ELECTRONIC TRANSACTIONS ACT

CHAPTER 145

Act No.
42 of 2007

Printed and published with the authority of the
Government of Saint Vincent and the Grenadines

CHAPTER 145

ELECTRONIC TRANSACTIONS ACT

ARRANGEMENT OF SECTIONS

PART I

Preliminary

PART IV

Accreditation

SECTION

PART V

Cryptography Providers

PART VI

Consumer Protection

PART VII

Protection of Critical Information Systems

PART VIII

Liability of Service Providers

SECTION

PART XII

General Law

CHAPTER 145

ELECTRONIC TRANSACTIONS ACT

An Act to provide for the facilitation and regulation of electronic communications and transactions, to prevent abuse of information systems, and to provide for matters connected therewith.

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.

[Act No. 42 of 2007.]

[Date of commencement: 31*st December*, 2007.]

PART I

Preliminary

1. Short title and commencement

This Act may be cited as the Electronic Transactions Act, 2007, and shall come into operation on a day appointed by the Governor-General by Proclamation in the *Gazette*.

2. Interpretation

In this Act—

"addressee" means a person who is intended by the originator to receive data message but does not include a person acting as intermediary in respect of the data message;

"advanced electronic signature" means an electronic signature which results from a process which has been accredited by the Accreditation Authority as provided for in section 29;

"authentication products or services" means products or services designed to identify the holder of an electronic signature to other persons;

"authentication service provider" means a person whose authentication products or services have been accredited by the Accreditation Authority under section 29 or recognised under section 32;

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

"certification service provider" means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with a data message;

"consumer" means any natural 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 that supplier;

"critical information system" means a collection of critical information in electronic form from where it may be accessed, reproduced or extracted;

"critical information systems administrator" means the person responsible for the management and control of a critical information system;

"cryptography product" means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring—

(*a*) that the data can be accessed only by relevant persons;

(*b*) the authenticity of the data;

(*c*) the integrity of the data;

(*d*) that the source of the data can be correctly ascertained;

"cryptography provider" means any person who provides or who proposes to provide cryptograph services or products in the State;

"cryptography service" means any service which is provided to a sender or recipient of a data message or to anyone storing a data message, and is designed to facilitate the use of cryptographic techniques for the purpose of ensuring—

(*a*) that the data or data message can be accessed or can be put into an intelligible form only by certain persons;

(*b*) that the authenticity or integrity of the data or data message is capable of being ascertained;

(*c*) the integrity of the data or data message; or

(*d*) that the source of the data or data message can be correctly ascertained;

"cyber inspector" means a person appointed under Part IX;

"data" means electronic representations of information in any form;

"data message" means data generated, received or stored by electronic means and includes—

(*a*) a voice, where the voice is used in an automated transaction;

(*b*) a stored record;

"e-government services" means any public service provided by electronic means by any public authority of the State;

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

"electronic signature" means data attached to, incorporated in or logically associated with other data and which is intended by the user to serve as a signature;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the internet and wireless application protocol communications;

"Minister" means the Minister responsible for telecommunications;

"Ministry" means the Ministry responsible for telecommunications;

"public authority" includes—

(*a*) Parliament, or any committee of Parliament;

(*b*) the Cabinet as constituted under the Constitution;

(*c*) a Ministry or a department or division of a Ministry;

(*d*) a local authority;

(*e*) a public statutory corporation or body;

(*f*) a body corporate or an incorporated body established for a public purpose, which is owned or controlled by the State;

(*g*) an embassy, consulate or mission of the State or any office of the State situated outside of Saint Vincent and the Grenadines whose functions include the provision of diplomatic or consular services for or on behalf of Saint Vincent and the Grenadines;

(*h*) any other body designated by the Minister by Regulation made under this Act, to be a public authority for the purposes of this Act;

"rule of law" means the common law, an Act of Parliament or subsidiary legislation made under an Act of Parliament;

"signature creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

"State" means Saint Vincent and the Grenadines;

"transaction" means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services;

"website" or **"web portal"** means any computer on the internet containing a home page or web page.

3. Act to bind Crown

This Act shall bind the Crown.

PART II

Legal Requirements for Electronic Transactions

4. Non-discrimination against electronic information

(1) Information shall not be denied legal effect, validity or enforcement solely on the ground that it is in electronic form.

(2) In sections 5, 6, 7, 8 and 22—

(*a*) where a rule of law requires information to be in writing, given, signed, original or retained, the requirement is met if the section is complied with;

(*b*) where a rule of law provides consequences where the information is not in writing, given, signed, original or retained, the consequences are avoided if the section is complied with; and

(*c*) where a rule of law provides consequences if the information is in writing, given, signed, original or retained, the consequences are achieved if the section is complied with.

5. Writing requirements

(1) A rule of law that requires information to be in writing or to be given in writing is satisfied by information in electronic form if the information is accessible so as to be usable for subsequent reference.

(2) In subsection (1), giving 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;

(*h*) making, varying or cancelling a choice;

(*i*) filing or lodging an objection;

(*j*) giving a statement of reasons.

(3) Information in electronic form is not given unless the information is capable of being retained by the person to whom it is given.

6. Prescribed forms

A rule of law that requires a person to provide information in a prescribed non-electronic form to another person is satisfied by the provision of the information in an electronic form that is—

(*a*) organised in the same or substantially the same way as the prescribed non-electronic form;

(*b*) accessible to the other person so as to be usable for subsequent reference; and

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

7. Original documents

A rule of law that requires a person to produce, examine or keep an original document is satisfied if the person produces, examines or retains the document in electronic form, if—

(*a*) having regard to all the relevant circumstances, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and

(*b*) in a case where an original document is to be given to the person in electronic form it is accessible so as to be usable for subsequent reference and capable of being retained by the person.

8. Keeping written documents

A rule of law that requires a person to keep information that is in writing or that is in electronic form, is satisfied by keeping the information in electronic form, if—

(*a*) having regard to all the relevant circumstances when the electronic form of the document was generated, the method of generating the electronic form of the document provided a reliable means of assuring the maintenance of the integrity of the information contained in the document; and

(*b*) when the electronic form of the document was generated, the information contained in the electronic form of the document is accessible so as to be usable for subsequent reference to any person entitled to have access to the information or to require its production.

9. Soundness of information

For the purposes of sections 7 and 8 the soundness of the information is maintained if the information has remained complete and unaltered, apart from—

(*a*) the addition of any endorsement; or

(*b*) any immaterial change,

which arises in the normal course of communications, storage or display.

10. E-government services

(1) If a public authority has power to create, collect, receive, store, transfer, distribute, publish, issue or otherwise deal with information and documents, it has the power to do so electronically.

(2) Subsection (1) is subject to any rule of law that expressly prohibits the use of electronic means or expressly requires them to be used in specified ways.

(3) For the purposes of subsection (2) a reference to writing or signature does not in itself constitute an express prohibition of the use of electronic means.

(4) Where a public authority consents to receive any information in electronic form, it may specify—

(*a*) the manner, and format in which the information shall be communicated to it;

(*b*) the type or method of electronic signature required, if any;

(*c*) control processes and procedures to ensure integrity, security and confidentiality of the information;

(*d*) any other attributes for the information that are currently specified for corresponding information on paper.

(5) The requirements of subsections (1) and (3) and section 6 also apply to information described in subsection (4) of this section.

(6) A public authority may make or receive payment in electronic form by any manner specified by the authority and approved by the Minister of Finance.

11. Notarisation, acknowledgment and certification

(1) Where a rule of law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, the requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.

(2) Where a rule of law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, the requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.

(3) Where a rule of law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, the requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

12. Other requirements

(1) A requirement in a rule of 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 data message that is capable of being reproduced by that addressee.

(2) An expression in a rule of law, whether used as a noun or verb, including the terms, "document", "record", "file", "submit", "register", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect, must be

interpreted so as to include or permit such form, format or action in relation to a data message unless otherwise provided for in this Act.

(3) Where a seal is required by a rule of 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, the requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(4) Where a rule of law requires or permits a person to send a document or information by registered or certified post, the requirement is met if an electronic copy of the document or information is sent to the Saint Vincent and the Grenadines Postal Corporation, is registered by the Saint Vincent and the Grenadines Postal Corporation and sent by the Saint Vincent and the Grenadines Postal Corporation to the electronic address provided by the sender.

13. Exclusions

This Act does not apply to—

(*a*) the creation or transfer of interests in real property;

(*b*) negotiable instruments;

(*c*) documents of title;

(*d*) wills and trusts created by wills;

(*e*) any class of documents, transactions or rules of law excluded by Regulations under this Act.

14. Certain other laws not affected

(1) Nothing in this Act limits the operation of any other rule of law that expressly authorises, prohibits or regulates the use of information in electronic form including a method of electronic or advanced electronic signature.

(2) Nothing in this Act limits the operation of any other rule of law requiring information to be posted or displayed in a specific manner or requiring information to be transmitted by a specified method.

(3) A reference to writing or signature does not itself constitute a prohibition for the purpose of subsection (1) or a legal requirement for the purpose of subsection (2).

15. Consent

(1) Nothing in this Act requires a person to use, provide or accept information in electronic form without consent, but a person's consent to do so may be inferred from the person's conduct.

(2) Notwithstanding subsection (1), the consent of a public authority to accept information in electronic form may not be inferred from its conduct but must be expressed by communication accessible to the public or to those most likely to communicate with it for particular purposes.

(3) Nothing in this Act authorises a public authority to require any person to use, provide or accept information in electronic form without consent.

16. Contracts

(1) Unless the parties agree otherwise, an offer, the acceptance of an offer or any other matter that is material to the formation or operation of a contract may be expressed—

(*a*) by means of information in electronic form; or

(*b*) by an act that is intended to result in electronic communication, such as touching or clicking an appropriate icon or other place on a computer screen, or by speaking.

(2) A contract is not invalid or unenforceable by reason only of being in electronic form.

17. Automated contracts

A contract may be formed by interaction of computer programmes or other electronic means used to initiate an act or to respond to electronic information, in whole or in part, without review by an individual at the time of the response or act.

18. Mistakes in partly automated contracts

(1) An electronic transaction between an individual and another person's automated source of information has no legal effect if—

(*a*) the individual makes a material error in electronic information or an electronic document used in the transaction;

(*b*) the automated source of information does not give the individual an opportunity to prevent or correct the error;

(*c*) on becoming aware of the error, the individual promptly notifies the other person; and

(*d*) in a case where consideration is received as a result of the error, the individual, returns or destroys the consideration in accordance with the other person's instructions, deals with the consideration in a reasonable manner, and does not benefit materially by receiving the consideration.

(2) This section does not limit any other rule of law relating to mistake.

19. Expressions of intent

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

20. Time and place of sending and receiving electronic communications

(1) An electronic communication is sent when it enters an information system outside the sender's control or, if the sender and the addressee use the same information system, when it becomes capable of being retrieved and processed by the addressee.

(2) An electronic communication is presumed to be received by the addressee—

(*a*) if the addressee has designated or uses an information system for the purposes of receiving communications of the type sent, when it enters that information system and becomes capable of being retrieved and processed by the addressee; or

(*b*) if the addressee has not designated or does not use an information system for the purpose of receiving communications of the type sent, or if the addressee has designated or used such a system but the communication has been sent to another system, when the addressee becomes aware of the communication in the addressee's information system and it becomes capable of being retrieved and processed by the addressee.

(3) Subsections (1) and (2) apply unless the parties agree otherwise.

(4) An electronic communication is deemed to be sent from the sender's place of business and received at the addressee's place of business.

(5) If the sender or addressee has more than one place of business, the place of business for the purpose of subsection (4) is the one with the closest relationship to the underlying transaction to which the electronic communication relates or, if there is no underlying transaction, the person's principal place of business.

(6) If the sender or addressee does not have a place of business, the person's place of habitual residence is deemed to be the place of business for the purposes of subsection (4).

21. Attributions of electronic communications

An electronic communication is that of the person who sends it, if it was sent by—

(*a*) the originator personally;

(*b*) a person who had authority to act on behalf of the originator in respect of the electronic communication; or

(*c*) an information system programmed by or on behalf of the originator to operate automatically unless it is proved that the information system did not properly execute such programming.

PART III

Electronic Signatures

22. Signature

(1) If a rule of law requires the signature of a person, the requirement is met by an electronic signature if the electronic signature that is used is as reliable and as appropriate for the purpose for which it was generated or communicated, in all the circumstances, including any relevant agreements.

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

(3) An electronic signature is not without legal force and effect merely on the ground that it is in electronic form.

(4) Parties may agree to use a particular method of electronic signature, unless otherwise provided by law.

(5) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, the requirement is met in relation to the data message if—

(*a*) the signature creation data is linked to the signatory and no other person;

(*b*) the signature creation data at the time of signing is under the control of the signatory and no other person;

(*c*) any alteration to the electronic signatures made after the time of signing is detectable; and

(*d*) where a purpose of the legal requirement for a signature is to provide assurance as to the soundness of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(6) Subsection (5) does not limit the ability of a person—

(*a*) to establish in any other way, for the purpose of satisfying the requirement referred to in subsection (1), the reliability of an electronic signature; or

(*b*) to adduce evidence of the non-reliability of an electronic signature.

23. Standards for signatures

The Minister may make regulations prescribing methods which satisfy the requirements of section 22.

24. Conduct of a person relying on an electronic signature

A person relying on an electronic signature shall bear the legal consequences of his failure to take reasonable steps to verify the reliability of an electronic signature.

25. Recognition of foreign electronic documents and signatures

In determining whether or to what extent information in electronic form is legally effective, no regard shall be had to the location where the information was created or used, or to the place of business of its creation.

PART IV

Accreditation

26. Interpretation

In this Part, unless the context indicates otherwise, **"accreditation"** means recognition of an authentication product or service by the Accreditation Authority.

27. Designation of Accreditation Authority

(1) For the purposes of this Part the Minister shall be the Accreditation Authority.

(2) Public officers may be appointed or designated as Deputy Accreditation Authorities and officers of the Accreditation Authority.

28. Powers and duties of Accreditation Authority

(1) The Accreditation Authority may—

(*a*) monitor the conduct, systems and operations of an authentication service provider to ensure its compliance with section 30 and the other obligations of authentication service providers under this Act;

(*b*) temporarily suspend or revoke the accreditation of an authentication product or service; and

(*c*) appoint an independent auditing firm to conduct periodic audits of the authentication service provider to ensure its compliance with section 30 and the other obligations of authentication service providers under this Act.

(2) The Accreditation Authority shall maintain a publicly accessible database in respect of—

(*a*) authentication products or services accredited in terms of section 30;

(*b*) authentication products and services accepted in terms of section 32;

(*c*) revoked accreditations or acceptances; and

(*d*) any other information as may be prescribed.

29. Accreditation of authentication products and services

(1) The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures.

(2) An application for accreditation shall be—

(*a*) made to the Accreditation Authority in the prescribed manner supported by the prescribed information; and

(*b*) accompanied by a non-refundable prescribed fee.

(3) A person who falsely holds out its products or services to be accredited by the Accreditation Authority commits an offence and is liable on summary conviction to a fine not exceeding ten thousand dollars.

30. Criteria for accreditation

(1) The Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an advanced electronic signature to which such authentication products or services relate—

(*a*) is uniquely linked to the user;

(*b*) is capable of identifying the user;

(*c*) is created using means that can be maintained under the sole control of the user;

(*d*) will be linked to the information to which it relates in such a manner that any subsequent change of the information is detectable; and

(*e*) is based on the face-to face identification of the user.

(2) For the purposes of subsection (1), the Accreditation Authority must have regard to the following factors in respect of an authentication service provider prior to accrediting authentication products or services—

(*a*) its financial and human resources including its assets;

(*b*) the quality of its hardware and software systems;

(*c*) its procedures for processing of products and services;

(*d*) the availability of information to third parties relying on the authentication product or service;

(*e*) the regularity and extent of audits by an independent body;

(*f*) the factors referred to in subsection (4) where the products and services are rendered by a certification service provider; and

(*g*) any other relevant factor that may be prescribed.

(3) For the purposes of subsection (2)(*b*) and (*c*), the hardware and software systems and procedures must—

(*a*) be reasonably secure from intrusion and misuse;

(*b*) provide a reasonable level of availability, reliability and correct operation;

(*c*) be reasonably suited to performing their intended functions; and

(*d*) adhere to generally accepted security procedures.

(4) For the purposes of subsection (1), where the products or services are provided by a certification service provider, the Accreditation Authority may stipulate, prior to accrediting authentication products or services—

(*a*) the technical and other requirements which certificates must meet;

(*b*) the requirements for issuing certificates;

(*c*) the requirements for certification practice statements;

(*d*) the responsibilities of the certification service provider;

(*e*) the liability of the certification service provider;

(*f*) the records to be kept and the manner in which and length of time for which they must be kept;

(*g*) requirements as to adequate certificate suspension and revocation procedures; and

(*h*) requirements as to adequate notification procedures relating to certificate suspension and revocation.

(5) The Accreditation Authority may impose any conditions or restrictions necessary when accrediting an authentication product or service.

31. Suspension or revocation of accreditation

(1) The Accreditation Authority shall suspend or revoke an accreditation if it is satisfied that the authentication service provider has failed or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted under section 30 or acceptance was given in terms of section 32.

(2) Subject to the provisions of subsection (3), the Accreditation Authority shall not suspend or revoke the accreditation or acceptance contemplated in subsection (1) unless it has—

(*a*) notified the authentication service provider in writing of the intention to do so;

(*b*) given a description of the alleged breach of any of the requirements, conditions or restrictions subject to which accreditation was granted under section 30 or acceptance was given in terms of section 32; and

(*c*) afforded the authentication service provider the opportunity to—

(i) respond to the allegations in writing,

(ii) remedy the alleged breach within a reasonable time.

(3) The Accreditation Authority may suspend accreditation granted under section 30 or acceptance given in terms of section 32 with immediate effect for a period not exceeding ninety days, pending implementation of procedures required by subsection (2) of this section, if the continued accreditation or acceptance of the authentication service provider is reasonably likely to result in irreparable harm to consumers or any person involved in an electronic transaction in Saint Vincent and the Grenadines.

(4) An authentication service provider whose products or services have been accredited under the terms of this Act may terminate the accreditation at any time, subject to terms and conditions as may be agreed to at the time of accreditation or thereafter.

32. Acceptance of foreign authentication service providers, products or services

(1) The Minister, may, by notice in the *Gazette* and subject to conditions as may be determined by him, accept the accreditation or similar recognition granted to an authentication service provider or its authentication products or services in any foreign jurisdiction.

(2) An authentication service provider who falsely holds out its products or services to have been accepted by the Minister commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars.

33. Regulations under this Part

The Minister may make Regulations in respect of—

(*a*) the rights and obligations of persons relating to the provision of accredited products and services;

(*b*) the manner in which the Accreditation Authority must administer and supervise compliance with the obligations in relation to paragraph (*a*);

(*c*) the procedure pertaining to the granting, suspension and revocation of accreditation;

(*d*) fees to be paid;

(*e*) information security requirements or guidelines; and

(*f*) any other relevant matter which it is necessary or expedient to prescribe for the proper implementation of this Part.

PART V

Cryptography Providers

34. Register of cryptography providers

(1) The Minister shall establish and cause to be maintained a register of cryptography providers.

(2) The following particulars in respect of a cryptography provider shall be recorded in the register—

(*a*) the name and address of the cryptography provider;

(*b*) a description of the type of cryptography service or product being provided; and

(*c*) any other particulars as may be prescribed to adequately identify and locate the cryptography provider and its products or services.

(3) A cryptography provider is not required to disclose confidential information or trade secrets in respect of its cryptography products or services by virtue of this section.

35. Registration or acceptance

(1) A person shall not provide cryptography services or products in the State unless—

(*a*) he is registered as a cryptography provider; or

(*b*) his accreditation or similar recognition as a cryptography provider in any foreign jurisdiction is accepted by the Minister.

(2) A cryptography provider shall in the prescribed manner provide the Minister with the information required and pay the prescribed fee.

(3) For the purposes of subsection (1), a cryptography service or product is regarded as being provided in the State if it is provided—

(*a*) from premises in the State;

(*b*) to a person who is present in the State when that person makes use of the service or product; or

(*c*) to a person who uses the service or product for the purposes of a business carried on in the State or from premises in the State.

36. Restriction on disclosure of information

(1) Information contained in the register in respect of section 34 shall not be disclosed to any other person other than the officers of the Accreditation Authority who are responsible for keeping the register.

(2) The restriction on the disclosure of the information in subsection (1) shall not apply in respect of information which is disclosed—

(*a*) to a relevant authority which investigates a criminal offence or for the purposes of criminal proceedings;

(*b*) to government agencies responsible for safety and security in the State pursuant to an official request;

(*c*) to a cyber inspector;

(*d*) pursuant to the provisions of the Freedom of Information Act; or

(*e*) for the purposes of any civil proceedings which relate to the provision of cryptography services or products and to which a cryptography provider is a party.

[Chapter 367.]

PART VI

Consumer Protection

37. Scope of application

(1) This Part applies only to electronic transactions.

(2) This Part does not apply to a regulatory authority established under a rule of law if that rule of law prescribes consumer protection provisions in respect of electronic transactions.

38. Information to be provided

(1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction shall make the following information available to consumers on the website where the goods or services are offered—

(*a*) its full name and legal status;

(*b*) its physical address and telephone number;

(*c*) its website 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;

(*g*) the manner 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 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; and

(*m*) the rights of consumers under section 36, where applicable.

(2) The supplier shall provide a consumer with the opportunity—

(*a*) to review the entire electronic transaction;

(*b*) to correct any mistakes; and

(*c*) to withdraw from the transaction before finally placing any order.

(3) If the supplier fails to comply with the provisions of subsection (1) or (2), 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.

(5) The supplier shall utilise 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).

39. Cooling off period

(1) A consumer is entitled to cancel without reason and without penalty any transaction and any related credit agreement for the supply—

(*a*) of goods within seven days after the date of receipt of the goods; or

(*b*) of services within seven 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 but not limited to, investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;

(*b*) by way of an auction;

(*c*) for the supply of food stuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer;

(*d*) for services which began with the consumer's consent before the end of the seven day period referred to in subsection (1);

(*e*) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;

(*f*) where the goods—

(i) are made to the consumer's specifications,

(ii) are clearly personalised,

(iii) by reason of their nature cannot be returned, or

(iv) are likely to deteriorate or expire rapidly;

(*g*) where audio or video recordings or computer software were unsealed by the consumer;

(*h*) for the sale of newspapers, periodicals, magazines and books;

(*i*) for the provision of gaming and lottery services; or

(*j*) for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is concluded, to provide these services on a specific date or within a specific period.

(5) This section must not be construed as prejudicing the rights of a consumer provided for in any other law.

40. Unsolicited goods, services or communications

(1) A person who sends unsolicited commercial communications to consumers must provide the consumer with—

(*a*) the option to cancel his subscription to the mailing list of that person; and

(*b*) the identifying particulars of the source from which that person obtained the consumer's personal information, on the request of the consumer.

(2) Where a consumer fails to respond to an unsolicited commercial communication, no agreement is considered to be concluded.

(3) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding five thousand dollars.

(4) A person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcomed, commits an offence and is liable upon summary conviction to a fine not exceeding six thousand dollars.

41. Applicability of foreign law

The protection provided to consumers in this Part applies irrespective of the legal system applicable to the agreement in question.

42. Non exclusion

Any provision in an agreement which excludes any rights provided for in this Part is void.

43. Complaint

A consumer may lodge a complaint with the appropriate consumer protection body in respect of non-compliance with the provisions of this Part by a supplier.

PART VII

Protection of Critical Information Systems

44. Application

The provisions of this Part only apply to critical information systems of public authorities.

45. Identification of critical information and critical information systems

The Minister may by notice in the *Gazette*—

(*a*) declare certain classes of information which are of importance to the protection of the national security of Saint Vincent and the Grenadines or the economic and social well-being of its citizens to be critical information for the purposes of this Part;

(*b*) establish procedures to be followed in the identification of critical information systems for the purposes of this Part.

46. Registration of critical information systems

(1) The Minister may by notice in the *Gazette* determine—

(*a*) requirements for the registration of critical information systems with the Ministry or such other body as the Minister may specify;

(*b*) procedures to be followed for registration; and

(*c*) any other matter relating to registration.

(2) For the purposes of this Part, registration of critical information systems means recording the following information in a register maintained by the Ministry or by such other body as the Minister may specify—

(*a*) the full name, address and contact details of the critical information system administrator;

(*b*) the location of the critical information system including the location of component parts thereof where a critical information system is not stored at a single location; and

(*c*) a general description of the categories or types of information stored in the system excluding the contents of such system.

47. Management of critical information systems

(1) The Minister may prescribe minimum standards or prohibitions in respect of—

(*a*) the general management of critical information systems;

(*b*) access to, transfer and control of critical information systems;

(*c*) infrastructural or procedural rules and requirements for securing the integrity and authenticity of critical information;

(*d*) procedures and technological methods to be used in the storage or archiving of critical information systems;

(*e*) disaster recovery plans in the event of loss of critical information systems or parts thereof;

(*f*) any other matter required for the adequate protection, management and control of critical information systems.

(2) This Part must not be construed so as to prejudice the right of a public authority to perform any function authorised in terms of any other law.

48. Restrictions on disclosure of information

(1) Information contained in the register provided for in section 46 must not be disclosed to any other person than to employees of the Ministry or body who are responsible for keeping the register.

(2) The restriction on the disclosure of information in subsection (1) does not apply in respect of information which is disclosed—

(*a*) to a relevant authority which is investigating a criminal offence or for the purposes of any criminal proceedings;

(*b*) to public authorities responsible for safety and security in Saint Vincent and the Grenadines pursuant to an official request;

(*c*) to an independent auditor for the purposes of section 49;

(*d*) pursuant to the provisions of the Freedom of Information Act;

(*e*) for the purposes of any civil proceedings which relate to the critical information system or parts thereof.

[Chapter 367.]

49. Right of inspection

(1) The Minister may, from time to time, cause audits to be performed in relation to critical information systems to evaluate compliance with Regulations made under this Part.

(2) The audit may be performed by an independent auditor.

50. Non-compliance with Part VII

Where the audit performed under section 49 reveals non-compliance with this Part, the Minister shall notify the appropriate officer of the public authority in writing of the non-compliance, stating—

(*a*) the finding of the audit report;

(*b*) the action required to remedy the non-compliance; and

(*c*) the period within which the remedial action must be performed.

PART VIII

Liability of Service Providers

51. Interpretation

In this Part, **"service provider"** means any person providing information system services.

52. Recognition of representative body

(1) The Minister may, on application by an industry representative body for service providers, by notice in the *Gazette*, recognise the body.

(2) The Minister may only recognise a representative body referred to in subsection (1) if the Minister is satisfied that—

(*a*) its members are subject to a code of conduct;

(*b*) the code of conduct requires continued adherence to adequate standards of conduct; and

(*c*) the representative body is capable of monitoring and enforcing its code of conduct adequately.

53. Conditions for eligibility

The limitations on liability established by this Part apply to a service provider only if—

(*a*) the service provider is a member of the representative body referred to in section 52; and

(*b*) the service provider has adopted and implemented the official code of conduct of that representative body.

54. Mere conduit

(1) A service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the 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 data;

(*d*) does not modify the data contained in the transmission.

(2) The acts of transmission, routing and 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.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

55. Caching

(1) A service provider that transmits data provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider—

(*a*) does not modify the data;

(*b*) complies with the conditions on access to the data;

(*c*) complies with rules regarding the updating of the data, specified in a manner widely recognised and used by the industry;

(*d*) does not interfere with the lawful use of technology, widely recognised and used by the industry, to obtain information on the use of data; and

(*e*) removes or disables access to the data it has stored upon receiving a notification referred to in section 57.

(2) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in the terms of any other law.

56. Hosting

(1) A service provider that provides a service that consists of the storage of data provided by a recipient of the service, is not liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider—

(*a*) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party; or

(*b*) is not aware of facts or circumstances from which infringing activity or the infringing nature of the data message is apparent; and

(*c*) upon receipt of a notification referred to in section 57, acts expeditiously to remove or to disable access to the data.

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

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent an unlawful activity in terms of any other law.

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

57. Notification of unlawful activity

(1) In this section, **"competent public authority"** means an inspector appointed under this Act or under the Telecommunications Act or a member of the Royal Saint Vincent and the Grenadines Police Force.

[Chapter 418.]

(2) A person may lodge a notification of alleged unlawful activity with a competent public authority in relation to the services provided by a service provider.

(3) The competent public authority shall issue to the appropriate service provider the notification received under subsection (2) and shall investigate or cause the complaint to be investigated.

(4) For the purposes of this Part, notification of unlawful activity shall be in writing and be addressed to the service provider or its designated agent and must include—

(*a*) the full names and address of the complainant;

(*b*) the written or electronic signature of the complainant;

(*c*) identification of the right that has allegedly been infringed;

(*d*) identification of the material or activity that is claimed to be subject of unlawful activity;

(*e*) the remedial action required to be taken by the 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 knowledge true and correct; and

(*i*) an undertaking given by the complainant to indemnify the service provider from any liability incurred as a result of remedial action taken by it in complying with the notification.

58. No general obligation to monitor

When providing the services contemplated in this Part, there is no general obligation of a service provider to—

(*a*) monitor the data which it transmits or stores; or

(*b*) actively seek facts or circumstances indicating an unlawful activity.

59. Obligations not affected by this Part

This Part does not affect—

(*a*) any obligation founded on an agreement;

(*b*) the obligation of a service provider under a licensing or other regulatory regime.

PART IX

Cyber Inspectors

60. Savings

(1) An officer of the Ministry or any other qualified person may be appointed as a cyber inspector to perform the functions provided for in this Part.

(2) A cyber inspector must be provided with a certificate of appointment signed by or on behalf of the Minister in which it is stated or evidenced that he is appointed as a cyber inspector.

(3) A certificate provided for in subsection (2) may be in the form of an advanced electronic signature.

(4) When a cyber inspector performs any function in terms of this Act, he shall—

(*a*) be in possession of a certificate of appointment referred to in subsection (2); and

(*b*) show that certificate to any person who—

(i) is subject to an investigation or an employee of that person, or

(ii) requests to see the certificate.

(5) A person who—

(*a*) hinders or obstructs a cyber inspector in the performance of his functions; or

(*b*) falsely holds himself out as a cyber inspector,

commits an offence and is liable on summary conviction to a fine not exceeding five thousand dollars or imprisonment for a term not exceeding one year, or both a fine and imprisonment.

61. Appointment of cyber inspectors

(1) A cyber inspector may—

(*a*) monitor and inspect any website or activity on an information system in the public domain and report any unlawful activity to the appropriate authority;

(*b*) in respect of a cryptography service provider—

(i) investigate the activities of a cryptography service provider in relation to its compliance or non-compliance with the provisions of this Act, and

(ii) issue an order in writing to a cryptography service provider to comply with the provisions of this Act;

(*c*) in respect of an authentication service provider—

(i) investigate the activities of an authentication service provider in relation to its compliance or non-compliance with the provisions of this Act,

(ii) investigate the activities of an authentication service provider falsely holding itself, its products or services out as having been accredited by the Ministry,

(iii) issue an order in writing to an authentication service provider to comply with the provisions of this Act;

(*d*) in respect of a critical information system administration, perform an audit as provided for in section 49.

(2) A cyber inspector may assist police officers in an investigation arising under this Act.

62. Powers to inspect, search and seize

(1) A cyber inspector may, in the performance of his functions on the authority of a warrant issued in terms of section 63, enter any premises or access an information system that has a bearing on an investigation and—

(*a*) search the premises or the information system;

(*b*) search any person on the premises if there are reasonable grounds for believing that the person has personal possession of an article, document or record that has a bearing on the investigation;

Powers of cyber inspectors—

(*c*) take extracts from, or make copies of, any book, document or record that is on or in the premises or information system that has a bearing on the investigation;

(*d*) demand the production and inspect relevant licences and registration certificates as provided in any law;

(*e*) inspect any facilities on the premises which are linked or associated with the information system and which have a bearing on the investigation;

(*f*) have access to and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to believe is or has been used in connection with any offence on which the investigation is based;

(*g*) use or cause to be used any information system or part thereof to search any data contained in or available to such information systems;

(*h*) require the person by whom or on whose behalf the cyber inspector has reasonable cause to believe the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system, to provide him with such reasonable technical assistance as he may require for the purposes of this Part; or

(*i*) make inquiries as may be necessary to ascertain whether the provisions of this Act or any other law on which an investigation is based have been complied with.

(2) A person who refuses to co-operate or hinders a person conducting a lawful search and seizure in terms of this section commits an offence and is liable to pay a fine not exceeding five thousand dollars or a term of imprisonment not exceeding one year, or both a fine and imprisonment.

63. Obtaining a warrant

(1) A cyber inspector may obtain a warrant pursuant to section 41 of the Criminal Procedure Code.

[Chapter 172.]

(2) For the purposes of subsection (1), a warrant may be issued where—

(*a*) an offence under this Act has been committed within the State; or

(*b*) the subject of an investigation is either—

(i) a citizen or ordinarily resident in the State, or

(ii) present in the State at the time when the warrant is applied for; or

(*c*) information pertinent to the investigation is accessible from within the area of jurisdiction of the court.

(3) A warrant to enter, search and seize may be issued at any time and shall—

(*a*) identify the premises or information system that may be entered and searched; and

(*b*) specify which act may be performed thereunder by the cyber inspector to whom it is issued.

(4) A warrant to enter and search premises under this Part may be executed only during the day, unless the judicial officer, who issues it authorises that it may be executed at any other time.

PART X

Information Systems and Computer Related Crimes

64. Interpretation

In this Part, unless the contrary intention appears—

"access" includes the action of a person who, after taking note of any data, becomes aware of the fact that he is not authorised to access that data and still continues to access that data;

"electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature, transmitted in whole or in part by a wire, radio, computer, electromagnetic, photo-electric or photo-optical system;

"electronic data storage medium" means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of other article or device;

"electronic mail" means the transmission of information or communication by the use of the internet, a computer, a facsimile machine, a pager, a cellular telephone or other electronic means sent to a person identified by a unique address or address numbers and received by that person;

"service provider" means—

(*a*) a public or private entity that provides to users of its services the ability to communicate by means of an information system;

(*b*) any other entity that processes or stores computer data on behalf of that entity or those users;

"traffic data" means computer data that—

(*a*) relates to a communication by means of a computer system;

(*b*) is generated by a computer system that is part of the chain of communication;

(*c*) shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services.

65. Scope of Part

This Part applies to an act done or an omission made in any or all of the following circumstances—

(*a*) in Saint Vincent and the Grenadines;

(*b*) on a ship or air craft registered in Saint Vincent and the Grenadines;

(*c*) by a national of Saint Vincent and the Grenadines;

(*d*) by a national of Saint Vincent and the Grenadines outside the territory of Saint Vincent and the Grenadines, if the person's act or omission would also constitute an offence under a law of the country where the offence was committed;

(*e*) by a person who is not a national of Saint Vincent and the Grenadines outside the territory of Saint Vincent and the Grenadines if the person's act or omission would also constitute an offence under a law of the country where the offence was committed and at least one result of the act or omission occurs wholly or partly in Saint Vincent and the Grenadines or on a ship or aircraft registered in Saint Vincent and the Grenadines.

66. Illegal access

A person who intentionally, without lawful excuse or justification, accesses the whole or any part of an information system commits an offence and is liable on conviction on indictment to a fine not exceeding five thousand dollars or to a term of imprisonment not exceeding two years.

67. Interfering with data

(1) A person who, intentionally or recklessly, without lawful excuse or justification, does any of the following acts—

(*a*) destroys or alters data;

(*b*) renders data meaningless, useless or ineffective;

(*c*) obstructs, interrupts or interferes with the lawful use of data;

(*d*) obstructs, interrupts or interferes with any person in the lawful use of data;

(*e*) denies access to data to any person entitled to it,

commits an offence and is liable on conviction on indictment to a fine not exceeding thirty thousand dollars or a term of imprisonment not exceeding four years, or to both a fine and imprisonment.

(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.

68. Interfering with an information system

(1) A person who intentionally or recklessly, without lawful excuse or justification—

(*a*) hinders or interferes with the functioning of an information system; or

(*b*) hinders or interferes with a person who is lawfully using or operating an information system,

commits an offence and is liable on conviction on indictment to a fine not exceeding one hundred thousand dollars or to a term of imprisonment not exceeding ten years, or both.

(2) In subsection (1), **"hinder"**, in relation to an information system, includes—

(*a*) cutting the electricity supply to an information system;

(*b*) causing electromagnetic interference to an information system;

(*c*) corrupting a computer system by any means; or

(*d*) inputting, deleting or altering data.

69. Illegal interception of data

A person who intentionally without lawful excuse or justification intercepts by technical means—

(*a*) any private transmission to, from or within an information system; or

(*b*) electromagnetic emissions from an information system that are carrying data,

commits an offence and is liable on conviction on indictment to a fine not exceeding fifteen thousand dollars or to a term of imprisonment not exceeding one year, or to both a fine and imprisonment.

70. Illegal devices

(1) A person commits an offence if the person—

(*a*) intentionally or recklessly, without lawful excuse or justification, produces, sells, offers for sale, procures for use, designs, adapts for use, imports, exports, distributes or otherwise makes available—

(i) a device, including a computer programme, that is designed primarily or adapted to overcome security measures for the protection of data for the purpose of contravening section 66, 67, 68 or 69,

(ii) a password, access code or similar data by which the whole or any part of an information system is capable of being accessed, intercepted or interfered with;

(*b*) has an item mentioned in subparagraph (i) or (ii) in his possession with the intent that it be used by any person to unlawfully overcome security measures designed to protect data or access thereto for the purpose of contravening section 66, 67, 68 or 69.

(2) A person found guilty of an offence under this section is liable on conviction on indictment to a fine not exceeding ten thousand dollars or to a term of imprisonment not exceeding twelve months, or to both a fine and imprisonment.

71. Child pornography

(1) A person who intentionally, does any of the following acts—

(*a*) publishes child pornography through an information system;

(*b*) produces child pornography for the purpose of its publication through an information system; or

(*c*) possesses child pornography in an information system or on an electronic data storage medium,

commits an offence and is liable on conviction on indictment—

(*d*) in the case of an individual, to a fine not exceeding twenty thousand dollars or a term of imprisonment not exceeding fifteen years, or to both a fine and imprisonment;

(*e*) in the case of a corporation to a fine not exceeding twenty-five thousand dollars.

(2) It is a defence to a charge of an offence under subsection (1)(*a*) or (*c*) if the person establishes that the child pornography was for a *bona fide* scientific, research, medical or law enforcement purpose.

(3) In this section—

"child pornography" includes material that visually depicts—

(*a*) a minor engaged in sexually explicit conduct;

(*b*) a person who appears to be a minor engaged in sexually explicit conduct; or

(*c*) realistic images representing a minor engaged in sexually explicit conduct;

"minor" means a person who is under the age of fifteen years;

"publish" includes—

(*a*) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(*b*) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (*a*); or

(*c*) print, photograph, copy or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing an act referred to in paragraph (*a*).

72. Electronic fraud and identity theft

(1) A person who fraudulently causes loss of property to another person by—

(*a*) any input, access, alteration, deletion or suppression of data;

(*b*) any interference with the functioning of an information system,

with intent to procure for himself or another person an advantage, commits an offence and is liable upon conviction on indictment to a fine not exceeding ten thousand dollars or a term of imprisonment not exceeding five years, or to both a fine and imprisonment.

(2) A person who uses an information system or knowingly causes an information system to perform any function for the purpose of securing access to any programme or data held in that information system or in any other information system with intent to

impersonate or cause the impersonation of another person or with intent to steal or impersonate or cause the stealing or impersonation of their identity commits an offence and is liable on conviction on indictment to a fine not exceeding twenty-five thousand dollars or to imprisonment for a term not exceeding two years, or to both a fine and imprisonment.

73. Cyber-stalking

A person who—

(*a*) in an electronic mail or communication uses any words or language threatening to inflict bodily or mental harm to any person or to any member of that person's family or damage to the property of any person;

(*b*) uses electronic mail or communication, whether or not conversation ensues, for the purpose of abusing, annoying, threatening, terrifying, harassing or embarrassing any person;

(*c*) uses electronic mail or communication to knowingly make any false statement or representation of any kind including a statement concerning death, injury, illness, disfigurement, indecent conduct or criminal conduct with the intent to abuse, annoy, threaten, terrify, harass or embarrass,

commits an offence and is liable on summary conviction to a fine not exceeding ten thousand dollars or a term of imprisonment not exceeding five years, or to both a fine and imprisonment.

PART XI

Procedural Powers

74. Interpretation

In this Part—

"seize" includes—

(*a*) make and retain a copy of data, including by using on-site equipment;

(*b*) render inaccessible, or remove data in the accessed information system; and

(*c*) take a printout of output of data;

"thing" includes—

(*a*) an information system or part of an information system;

(*b*) another information system if—

(i) data from that information system is available to the first information system being searched, and

(ii) there are reasonable grounds for believing that the information data sought is stored in the other information system;

(*c*) a data storage medium.

75. Search and seizure warrants

If a judicial officer is satisfied on the basis of evidence on oath that there are reasonable grounds to believe that there may be data or in a place or, a thing—

(*a*) material that may constitute evidence in proving an offence; or

(*b*) material that has been acquired or used by a person as a result of an offence,

the judicial officer may issue a warrant authorising a police officer to enter the place to search and seize the data or thing.

76. Assisting Police

(1) A person who is in possession or control of an electronic data storage medium or information system that is the subject of a search under section 75 must permit, and assist if required, the person making the search to—

(*a*) access and use an information system or electronic data storage medium to search any data available to or in the system;

(*b*) obtain and copy that data;

(*c*) use equipment to make copies; and

(*d*) obtain an intelligible output from an information system in a plain text format that can be read by a person.

(2) A person who fails without lawful excuse or justification to permit a person to search or a person in making a search commits an offence and is liable on summary conviction—

(*a*) in the case of an individual, to a fine not exceeding five thousand dollars or a term of imprisonment not exceeding two years, or to both a fine and imprisonment;

(*b*) in the case of a corporation, to a fine not exceeding fifty thousand dollars.

(3) In this section, **"assist"** includes—

(*a*) providing passwords;

(*b*) providing encryption keys;

(*c*) making available any other information necessary to access an information system.

77. Record of and access to seized data

(1) If an information system or computer data has been removed or rendered inaccessible following a search or a seizure under section 75, the person who made the search must, at the time of the search or as soon as practicable after the search—

(*a*) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(*b*) give a copy of the list to—

(i) the occupier of the premises, or

(ii) the person in control of the information system.

(2) Subject to subsection (3), on request, a police officer or another authorised person shall—

(*a*) permit a person who had the custody or control of the information system, or someone acting on the person's behalf to access and copy data on the system; or

(*b*) give the person a copy of the data.

(3) The police officer or another authorised person may refuse to give access or provide copies if he has reasonable grounds for believing that giving the access, or providing the copies—

(*a*) would constitute a criminal offence;

(*b*) would prejudice—

(i) the investigation in connection with which the search was carried out,

(ii) another ongoing investigation, or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

78. Disclosure of data, etc., required for criminal investigation or proceedings

(1) If a judicial officer is satisfied on the basis of an application by a police officer that specified data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the judicial officer may order that—

(*a*) a person in Saint Vincent and the Grenadines in control of an information system produce from the system specified data or a printout or other intelligible output of that data;

(*b*) a service provider in Saint Vincent and the Grenadines produce information about persons who subscribe to or otherwise use the service.

(2) Where any material to which a criminal investigation relates consists of data stored in an electronic data storage medium, or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

79. Disclosure of stored traffic data

If a judicial officer is satisfied on the basis of an *ex parte* application by a police officer for the purpose of a criminal investigation or criminal proceedings, the judicial officer may order that a person in control of the information system disclose sufficient traffic data about a specified communication to identify—

(*a*) the service providers; and

(*b*) the path through which the communication was transmitted.

80. Preservation of data

(1) If a police officer is satisfied that—

(*a*) data stored in an information system is reasonably required for the purposes of a criminal investigation; and

(*b*) there is risk that the data may be destroyed or rendered inaccessible,

the police officer may, by written notice given to a person in control of the information system, require the person in control of the information system to ensure that the data specified in the notice be preserved for a period of up to seven days as specified in the notice.

(2) The period may be extended beyond seven days if, on an *ex parte* application, a judicial officer authorizes an extension for a further specified period of time.

81. Interception of electronic communications

If a judicial officer is satisfied on the basis of information on oath that there are reasonable grounds to believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the judicial officer may—

(*a*) order a service provider whose service is available in Saint Vincent and the Grenadines through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of data associated with specified communications transmitted by means of an information system;

(*b*) authorise a police officer to collect or record that data through application of technical means.

82. Interception of traffic data

If a police officer is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of such data, request that person to—

(*a*) collect or record traffic data associated with specified communication during a specified period;

(*b*) permit and assist a specified police officer to collect or record that data.

(2) If a judicial officer is satisfied on the basis of information on oath that there are reasonable grounds to believe that traffic data is reasonably required for the purposes of a criminal investigation, the judicial officer may authorise a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

83. Evidence

In proceedings for an offence against a law of Saint Vincent and the Grenadines, the fact that—

(*a*) it is alleged that an offence of interfering with an information system has been committed; and

(*b*) evidence has been generated from that information system,

does not of itself prevent that evidence from being admitted.

84. Confidentiality and limitation liability

(1) A service provider who without lawful authority discloses—

(*a*) the fact that an order under section 76, 77, 78, 79, 80 or 81 has been made;

(*b*) anything done under the order; or

(*c*) any data collected or recorded under the order,

commits an offence and is liable on summary conviction to a fine not exceeding twelve thousand dollars.

(2) A service provider is not liable under a civil or criminal law of Saint Vincent and the Grenadines for the disclosure of any data or other information that he discloses under section 76, 77, 78, 79, 80 or 81.

85. Extradition

An offence under Part X of this Act shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act.

[Act No. 29 of 1977.]

PART XII

General Law

86. Savings of common law

This Act does not affect criminal or civil liability in terms of the common law.

87. Delegation by Minister

The Minister may, in writing, delegate to a public authority his powers and duties—

(*a*) under Part IV as the Accreditation Authority;

(*b*) under Part V in respect of the establishment and maintenance of a register of cryptography providers.

88. Regulations and Rules

(1) The Minister may make Regulations—

(*a*) to designate an entity as a public body;

(*b*) to provide that electronic signatures for specified purposes shall be reliable as appropriate for those purposes;

(*c*) to provide that electronic signatures for specified purposes shall be created by specified means;

(*d*) to provide formats by which information may be communicated electronically, whether or not there exist prescribed non-electronic forms;

(*e*) to exclude classes of transactions, documents, or rules of law from the application of this Act;

(*f*) for any other purpose for the more effective achievement of the objects of the Act.

(2) The Chief Justice of the Eastern Caribbean Supreme Court may make rules governing the conduct of legal proceedings in respect of any matter which is required by virtue of this Act to be made.

CHAPTER 145

ELECTRONIC TRANSACTIONS ACT

SUBSIDIARY LEGISLATION

No Subsidiary Legislation