1st April 2018

GUYANA

BILL No. of 2018

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS BILL 2018

ARRANGEMENT OF SECTIONS

Section

1st April 2018

A BILL

Intituled

AN ACT to provide for the facilitation and regulation of secure electronic communications and transactions and for their legal recognition, to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce and to enhance efficient delivery of governance by public authorities by means of reliable electronic records and electronic filing of documents and for related matters.

A.D. 2018 Enacted by the Parliament of Guyana:-

PART I
PRELIMINARY

Short title.

1. This Act may be cited as the Electronic Communications and Transactions Act 2018.

Interpretation.

2. (1) In this Act –

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

"automated message system" means a computer program or an electronic or other automated means used to initiate an action or respond to electronic communications 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 an electronic record that confirms the link between a signatory and the signature creation data, identifies the signatory and the entity that issues it and includes other information such as its operational period;

"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 an electronic-commerce service provider as the end user of the goods or services offered by the provider;

"Court" means the High Court of Guyana;

"data" means any document, correspondence, memorandum, book, plan, map, drawing, pictorial or graphic work, photograph, film, microfilm, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of those things;

"digital signature" means is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document;

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

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

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

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

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

“electronic security procedure” means a procedure established under section 37 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 such as a certificate;

"electronic security procedure provider" means a person involved in the provision of an electronic security procedure and related services;

“electronic signature” means the various ways that an electronic document or record can be signed, such as a digitized image of a signature, a name typed at the end

of an e-mail message by the sender, a biometric identifier, a secret code or PIN, or a digital signature;

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

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

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

"intermediary" with respect to an electronic communication, means a person including a host who on behalf of another person, sends, receives, transmits or stores either temporarily or permanently that electronic communication or provides related services with respect to that electronic communication and includes telecommunication service providers, network service providers, internet service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes;

"Minister" means the Minster with responsibility for electronic commerce;

"originator", in relation to an electronic communication,

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

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

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

"secure electronic communication or record" means an electronic record that is treated as a secure electronic record by virtue of section 33(1);

"secure electronic signature" means an electronic signature that is treated as a secure electronic signature by virtue of section 34;

"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 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.

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

Act binds the State.

3. (1) This Act binds the State.

(2) Except as otherwise provided, nothing in this Act obliges any public authority to generate, send, receive, store or otherwise process any record by electronic means, but the Minister may, by notice published in the *Gazette*, declare that a public authority may receive and process electronic communications relating to the matters specified in the notice.

Non-application of Act. Schedule

4. (1) This Act does not apply to the documents and transactions specified in the Schedule.

(2) The Minister may, by order, amend the Schedule.

Autonomy of parties.

5. (1) Nothing in this Act shall –

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

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

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

(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.

Consumer consent to electronic record.

6. Where a statutory or legal requirement exists for a record to be provided in writing (paper form) to a consumer, the requirement for writing shall be satisfied by the record provided in electronic form if –

(a) the consumer has expressly consented to the use and has not withdrawn his consent; and

(b) prior to consenting, the consumer is provided with a clear and conspicuous statement informing the consumer-

(i) about the right to have the record provided in

paper form;

(ii) about the right to withdraw consent to have the record provided in electronic form and of any conditions, consequences or fees in the event of the withdrawal;

(iii) whether the consent applies only to the particular transaction which gave rise to the obligation to provide the record, or to identified categories of records that may be provided during the course of the parties' relationship;

(iv) of the hardware and software requirements for access to, and retention of, the relevant electronic record;

(v) of the procedures for withdrawal of consent and to update information needed to contact the consumer electronically; and

(vi) of the procedures, after consent has been given, for obtaining a paper copy of the electronic record and any fee to be charged;

(c) the record is accessible to the consumer in a manner usable for subsequent reference.

PART II
LEGAL REQUIREMENTS RESPECTING ELECTRONIC COMMUNICATIONS AND RECORDS

Legal recognition of electronic communications.

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

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

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

Legal recognition of electronic records.

8. (1) Where any information or other matter is required by law to be given or rendered in writing or recorded in writing or in printed form or is described by law as being written, then, notwithstanding anything contained in that law, the requirement or description is satisfied if the information or matter is-

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

(b) accessible to, and is capable of retention by, the intended recipient so as to be usable or retrievable for a subsequent reference.

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

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

(4) In subsection (1), giving information includes, but is not limited to, the following-

(a) making an application;

(b) filing, making or lodging a claim;

(c) giving, sending or serving a notice;

(d) filing or lodging a return;

(e) making a request or requisition;

(f) making a declaration;

(g) filing, lodging or issuing a certificate;

(h) making, varying or cancelling an option;

(i) filing or lodging an objection or reply; or

(j) giving a statement of reasons.

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

Requirement to provide access to information in paper form.

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

(a) the form and means of access to the information reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, access to the information is required to be provided; and

(b) the person to whom access is required to be provided consents to accessing the information in that electronic form.

Furnishing of information in prescribed forms.

10. 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.

Delivery of information.

11. (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.

(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.

Information in original form.

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

(a) there exists a reliable assurance as to the integrity of the information from the time it was first generated in its final form as an electronic communication or electronic record; 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.

13. (1) Where any document, record or information is 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 document, record or 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 document, record or 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 any document, record or information in accordance with subsection (1) shall not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person if the conditions set out in subsection (1) are met.

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

Other requirements.

14. (1) An expression in a law, whether used as a noun or verb, including the terms “document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to an electronic record unless otherwise provided for in this Act.

(2) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that

requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(3) Where information or a signature, document or record is required by any law, or by contract or deed to be notarised, acknowledged, verified or made under oath, the requirement shall be satisfied if, in relation to electronic information, 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 information, electronic signature, electronic document or electronic record to be notorised, acknowledged, verified or made under oath.

Comparison of documents with original.

15. 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.

Admissibility and evidential weight of electronic communications.

16.(1) In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility of an electronic communication, or information or record in evidence solely on the ground that it is in electronic form.

(2) Information or record 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 given 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 sections 91 and 92 of the Evidence Act (which relate to the admissibility of computer-generated evidence).

Cap.5:03

PART III
ELECTRONIC CONTRACTS

Formation and validity of contracts.

17. (1) In the context of the formation of contracts, an offer and the acceptance of an offer or any other matter that is material in the operation or formation of a contract may be expressed by means of electronic communications.

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

Effectiveness between parties.

18. 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.

Invitation to make offer.

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.

Use of automated message systems for contract formation.

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

Error in electronic contract or transaction.

21. (1) An electronic contract concluded or an electronic transaction undertaken through the interaction of a person and an electronic agent of another person is void where –

(a) the first referred person made a material error in the information;

(b) the electronic agent of the second referred person did not provide an opportunity to prevent or correct the error;

(c) on becoming aware of the error, the first referred person notifies the second referred person of the error;

(d) the second referred person has taken no reasonable steps

to correct the error; and

(e) the first referred person has not received or used any material benefit or value from the second referred person.

(2) Subsection (1) shall not apply to electronic auctions.

(3) Where there is an agreement between the parties to use a security procedure to detect changes or errors in the electronic document and –

(a) only one of the parties has conformed to the procedure; and

(b) the non-conforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic document.

(4) The provisions of this section shall not be varied by agreement nor 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 (3).

Attribution.

22. (1) An electronic communication is that of the originator if it was sent by the originator himself.

(2) As between the originator and the addressee, an electronic communication is deemed to be that of the originator if it was sent –

(a) by a person who had the authority to act on behalf of the originator; or

(b) by an information system programmed by or on behalf of the originator to operate automatically.

(3) As between the originator and the addressee an addressee is entitled to regard an electronic communication as that of the originator and to act on that assumption if –

(a) the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the electronic communication resulted from the actions of a person whose relationship with the originator or an agent of the originator enabled that person to gain access to a method used by the originator to identify electronic communications as his own.

(4) Subsection (3) does not apply –

(a) where the addressee has received notice that the electronic communication is not that of the originator and the addressee has had reasonable time to act;

(b) in a case within subsection (3)(b), at a time when the addressee knew or should have known that the message was not that of the originator.

(5) The addressee is entitled to act on the assumption that the electronic communication as received is what the originator intended to send unless the addressee knew or should have known that there was an error in transmission.

(6) The addressee is entitled to regard each electronic communication as a separate message unless it duplicates another

message and the addressee knew or should have known.

Acknowledgment.

23. (1) Where the originator and addressee have not agreed on the form of acknowledgement, acknowledgement can be given by any communication or conduct of the addressee sufficient to indicate to the originator that the electronic communication has been received.

(2) Where the electronic communication is conditional on receipt of acknowledgement, the electronic communication is treated as never sent until acknowledgement is received.

(3) Where the electronic communication is not conditional on receipt of acknowledgement and the acknowledgement has not been received by the time specified or a reasonable time, the originator may give notice to the addressee specifying a reasonable time by which the acknowledgement must be received or may, upon notice to the addressee, treat the electronic communication as never sent.

(4) Where there is acknowledgement of receipt, it is presumed that the electronic communication was received, but it is not presumed that the electronic communication corresponds to the electronic communication received.

Time of dispatch of electronic communications.

24. Unless the originator and addressee otherwise agree, an electronic communication is dispatched –

(a) when it enters an information system outside the control of the originator or of the party who sent it on behalf of the originator; or

(b) in the case where the originator and the addressee are

in the same information system, when the electronic communication becomes capable of being retrieved and processed by the addressee.

Time of receipt.

25. (1) Unless the originator and addressee otherwise agree, 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.

(2) Unless the originator and addressee otherwise agree, 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.

(3) For the purposes of subsection (2), an electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the electronic address of the addressee.

Place of dispatch and receipt.

26. (1) 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.

(2) Section 25 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 (1).

PART IV
ELECTRONIC SIGNATURES

Requirement for signature.

27. 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 document or record if –

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

(b) the electronic signature used is either —

(i) as reliable as appropriate for the purpose for which the electronic document or 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.

28. 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 relying party.

29. (1) In this Part, "relying party" means a person who may act on the basis of a certificate or encrypted signature.

(2) A relying party shall bear the legal consequences of that party's failure-

(a) to take reasonable steps to verify the reliability of an encrypted signature;

(b) where an encrypted signature is supported by a certificate, to take reasonable steps to verify the validity and currency of the certificate and to observe any limitation with respect to the certificate.

Conduct of the signatory.

30. Where signature creation data or authentication data is used to create a signature or authenticate any electronic communication or record that has legal effect, each signatory shall-

(a) exercise reasonable care to avoid unauthorised use of his 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.

Conduct of electronic security procedures provider.

31. (1) An electronic security procedures provider who issues a certificate shall –

(a) act in accordance with representations made by it with respect to its policies and practices;

(b) exercise reasonable care to ensure, throughout the life cycle of the certificate, the accuracy and completeness of all material representations made by it in or in relation to the certificate;

(c) provide reasonably accessible means for enabling a relying party to ascertain from the certificate –

(i) the identity of the electronic security procedures provider;

(ii) that the signatory identified in the certificate had control of the encrypted signature creation device at the time when the certificate was issued; and

(iii) that the encrypted signature creation device was valid at the time when the certificate was issued;

(d) provide reasonably accessible means for enabling a relying party to ascertain from the certificate or otherwise –

(i) the method used to identify the signatory;

(ii) every limitation on the purpose or value for which the encrypted signature creation device

or the certificate may be used;

(iii) whether the encrypted signature creation device is valid and has not been comprised;

(iv) every limitation on the scope or extent of liability stipulated by the electronic security procedures provider;

(v) the facilities provided for the signatory to give notice pursuant to section 30(b);

(vi) the procedures in place to effect revocation;

(e) provide a means for a signatory to give notice pursuant to section 30(b);

(f) ensure the availability of a timely revocation service;

(g) utilize trustworthy systems, procedures and human resources in performing its services.

(2) For the purposes of this section, in determining whether any systems, procedures or human resources utilised by an electronic security procedures provider are trustworthy, regard may be had to –

(a) the financial and human resources, including the existence of assets and the quality of hardware and software systems of the provider;

(b) the provider's procedures for processing certificates and applications for certificates;

(c) the provider's retention of records and the availability of information to relying parties and to signatories identified in certificates;

(d) the regularity and extent of audits of the provider's operations by an independent body;

(e) any other relevant factor.

Recognition of foreign certificates and electronic signatures.

32. (1) In determining whether, or the extent to which, a certificate or an electronic signature is legally effective, no regard shall be had to the place where the certificate or the electronic signature was issued, nor to the jurisdiction in which the issuer had its place of business.

(2) Parties to commercial and other transactions may specify that a particular information security service provider or class of certificates shall be used in connection with electronic communications, information, records or signatures submitted to them.

(3) Where the parties to a transaction agree to the use of particular types of electronic signatures and certificates, that agreement shall be recognised as sufficient for the purpose of cross-border recognition in respect of that transaction.

PART V
SECURE ELECTRONIC COMMUNICATIONS, RECORDS AND SIGNATURES

Secure electronic communication or record.

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

(2) For the purposes of this section and section 34, 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.

34. (1) A signature shall be treated as a secure electronic signature if, through the application of a security procedure, or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that the electronic signature was, at the time it was made –

(a) unique to the person using it;

(b) capable of identifying the person using it;

(c) created in a manner or using a means under the sole control of the person using it; and

(d) linked to the electronic communication or record to which it relates in such a manner that if the communication or record was changed the electronic signature would be invalidated.

(2) Whether a security procedure is commercially reasonable shall be determined in accordance with section 33(2).

Presumptions relating to secure electronic communications, records and signatures.

35. (1) In any proceedings involving a secure electronic communication or record, it shall be presumed, unless evidence to the contrary is adduced, that the secure electronic communication or 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 communication or record.

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

PART VI
ELECTRONIC SECURITY PROCEDURES PROVIDERS

Designated Authority.

36. The Minister may by order designate an authority to be responsible for the regulation, registration, licensing or accreditation

of electronic security procedure providers.

Electronic security procedures and providers.

37. (1) The electronic security procedures include electronic certificates and any other procedure as maybe prescribed by the Minister by order.

(2) The Minister may by order list the electronic security procedures providers.

Regulation of security procedures and security procedure providers.

38. (1) The Minister may make regulations for the carrying out of this Part and, without prejudice to the general power, the Minister may make regulations for all or any of the following purposes –

(a) the regulation, registration, licensing or accreditation of electronic 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 communications and records, including the imposition of requirements to ensure interoperability between electronic 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 communications and records complies with Guyana's international obligations;

(d) prescribing the forms and fees applicable for the purposes of this Part.

(2) The Minister may, in making regulations under subsection (1)(a) for the regulation, registration, licensing or accreditation of electronic security procedure providers and their authorised representatives –

(a) prescribe the accounts to be kept by electronic security procedure providers;

(b) provide for the appointment and remuneration of an auditor;

(c) provide for the establishment and regulation of any information system by an electronic security procedure provider, whether by itself or in conjunction with other electronic security procedure providers, and for the imposition and variation of requirements or conditions relating to the system 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 electronic security procedure providers and for controls over its use;

(f) prescribe the duties and liabilities of electronic 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 electronic security procedure providers and their authorised representatives.

(3) Regulations made under this section may provide that a contravention of a specified provision of the Regulations shall be an offence and that the penalty for the commission of the offence may, notwithstanding anything in this Act, be a fine of one million dollars and imprisonment for five years.

PART VII
ELECTRONIC RECORDS, SIGNATURES AND ELECTRONIC SYSTEMS IN PUBLIC AUTHORITIES

Use of electronic records, information and signatures by public authorities.

39. (1) Where a public authority pursuant to a written law –

(a) accepts the filing of any form, application or any other document or obtains information in a particular manner;

(b) issues or grants any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) receives or pays money in a particular manner,

then, notwithstanding anything contained in any other law, the public authority may discharge the functions under this subsection by electronic means as may be specified by the Minister responsible for governance by order.

(2) The Minister responsible for electronic governance may, after consulting the Minister responsible for the public authority, for the purposes of subsection (1), specify by order –

(a) the manner and format in which the form, application and other documents in electronic form shall be filed, created, retained, issued or provided;

(b) the manner or method of payment of any fee or charges for filing, creating or issuing any electronic document and record under paragraph (a);

(c) the manner and format in which a signature shall be affixed to the form, application or other document in electronic form and the identity of the electronic security procedure provider used by the person filing the document;

(d) such control processes and procedures as may be appropriate to ensure adequate integrity, security and confidentiality of documents, records or information in electronic form; or

(e) any other required attributes for documents, records or information in electronic form that are currently specified for corresponding paper documents, records or information.

(3) Where a document, record or information in electronic form under subsection (2) is required to be signed, the Minister responsible for governance may, after consulting the Minister responsible for the public authority, specify by order the type of signature required, including, where applicable, the requirement that the sender use a particular type of encrypted electronic signature.

(4) For the avoidance of doubt, notwithstanding anything to the contrary in any written law but subject to any specification made under subsections (2) and (3), where any person is required by any written law to –

(a) file any document with or provide information in any

form to a public authority;

(b) create or retain any document for a public authority;

(c) use a prescribed form for an application or notification to, or other transaction with, a public authority;

(d) provide to or retain for a public authority any document, record or information in its original form; or

(e) hold a licence, permit or other approval from a public authority,

that requirement is satisfied by a document, record or information in electronic form specified for that purpose by the Minister responsible for governance.

(5) Notwithstanding anything contained in subsection (1), if the Minister is satisfied that due to technical failure or lack of facilities it is not practicable to give effect to subsection (1) in any office or in respect of any work or service, the Minister may, by order, specify the period during which subsection (1) shall not operate in the office or in respect of the work or service.

Establishment of electronic systems.

40. In the discharge of its functions under section 39, a public authority may where necessary, set up such electronic systems to facilitate the work of that authority.

PART VIII
INTERMEDIARIES AND ELECTRONIC-COMMERCE SERVICE PROVIDERS

Liability of intermediaries.

41. (1) An intermediary who provides a conduit shall not be subject

to any civil or criminal liability in respect of third-party information contained in an electronic communication for which such intermediary is only providing access and the intermediary-

(a) exercises reasonable care to ensure the accuracy of all representations;

(b) provides reasonably accessible means to enable a relying party to ascertain the identity of the electronic-commerce service provider and to ascertain the method used to identify the signatory;

(c) has no actual knowledge that the information gives rise to civil or criminal liability;

(d) 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

(e) follows the procedure set out in section 42, if the intermediary-

(i) acquires knowledge that the information gives rise to civil or 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 shall not be required to monitor any information contained in an electronic communication in respect of which the intermediary provides services in order to establish knowledge of, or to become aware of, facts or circumstances to determine whether or not the information gives rise to civil or

criminal liability.

(3) Nothing in this section shall relieve an intermediary from complying with any court order, injunction, writ, direction from the Government, regulatory requirement, or contractual obligation in respect of an electronic communication.

(4) For the purposes of this section-

(a) "provides access," in relation to a third-party information, means the provision of the necessary technical means by which third-party information may be accessed and includes the automatic and temporary storage of the third-party information for the purpose of providing access;

(b) "third-party information" means information of which the intermediary is not the originator.

Procedure for dealing with unlawful or defamatory information.

42. (1) If an intermediary has actual knowledge that the information in an electronic communication gives rise to civil or criminal liability, as soon as practicable, the intermediary shall-

(a) remove the information from any information processing system within the intermediary's control and cease to provide or offer to provide services in respect of that information; and

(b) notify the police of the relevant facts and of the identity of the person for whom the intermediary was supplying services in respect of the information if the identity of that person is known to the intermediary.

(2) If an intermediary is aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information in an electronic communication ought reasonably to have been known, as soon as practicable after becoming so aware the intermediary shall-

(a) follow the relevant procedure set out in any code of conduct that is applicable to such intermediary under section 43; or

(b) notify the police and the Minister.

(3) Upon being notified in respect of any information under subsection (2), the Minister may direct the intermediary to –

(a) remove the electronic communication from any information processing system within the control of the intermediary; and

(b) cease to provide services to the person to whom the intermediary was supplying services in respect of that electronic communication.

(4) An intermediary shall not be liable, whether in contract, tort, under any written law or pursuant to any other right, to any person including any person on whose behalf the intermediary provides services in respect of the information in an electronic communication, for any action the intermediary takes in good faith in exercise of the powers conferred by, or as directed by the Minister under, this section.

Codes of conduct and standards for intermediaries and

43. (1) The Minister may develop codes of conduct or standards for intermediaries and electronic-commerce service providers for the

e-commerce service providers.

purposes of this Act, which the Minister shall by notice publish in the *Gazette*.

(2) Where the Minister has developed a code of conduct or standards for intermediaries and electronic-commerce service providers, the intermediaries and electronic-commerce service providers shall comply with the code of conduct or service standards.

(3) An intermediary or electronic-commerce service provider who fails to comply with a code of conduct or standards, shall in the first instance be given a written warning by the Minister and the Minister may, in writing, direct that intermediary or electronic-commerce service provider to cease and desist or otherwise to correct his practices, and, if that person fails to do so within such period as may be specified in the direction, the intermediary or electronic-commerce service provider, as the case may be, commits an offence and shall be liable on summary conviction to a fine of one hundred thousand dollars and if the offence is a continuing one to a further fine of five thousand dollars for each day the offence continues.

(4) Compliance with relevant codes of conduct and service standards may be taken into account by the courts in determining liability.

PART IX
CONSUMER PROTECION

Consumer protection.

44.(1) An electronic-commerce service provider who by use of electronic transactions sells or hires any goods, services or facilities to consumers shall provide accurate, clear and accessible information about themselves, sufficient to allow-

(a) the legal name of the provider, his principal geographic address, and an electronic means of contact or telephone number;

(b) prompt, easy and effective consumer communication with the seller; and

(c) service of legal process.

(2) An electronic-commerce service provider who by use of electronic transactions sells or hires any goods, services or facilities to consumers shall provide accurate and accessible information describing the goods or services offered, sufficient to enable consumers to make an informed decision about the proposed transaction and to maintain an adequate record of the information.

(3) An electronic-commerce service provider who by use of electronic transactions sells or hires any goods, services or facilities to consumers shall, before the conclusion of the electronic contract based on such transaction, provide information to consumers in respect of the electronic contract, about the terms, conditions and costs associated with a transaction, and notably-

(a) terms, conditions and methods of payment; and

(b) details of and conditions and policies related to privacy,

withdrawal, termination, return, exchange, cancellation and refund policy information;

(c) the arrangements for delivery or performance; and

(d) a copy of the contract for the consumer in a format that can be retained.

(4) The Minister may make regulations relating to the sale of goods or services by an electronic-commerce service provider using electronic transactions.

Right of rescission.

45. A consumer who is not provided with the information required by section 44 has the right to rescind the contract within thirty calendar days provided that the consumer has not received any material benefit from the transaction.

Unwanted communications.

46. (1) Any person who sends unsolicited commercial communications through electronic media to consumers based in Guyana or knowingly uses an intermediary to send, or who has a place of business in Guyana and sends, unsolicited electronic correspondence to consumers shall provide the consumer with a clearly specified and easily activated option to opt out of receiving future communications.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of one hundred thousand dollars.

PART X
MISCELLANEOUS

Audit of documents, etc.

47. Where in any law there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained as electronic records or in the electronic form.

Regulations.

48.(1) The Minister may make regulations for carrying out the provisions of this Act.

(2) In particular and without prejudice to the generality of subsection (1), and subject to Part VII, the regulations may provide for all or any of the following matters –

(a) the methods which may satisfy the requirements of electronic signatures;

(b) the factors to which regard shall be had in determining whether and to what extent systems, procedures and human resources are trustworthy for the purposes of the electronic security procedures providers;

(c) the manner and the format in which electronic records shall be filed, created or issued;

(d) the manner or method of payment of any fee or charges for filing, creating or issuing any electronic record;

(e) the security practices and procedures to be in consultation with such professional bodies or associations as the Minister deems fit;

(f) the information which may be preserved and retained by an intermediary and the period, manner and format

in which such information may be retained;

(g) the procedure and safeguards subject to which blocking of any information generated, transmitted, received, stored or hosted in any electronic communication system may be ordered;

(h) for the purpose of authorizing, prohibiting or regulating the use of the ".gy" domain name or any successor domain name for Guyana;

(i) prescribing for the purposes of the registration of the ".gy" domain name or any successor domain name for Guyana –

(i) designated registration authorities;

(ii) the form and manner of registration; the period when registration stays in force and the terms and conditions for registration;

(iii) the manner, terms and conditions and the period for renewal of registration;

(iv) the circumstances and the manner in which registration may be granted, renewed or refused by the registration authorities;

(v) the appeal process and procedure;

(vi) the fees to be paid on the grant or renewal of registration and the time and manner the fees are to be paid; and

(vii) such other matters relating to the registration of domain names.

(3) Regulations made under this section may provide that a contravention of a specified provision of the Regulations shall be an

offence and that the penalty for the commission of the offence may, notwithstanding anything in this Act, be a fine of one million dollars and imprisonment for five years.

Act to have overriding effect.

49. (1) The provisions of this Act shall have effect notwithstanding anything inconsistent with it contained in any other law for the time being in force.

(2) An expression in a law, whether used as a noun or verb, including the terms “document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to an electronic record unless otherwise provided for in this Act.

Removal of difficulties.

50. If any difficulty arises in giving effect to the provisions of this Act, the Minister may, by order, make such provision not inconsistent with the provisions of this Act as appear to be necessary or expedient for removing the difficulty.

SCHEDULE s. 4

DOCUMENTS AND TRANSACTIONS

1. Creation or transfer of interest in real or immovable property.

2. Negotiable instruments.

3. Documents of title.

4. Wills and other testamentary instruments.

5. Trusts.

6. Court orders or notices or official court documents required to be executed in connection with court proceedings.

7. Power of attorney.

1st April 2018

EXPLANATORY MEMORANDUM

Consumers and the business community, including banks and commercial organisations are increasingly using computer and other related technologies to create, transmit and store information in electronic form instead of on traditional paper documents. Information stored in electronic form has many advantages as it is cheaper, easier to store and retrieve and speedier to communicate. Even though the general public is aware of all these advantages, many members are reluctant to conduct business or conclude any transaction in electronic form due to lack of an appropriate legal framework.

Government is currently unable to fully implement e-Government services due to inadequate legal framework and protection as well as some existing conflicting provisions in various laws. This lack of legal framework and uncertainty is inhibiting the development of electronic-commerce and e-Government activity in Guyana and fostering the adherence to traditional business and transaction models.

Nevertheless, international trade through the medium of electronic-commerce has grown rapidly in the past few years and many countries have switched over from traditional paper-based commerce to e-commerce.

A hurdle which stands in the way of facilitating electronic commerce and electronic governance relate to the requirement of the signature for legal recognition. At present, many legal provisions assume the existence of paper-based records and documents and records that should bear signatures.

The Bill enables the conclusion of contracts and creation of certain rights and obligations through the electronic medium.

With a view to facilitating electronic governance by government offices and agencies it is proposed to provide for the use and acceptance of electronic records and electronic signatures in government offices and agencies with suitable safeguard mechanisms.

Part I of the Bill comprises the preliminary clauses.

Clause 1 contains the short title.

Clause 2 defines certain words and expressions.

Clause 3 provides that the Act binds the State. However, the Act does not make it obligatory on the part of public authorities to process records by electronic means.

Clause 4 provides that the Act does not apply to the documents and transactions set out in the Schedule. These include the making of wills, the conveyance or transfer of any interest in real or immovable property. However, it also empowers the Minister to amend the Schedule.

Clause 5 provides for the autonomy of the parties to use or accept electronic communications, electronic signatures and electronic contracts in certain circumstances.

Clause 6 makes provisions for the circumstances requiring consent of consumers in electronic communications.

Part II of the Bill deals with the requirements for the legal recognition of electronic communications and records.

Clause 7 provides for the legal recognition of electronic communications. An electronic communication is not to be denied legal effect, validity, admissibility or enforceability solely on the ground that it is rendered or made available in electronic form.

Clause 8 provides for the legal recognition to electronic records. A legal requirement of giving, recording or rendering any information or other matter in writing or in printed form shall be met if the same is given, recorded or rendered in electronic form.

Clause 9 provides that a legal requirement to provide access to any information in paper form is met if it is given in electronic form that maintains integrity and accessibility.

Clause 10 provides that the legal requirement of furnishing information in paper or other non-electronic form is met if it is furnished in electronic form which contains the same or in substantially the same information and which could be accessible to the other person so as to enable that person to retrieve or retain it for subsequent reference.

Clause 11 provides that where any information is required by law to be delivered, dispatched, given, sent to or served on any person that requirement is met if it is delivered, dispatched, given, sent to or served on that person by electronic record and the originator of the electronic record states that the receipt of the electronic record is to be acknowledged and the addressee acknowledges the receipt.

Clause 12 deals with presentation or retention of information in original form. It provides that a legal requirement of presenting or retaining any information in its original form is met by presenting or retaining it by an electronic communication if there is reliability of accuracy of presentation and in its integrity in final electronic form.

Clause 13 provides for retention of documents, records or information in electronic form where a legal requirement to retain them in paper or other non-electronic form is

required. A legal requirement to retain any document, record or information in paper or other non-electronic form is met if the same is retained in electronic form subject to fulfilling certain conditions such as accessibility, accuracy, format, date and time of origin and destination of the electronic communication. This clause also allows public authorities to specify additional requirements in respect of electronic communications coming within their purview.

Clause 14 makes several provisions to allow for electronic commerce and e-government and is self-explanatory.

Clause 15 provides that a legal requirement for comparison of a document with its original will be satisfied if it is compared with the electronic form which assures the maintenance of integrity of the document.

Clause 16 provides for the admissibility of electronic communications in evidence.

Part III of the Bill provides for the formation and validity of electronic contracts.

Clause 17 provides for formation of electronic contracts and the mere fact that the contract is formed electronically does not affect its enforceability.

Clause 18 provides for the effectiveness of declaration of intent relating to electronic contracts.

Clause 19 provide for an invitation to conclude a contract made through electronic communications which is accessible to all parties making use of information systems is to be considered as an invitation to make offers.

Clause 20 allows the use of automated message systems for formation of contracts.

Clause 21 provides that certain errors made in partly automated transactions or contracts involving material errors may render the contract voidable.

Clause 22 provides for attribution. An electronic communication is that of the originator if it was sent by the originator himself and deemed to be that of the originator if it was sent by a person who had the authority to act on behalf of the originator or by an information system programmed by or on behalf of the originator to operate automatically.

Clause 23 provides for acknowledgement. Where the originator and addressee have not agreed on the form of acknowledgement, acknowledgement can be given by any communication or conduct of the addressee sufficient to indicate to the originator that the electronic communication has been received.

Clauses 24, 25 and 26 define the time and place of dispatch and receipt of electronic communications.

Part IV of the Bill provides for the use of electronic signatures.

Clause 27 provides for legal recognition of electronic signatures in electronic communications and transactions.

Clause 28 provides that parties to an electronic transaction may agree to the use of a particular method or form of electronic signature.

Clauses 29, 30 and 31 provides the requirements for conduct of the relying party, the signatory and electronic security procedures provider.

Clause 32 provides for the recognition of foreign certificates and electronic signatures.

Part V provides for secure electronic communications, records and signatures and deals with presumptions relating to secure electronic communications, records and signatures.

Clause 33 provides that if a security procedure, or a commercially reasonable security procedure agreed to by the parties involved, has been properly applied to an electronic communication or record to verify that the electronic communication or record has not been altered since a specific point in time, that communication or record shall be treated as a secure electronic record from that specific point in time to the time of verification.

Clause 34 provides that a signature shall be treated as a secure electronic signature if, through the application of a security procedure, or a commercially reasonable security procedure agreed to by the parties involved, if it can be verified, for instance, that the signature was unique to the person using it.

Part VI of the Bill deals with electronic security procedures providers.

Clauses 36 provides for the Minister to designate an authority to be responsible for the regulation, registration, licensing or accreditation of electronic security procedure providers.

Clause 37 provides that the electronic security procedures include electronic certificates and for the Minister to prescribe other procedures. The Minister may by order list the electronic security procedures providers.

Clause 38 gives the Minister power to issue regulations to safeguard or maintain the effectiveness and efficiency of information security procedure services.

Part VII of the Bill facilitates effective delivery of e-Government services. This Bill

supports e-Government efforts by enabling the use of electronic documents and transactions in citizens' and businesses' interactions with Government and its agencies.

Clause 39 of the Bill provides for information to be submitted using electronic forms in the manner specified by the authorities, even if these forms do not resemble the physical prescribed forms required for the transactions. The amendments are proposed to provide flexibility for public authorities to design electronic forms suited for online transactions, and hence improve the customer's overall e-governance experience.

Part VIII of the Bill sets out the duties and limits of liabilities of intermediaries and e-commerce service providers.

Clause 41 provides for limit of liability of intermediaries.

Clause 42 provides for the procedure for dealing with unlawful or defamatory information exchanged by intermediaries.

Clause 43 provides for approval of codes of conduct and specifying of standards required to be complied with by intermediaries and electronic-commerce service providers. It also provides for the penalties for non-compliance with approved codes of conduct or specified standards by an intermediary or an electronic-commerce service provider.

Part IX of the Bill contains consumer protection provisions for the conduct of online sale of goods and services as well as protection against "spam".

Part X of the Bill contains miscellaneous provisions.

Clause 47 provides for audit of documents, records or information processed and maintained as electronic records or in the electronic form.

Clause 48 empowers the Minister to make regulations for carrying out the provisions of the Act.

Clause 49 provides for the Act to have overriding effect.

Clause 50 empowers the Minister to remove any difficulty in giving effect to the proposed legislation by making order not inconsistent with the provisions of the Act.

The Schedule enumerates the documents and transactions to which the provisions of the Act will not apply.

……

HON. DOMINIC GASKIN, M.P.

MINISTER OF BUSINESS