contravenes any of the provisions of this Act the court may, in addition to any penalty it may impose for a criminal offence, impose a fine up to ten per cent of the annual turnover of the enterprise.

(4) In imposing a fine under subsection (3) the court shall take into account –

- (a) the estimate of the economic cost of the contravention to the consumers, users of the services in question or any other person affected by the contravention;
- (b) the estimate of the economic benefit of the contravention to the enterprise;
- (c) the time for which the contravention is in effect if continuing;
- (d) the number and seriousness of any other contraventions, if any, committed by the enterprise; and
- (e) any other matter the court considers appropriate in the circumstances.

PART XI**MISCELLANEOUS**

Regulations

41. (1) The Minister may make Regulations for the purpose of giving effect to this Act.

(2) Notwithstanding the generality of subsection (1), the Minister may make Regulations with respect to—

(a) any matter that is required to be prescribed under this Act; and

(b) the sale of goods or services by a person using electronic communications.

(3) Regulations made under this section may provide that a contravention of a specified provision shall be an offence and may provide penalties of a fine not exceeding fifty thousand dollars or imprisonment for a term not exceeding twelve months or both.

(4) Regulations made under this section are subject to negative resolution of the House of Assembly.

Repeal, Chapter
145

42. The Electronic Transactions Act is repealed.

Passed in the House of Assembly this 30th day of April, 2015.

NICOLE HERBERT

Clerk of the House of Assembly.

Printed by the Government Printer at the Government Printing Office,
Camden Park, St. Vincent and the Grenadines.