# The Official Gazette

## (EXTRAORDINARY)

## OF GUYANA

Published by the Authority of the Government

**GEORGETOWN, WEDNESDAY 16TH AUGUST, 2023**


**TABLE OF CONTENTS** **PAGE**

**FIRST SUPPLEMENT**

**LEGAL SUPPLEMENT**


**A.** **ACTS —** Act No. 12 of 2023 – The Electronic Communications and Transactions Act 2023 .... .... .... .... .... 215

**B.** **SUBSIDIARY LEGISLATION — NIL**

**C.** **BILLS — NIL**



GEORGETOWN, Demerara – Printed and Published every Saturday and on such Extraordinary Days as may be directed by the Government by Guyana National Printers Limited, 1 Public Road, La Penitence, Greater Georgetown.

THE OFFICIAL GAZETTE 16TH AUGUST, 2023
LEGAL SUPPLEMENT — A

GUYANA

ACT NO. 12 OF 2023

# ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 2023

I assent.

Mohamed Irfaan Ali,

President.

16th August, 2023

## ARRANGEMENT OF SECTIONS

**Section**

PART I

PRELIMINARY

1. Short title.
2. Interpretation.
3. Act binds the State.
4. Non-application of Act.
5. Autonomy of parties.
6. A person's consent to electronic record.

PART II

LEGAL REQUIREMENTS

RESPECTING ELECTRONIC COMMUNICATIONS, TRANSACTIONS AND RECORDS

7. Legal recognition of electronic communications and transactions.
8. Legal recognition of electronic records.
9. Requirement to provide access to information in paper form.
10. Furnishing of information in prescribed forms.
11. Delivery of information.
12. Information in original form.
13. Retention of documents, records or information in electronic form.
14. Legal recognition of receipt, payment or transfer of money by electronic form or means.
15. Other requirements for legal recognition.
16. Comparison of documents with original.
17. Audit of documents or records maintained as electronic records.
18. Admissibility and evidential weight of electronic communications.

PART III

ELECTRONIC CONTRACTS

19. Formation and validity of contracts.
20. Effectiveness between parties.
21. Invitation to make offer.
22. Use of automated message systems for contract formation.
23. Error in electronic contract or transaction.
24. Attribution.
25. Acknowledgment.
26. Time of dispatch of electronic communications.
27. Time of receipt.
28. Place of dispatch and receipt.

PART IV

ELECTRONIC SIGNATURES

29. Requirement for signature in relation to an electronic document or record.
30. Equal treatment of signatures.

PART V

SECURE ELECTRONIC SIGNATURES,

COMMUNICATIONS AND RECORDS

31. Secure electronic signature and requirements for reliability and integrity.

32. Secure electronic communication or record.

33. Presumptions relating to secure electronic signatures, communications and records.

34. Electronic signature associated with an accredited electronic security procedure.

PART VI

CERTIFYING AUTHORITY AND

ELECTRONIC SECURITY PROCEDURES PROVIDERS

35. Certifying Authority.

36. Functions of the Certifying Authority.

37. Electronic security procedures.

38. Registration of Electronic Security Procedures Providers.

39. Application for registration.

40. Requirements for an Electronic Security Procedures Provider that issues qualified procedures.

41. Grant of registration.

42. Recognition of qualified external electronic security procedures.

43. Registry of electronic security procedures and providers.

44. Annual updated notification of compliance and fee.

45. Audit by the Certifying Authority.

46. Responsibility to cooperate with an audit.

47. Confidentiality.

48. Power to the Certifying Authority to deal with failure to meet requirements.

49. Pseudonyms.

50. Additional responsibilities of an Electronic Security Procedures Provider.

51. Minimum information regarding electronic security procedures.

52. Immediate revocation upon request.

53. Liability of the Electronic Security Procedures Provider issuing a qualified procedure.

54. Release from liability.

55. Costs of audit.

PART VII

PUBLIC AUTHORITIES USE OF ELECTRONIC RECORDS, INFORMATION, SIGNATURES AND SYSTEMS

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

57. Collaboration with other public authorities and private entities.

PART VIII

INTERMEDIARIES AND ELECTRONIC-COMMERCE SERVICE PROVIDERS

58. Liability of intermediaries.

59. Procedure for dealing with unlawful or defamatory information.

60. Codes of conduct and standards for intermediaries and e-commerce service providers.

PART IX

OFFENCES IN RELATION TO RECEIPT, PAYMENT AND TRANSFER OF MONEY

61. False statement to procure a card.

62. Theft by taking or retaining possession of card.

63. Card theft.

64. Dealing in card of another.

65. Purchase or sale of card of another.

66. Obtaining control of card as security.

67. Forgery.

68. Signing a card of another.

69. Fraudulent use of card.

70. Fraud by person authorised to provide goods, services, etc.

71. Receipt of money, etc., obtained by fraudulent use of card.

72. General Offence for fraudulent electronic fund transfer.

73. Alteration of card invoice.

74. Card lists prohibited.

75. Obtaining goods, etc., by use of false, expired, or revoked card.

76. Trafficking in counterfeit card.

77. Possession of card-making equipment.

78. Defences not available.

79. Liability for misuse of card.

80. Territorial scope of offences under this Part.

PART X

MISCELLANEOUS

81. Liabilities of directors and officers.

82. General penalty.

83. Jurisdiction of the Courts.

84. Regulations.

SCHEDULE

**AN ACT** to provide for the facilitation and regulation of secure electronic communications, transactions and receipt, payment and transfer of money 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. 2023 Enacted by the Parliament of Guyana:-

## PART I

## PRELIMINARY

Short title.

1. This Act may be cited as the Electronic Communications and Transactions Act 2023.

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;

"authorised manufacturer" means a financial institution or any other person who is authorised under any written law to produce a card;

"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;

"bank card" means any instrument, token, device, or card, whether known as a bank service card, banking card, check guarantee card, credit card, debit card or token or by any other similar name, issued by an issuer for the use of the cardholder in obtaining goods, services, or anything else of value or for use in an

automated banking device or online to obtain money or any of the services offered through the device or online;

"card" means a bank card, smart card, electronic wallet, token or device or the number or data associated with a bank card, smart card, electronic wallet, token or device;

"cardholder" means the person named on the face of a card to whom or for whose benefit such a card is issued by an issuer;

"card-making equipment" means any equipment, machine, plate, mechanism, impression, or any other device designed, used, or capable of being used to produce a card, a counterfeit card, or any aspect or component of a card;

"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, contains a public key that corresponds to a private key under the control of the originator of the electronic document to which the certificate relates, and includes other information such as its operational period;

"Certifying Authority" means the Certifying Authority to be designated by the Minister under section 35;

"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 for the supply of the goods, services or anything else of value offered by the provider;

"counterfeit card" means a card which is fictitious, altered or forged and includes any facsimile or false representation, depiction, or component of such a card, or any such card which is stolen, obtained as part of a scheme to defraud, or otherwise unlawfully

obtained, and which may or may not be embossed with account information or an issuer's information;

"Court" means the High Court of Guyana;

"credit" includes a cash loan or any other financial accommodation;

"credit card" means any instrument, token, device or card, whether known as a charge card or by any other similar name, issued by an issuer for the use of the cardholder in obtaining goods, services, or anything else of value on credit from a creditor or for use in an automated banking device to obtain money or any of the services offered through the device;

"creditor" means a person who agrees or is authorised by an issuer to supply goods, services or anything else of value and to accept payment by use of a bank card, credit card, or smart card for the supply of such goods, services or anything else of value to the cardholder, and includes an electronic-commerce service provider and an intermediary;

"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;

"debit card" means a card or other instrument, by which money is automatically deducted from an account at a deposit-taking institution to pay for goods, services or any thing else of value purchased;

"digital signature" means 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 intermediary service provider" means the

intermediary service provider that enables placing orders or executing agreements pertaining to provision of electronic commerce service providers' goods, services or anything else of value in the electronic commerce marketplace."

"electronic-commerce service provider" means a person who uses electronic means in executing agreements or receiving orders on its goods, services and anything else of value in the electronic commerce market place or in its own electronic commerce medium;

"electronic commerce marketplace" means the electronic commerce medium of which the electronic commerce intermediary service provider provides its intermediary services including platforms such as website, mobile site or mobile application where electronic commerce activities are carried out;

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

"electronic form" with reference to –

(a) information, means any information generated, sent, received or stored in media, magnetic form, optical form, computer memory, microfilm, computer generated microfiche or similar device; and

(b) money, includes electronic money;

"electronic fund transfer" means any transfer of money that is initiated through an electronic terminal, telephone, computer, magnetic tape, the Internet, or through online services for the purpose of ordering, instructing, or authorising a financial institution to debit or credit an account;

"electronic means" with reference to money, includes a card;

No. 13 of 2018

"electronic money" has the same meaning assigned to it as in the National Payment Systems Act 2018;

"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 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, and includes a certificate;

"Electronic Security Procedure Provider" means a person registered as an accredited Electronic Security Procedure Provider under section 38 to provide qualified electronic security procedures and related services;

"electronic signature" means the various ways that an electronic document or record can be signed, such as a digitised 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 transaction" includes the single communication or outcome of multiple communications involved in the conduct of business, consumer or commercial affairs, including the sale of goods, services or anything else of value conducted over computer-mediated networks or information systems, where the goods or services or anything else of value may be ordered through such networks or systems but the payment or ultimate delivery of the goods, services or anything else of value may occur without the use of such networks or systems;

"electronic wallet" means an encrypted storage medium holding financial information that can be used to complete electronic

transactions without re-entering the stored data at the time of the transaction;

Cap. 85:03 "financial institution" means a company as defined under section 2 of the Financial Institutions Act or a foreign financial institution authorised under the law of its jurisdiction to issue cards;

"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 –

(a) 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; and

(b) the provision of goods, services and anything else of value, means includes an electronic commerce intermediary service provider;

"issuer" includes a financial institution which issues a card or any other person duly authorised to issue a card;

"Minister" means the Minster with responsibility for commerce except, as provided in Part VII;

"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 a Minister who has responsibility for the entity or body for a public service purpose;

"receives" with reference to a card, means acquiring possession, title or control or accepting a card as security for credit;

"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;

"revoked card" means a card which is no longer valid because permission to use it has been suspended or terminated by the issuer, whether on its own or on the request of the cardholder;

"secure electronic communication or record" means an electronic record that is treated as a secure electronic record by virtue of section 32(1);

"secure electronic signature" means an electronic signature that is treated as a secure electronic signature by virtue of section 31;

"signatory" means a person who may or may not hold a signature-creation device and acts either on that person's 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;

"smart card" means any instrument, token, device, or card, or whether known by any other similar name, and encoded with a stated money value and issued by an issuer for use of the cardholder in obtaining goods, services, or anything else of value, except money; and

"traffic" means to sell, transfer, distribute, dispense or otherwise dispose of property, or to buy, receive, possess, obtain control of, or use property with the intent to sell, transfer, distribute, dispense, or otherwise dispose of such property.

(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, services or anything else of value 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. This Act binds the State.

Non-application of Act.

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

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.

A person's consent to electronic record.

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

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

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

(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 person 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 person in a manner usable for subsequent reference.

## PART II

## LEGAL REQUIREMENTS RESPECTING

## ELECTRONIC COMMUNICATIONS, TRANSACTIONS AND RECORDS

Legal recognition of electronic communications and transactions.

7. An electronic communication or transaction 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 or transaction purporting to give rise to legal effect but is referred to in that electronic communication or transaction.

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 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 form of that information need not be retained.

(6) A person who gives information under this section that contains false or misleading information commits an offence and is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

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, by the electronic security measures or procedures employed, 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 in the record that the receipt of the electronic record must be acknowledged and the addressee has acknowledged its receipt by so stating in any communication.

(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, through the use of electronic security measures or procedures, 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, through the use of electronic security measures or procedures, 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 an intermediary 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.

Legal recognition of receipt, payment or transfer of money by electronic form or means.

14. (1) Where any law provides for the receipt, payment or transfer of money in a particular form or manner, then, notwithstanding anything contained in any other law that requirement is met if such receipt, payment or transfer is effected by electronic form, including electronic money, or electronic means, including a card.

(2) Offences and penalties in relation to the receipt, payment and transfer of money by electronic form and means are provided in Part IX.

Other requirements for legal recognition.

15. (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, shall be interpreted so as to include or permit such form, format or action in relation to an electronic record unless otherwise provided for in this Act.

(2) Where a seal is required by law to be affixed to a document and the law does not prescribe the method or form by which the document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the secure electronic signature of the person by whom it is required to be sealed.

(3) Where information or a signature, document or record is required by any law, or by contract or deed to be notarised, acknowledged, verified or made under oath, the requirement is 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 associated with the electronic information, electronic signature, electronic document or electronic record to be notarised, acknowledged, verified or made under oath.

Comparison of documents with original.

16. 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 assures, by the use of electronic security measures or procedures, the maintenance of the integrity of the document.

Audit of documents or records maintained as electronic records.

17. 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.

Admissibility and evidential weight of electronic communications.

18. (1) In any legal proceedings, nothing in the rules of evidence shall apply so as to deny the admissibility of an electronic communication, 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.

19. (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.

20. 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.

21. 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.

22. 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.

23. (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 –

(i) has not received or used any material benefit or value from the second referred person; or

(ii) in a case where consideration is received as a result of the error, returns or disposes of the consideration in accordance with the second referred person's instructions or in the absence of such instructions takes reasonable steps to return or dispose of the consideration, and does not benefit materially by receiving the consideration.

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

(3) Where there is an agreement between the parties to use an electronic 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.

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

(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 an electronic security 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 or an electronic security procedure used by the originator to identify electronic communications as being those of the originator.

(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.

25. (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.

26. 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.

27. (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.

28. (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 27 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 in relation to an electronic document or record.

29. 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.

30. 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 electronic security procedure.

## PART V

## SECURE ELECTRONIC

## SIGNATURES, COMMUNICATIONS AND RECORDS

Secure electronic signature and requirements for

31. (1) A signature shall be treated as a secure electronic signature if, through the application of an electronic security procedure, or a commercially

reliability and integrity.

reasonable electronic security procedure agreed to by the parties involved, it is shown that the electronic signature satisfies the following requirements for reliability and integrity –

(a) it is unique to the person using it;

(b) it is capable of identifying the person using it;

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

(d) it is 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; and

(e) any other requirement prescribed by the Minister by regulations.

(2) Whether an electronic security procedure is commercially reasonable shall be determined in accordance with section 32(2).

Secure electronic communication or record.

32. (1) If an electronic security procedure, or a commercially reasonable electronic 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 31, whether an electronic security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including the –

(a) nature of the transaction;

(b) experience and knowledge of the parties;

(c) volume of similar transactions engaged in by either or all parties;

(d) availability of alternatives offered to but rejected by any party;

(e) cost of alternative procedures; and

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

Presumptions relating to secure electronic signatures, communications and records.

33. (1) 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.

(2) 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.

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

Electronic signature associated with an accredited electronic security procedure.

34. An electronic signature that is associated with a qualified electronic security procedure issued by an Electronic Security Procedure Provider accredited under Part VI is deemed to satisfy the requirements set out in section 31 for reliability and integrity.

## PART VI

## CERTIFYING AUTHORITY AND

## ELECTRONIC SECURITY PROCEDURES PROVIDERS

Certifying Authority.

35. The Minister shall by Order designate or establish an authority to be the Certifying Authority which shall be responsible for the regulation, registration and accreditation of Electronic Security Procedure Providers.

Functions of the Certifying Authority.

36. (1) The functions of the Certifying Authority shall be to –

(a) regulate, register, and accredit Electronic Security Procedures

Providers;

(b) issue and regulate the use of certificates and any other electronic security procedures including private and public key pairs;

(c) authorise and regulate the issue of certificates, any other electronic security procedure and provision of related services by Electronic Security Procedures Providers;

(d) authenticate certificates and any other electronic security procedures issued by any local or overseas Electronic Security Procedures Providers;

(e) provide time stamping services in relation to electronic documents;

(f) provide application programming interface, including data encryption, encrypted signatures and digital envelopes; and

(g) carry out any other functions assigned to it by the Minister by Order.

(2) The Certifying Authority, in the discharge of its functions, may –

(a) carry out such investigations as may be necessary;

(b) cooperate with any overseas certifying authority in establishing a system of mutual accreditation; or

(c) issue, from time to time, practice statements on any electronic security procedure or related service.

Electronic security procedures.

37. The electronic security procedures include electronic certificates, and any other security procedure as may be prescribed by the Minister by Order.

Registration of Electronic Security Procedures Providers.

38. No person shall issue a qualified electronic security procedure and provide related services to the public unless he is registered as an accredited Electronic Security Procedure Provider by the Certifying Authority and has provided the information prescribed under this Act.

Application for registration.

39. (1) A person wishing to be registered as an accredited Electronic Security Procedure Provider (the applicant) shall apply to the Certifying Authority in the manner prescribed and pay the prescribed fee.

(2) The application under subsection (1) shall include at a minimum the following information –

(a) the name and business address of the person; and

(b) proof of accreditation of the operations of the person.

(3) Where an applicant has valid prior accreditation from another recognised jurisdiction, proof of accreditation shall be information relating to –

(a) the name and address of the accreditation authority;

(b) the period of validity of the accreditation; and

(c) any other information required by regulations as may be prescribed.

(4) Where an applicant has no valid prior accreditation, the applicant shall indicate same to the Certifying Authority who shall require the applicant to submit to an audit of the applicant's operations and systems to ensure compliance with the requirements of section 40 and any other standards which the Minister may prescribe by regulations.

(5) Where the Certifying Authority is satisfied that the applicant has met the requirements of this Act the Certifying Authority may issue a notice of accreditation to the applicant.

(6) The Minister may make regulations prescribing the procedures for registration and accreditation.

Requirements for an Electronic Security Procedures Provider that issues qualified procedures.

40. (1) An Electronic Security Procedure Provider that issues qualified electronic security procedures and provide related services to the public shall conduct operations of that Provider in a reliable manner and shall –

(a) employ personnel who possess the expert knowledge and experience required for these operations, especially with

regard to management, technology, electronic authentication and security procedures;

(b) apply such administrative and management routines that conform to recognised standards;

(c) use trustworthy systems and procedures that are protected against modification and that ensure technical and cryptographic security;

(d) maintain sufficient financial resources to conduct operations in accordance with these requirements and any other provisions set out in the Act and bear the risk of liability for damages;

(e) have secure routines to verify the identity of those signatories to whom qualified electronic security procedures are issued;

(f) maintain a prompt and secure system for registration and immediate revocation of a qualified electronic security procedure;

(g) take measures against forgery of a qualified electronic security procedure and, where applicable, guarantee full confidentiality during the process of generating signature creation data;

(h) comply with section 51; and

(i) comply with any other requirements prescribed by the Minister.

(2) A person who provides a consumer or a user of an electronic authentication product with false or misleading information commits an offence and is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

Grant of registration.

41. (1) Where the Certifying Authority is satisfied that an applicant has valid prior accreditation and has met the requirements of section 39, the Certifying Authority may grant the registration.

(2) Where the Certifying Authority is satisfied that an applicant who has no valid prior accreditation has met the requirements of sections 39 and

40, the Certifying Authority may issue a notice of accreditation to that applicant, and grant the registration.

Recognition of qualified external electronic security procedures and providers.

42. The Minister may by Order recognise a qualified electronic security procedure or classes of qualified electronic security procedures issued by Electronic Security Procedures Providers or classes of Electronic Security Procedures Providers established in any other jurisdiction, as qualified electronic security procedures in Guyana, that may be used in connection with electronic communications, information, records or signatures.

(2) Parties to commercial and other transactions may specify that a particular Electronic Security Procedure Provider, including a Provider from another jurisdiction, or class of electronic security procedures 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 electronic security procedures, that agreement shall be recognised as sufficient for the purpose of cross-border recognition in respect of that transaction.

Registry of electronic security procedures and providers.

43. The Certifying Authority shall maintain a public registry of accredited Electronic Security Procedures Providers that includes identification particulars of, and the security procedures and services provided by the Providers.

Annual updated notification of compliance and fee.

44. A registered Electronic Security Procedures Provider that issues qualified electronic security procedure shall annually provide the Certifying Authority with an updated notification of compliance with the requirements of section 40 and pay the prescribed fee.

Audit by the Certifying Authority.

45. (1) The Certifying Authority may conduct an audit to verify that the Electronic Security Procedures Provider has been or remains in compliance with the requirements of this Act.

(2) In the performance of an audit, the Certifying Authority may employ whatever experts it considers may be required.

(3) A person commits an offence where the person –

(a) knowingly makes any false or misleading statement, either orally or in writing to persons carrying out the audit; or

(b) otherwise obstructs or hinders the persons carrying out the audit in the conduct of their duties and functions.

(4) A person who commits an offence under this section is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

Responsibility to cooperate with an audit.

46. An Electronic Security Procedures Provider shall cooperate with and offer all reasonable assistance to the Certifying Authority while conducting an audit and shall make available information necessary to satisfy the Certifying Authority regarding compliance with the requirements of this Act.

Confidentiality.

47. (1) Notwithstanding any law to the contrary, no person who performs or has performed duties or functions in the administration or enforcement of this Act, including performing an audit pursuant to section 45, shall communicate or allow to be communicated information obtained in the course of performance of duties or functions under the Act to any other person except –

(a) to law enforcement authorities on the basis of a warrant; or

(b) by Order of the Court.

(2) A person who breaches the confidentiality obligations established under this section commits an offence and is liable on conviction of summary conviction to a fine of one million dollars and to imprisonment for three years.

Power to the Certifying Authority to deal with failure to meet requirements.

48. Where the Certifying Authority is satisfied that an Electronic Security Procedures Provider no longer meets the requirements to issue a qualified electronic security procedure, the Certifying Authority may –

(a) cancel the accreditation of the Electronic Security Procedures Provider;

(b) order the Electronic Security Procedures Provider to cease any or all of its activities, including the provision of qualified electronic security procedures;

(c) order the Electronic Security Procedures Provider to be removed from the registry;

(d) take any action that the Certifying Authority deems reasonable to ensure that the Electronic Security Procedures Provider is in compliance with the requirements set out in section 40; or

(e) make any other order that the Certifying Authority deems reasonable in the circumstances including, but not limited to reimbursement of fees and charges to users of the services of the Electronic Security Procedures Provider or public notification of cessation of business.

Pseudonyms.

49. An Electronic Security Procedures Provider may, at the request of a particular signatory, indicate in the relevant electronic security procedure a pseudonym instead of the signatory's name.

Additional responsibilities of an Electronic Security Procedures Provider.

50. An Electronic Security Procedures Provider shall ensure the operation of a prompt and secure directory of holders of qualified electronic security procedures and secure an immediate revocation service that makes it possible to ascertain –

(a) whether a qualified electronic security procedure was revoked;

(b) the validity period of the qualified electronic security procedure; or

(c) whether the qualified electronic security procedure contains any limitations on the scope or value of the electronic transactions for which the signature can be used.

Minimum information regarding electronic security procedures.

51. Before entering into an electronic contract requiring the issuance of a qualified electronic security procedure, an Electronic Security Procedures Provider shall inform the party seeking the electronic security procedure in writing of the following –

(a) the terms and conditions concerning the use of the electronic security procedure, including any limitations on its scope or amounts;

(b) any requirements concerning storage and protection of the signature-creation data by the signatory;

(c) the cost of obtaining and using the electronic security procedure and of using the other services of the Electronic Security Procedures Provider;

(d) whether the Electronic Security Procedures Provider is accredited; and

(e) procedures for settlement of complaints.

Immediate revocation upon request.

52. (1) An Electronic Security Procedures Provider shall revoke an electronic security procedure immediately on the receipt of a request to do so by the signatory or if otherwise warranted in the circumstances.

(2) An Electronic Security Procedures Provider shall ensure that the date and time when an electronic security procedure is revoked can be determined precisely.

Liability of the Electronic Security Procedures Provider issuing a qualified procedure.

53. (1) An Electronic Security Procedures Provider issuing a qualified electronic security procedure to the public is *prima facie* liable for any damages or loss caused to anyone relying on the qualified electronic security procedure due to –

(a) the Electronic Security Procedures Provider not continuing to meet the requirements set forth in section 31 or 40 at the time of the issuance of the qualified electronic security procedure; or

(b) the qualified electronic security procedure, when issued, having contained incorrect information.

(2) This section also applies to an Electronic Security Procedures Provider who guarantees that the electronic security procedure of another service provider is qualified.

Release from liability.

54. (1) An Electronic Security Procedures Provider issuing a qualified electronic security procedure may be exempted from liability if the provider can show that the injury or loss was not caused by its own negligence.

(2) The Electronic Security Procedures Provider is also not liable for damages for an injury or loss arising from the use of a qualified electronic security procedure in violation of any limitations of use or scope of transaction clearly stated in the qualified electronic security procedure.

(3) This section also applies to an Electronic Security Procedures Provider who guarantees that the electronic security procedure of another service provider is qualified.

Costs of audit.

55. The Certifying Authority may require an Electronic Security Procedures Provider to pay the costs reasonably incurred in the performance of an audit pursuant to section 45.

## PART VII

## PUBLIC AUTHORITIES USE OF ELECTRONIC RECORDS, INFORMATION, SIGNATURES AND SYSTEMS

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

56. (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; or

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

the public authority may discharge the functions by electronic form.

(2) Where a public authority pursuant to a written law receives, pays or transfers money in a particular manner, the public authority may discharge that function, subject to subsection (4)(b), by electronic form or means as provided under section 14.

(3) The Minister with responsibility for the public authority may establish electronic systems to facilitate the discharge of the functions under subsections (1) and (2).

(4) The Minister with responsibility for the public authority may, for the purposes of subsections (1) and (2), 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 form or means of receipt, payment or transfer of money by electronic means;

(c) the manner and format in which a signature shall be affixed to the form, application or other document in electronic form;

(d) the type of electronic signature required;

(e) the electronic security procedure and the identity of the Electronic Security Procedure Provider to be used;

(f) 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

(g) any other requirements for documents, records or information in electronic form.

(5) For the avoidance of doubt, notwithstanding anything to the contrary in any written law but subject to any specification made under subsection (4) 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 with responsibility for the public authority.

(6) If the Minister responsible for the public authority is satisfied that due to technical failure or lack of facilities it is not practicable to give effect to subsection (1) or (2) in any office or in respect of any work or service, that Minister may, by notice in the *Gazette*, specify the period during which subsection (1) or (2) shall not operate in the office or in respect of the work or service.

(7) Nothing in this Act obliges any public authority to generate, send, receive, store or otherwise process any record by electronic means, but the Minister with responsibility for a public authority may, by notice published in the *Gazette*, declare that the public authority may receive and process electronic communications relating to the matters specified in the notice.

Collaboration with other public authorities and private entities.

57. For the efficient running of electronic governance of public authorities, there may be collaboration, cooperation and harmonisation between public authorities and between public authorities and private entities as regards the establishment and use of electronic systems, and the requirements for electronic records, documents, fees or charges under section 56, and may necessarily enter into Memorandum of Understanding or agreement with each other.

## PART VIII

## INTERMEDIARIES AND ELECTRONIC-COMMERCE SERVICE PROVIDERS

Liability of intermediaries.

58. (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 59, 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, 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; and

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

Procedure for dealing with unlawful or defamatory information.

59. (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 60; 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 e-

60. (1) The Minister may develop codes of conduct or standards for intermediaries and electronic-commerce service providers for the purposes of this Act, which the Minister shall by notice publish in the *Gazette*.

commerce service providers.

(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 the practices.

(4) Where an intermediary or electronic-commerce service provider fails to comply with any direction given under subsection (3), within the period as may be specified in the direction, the intermediary or electronic-commerce service provider, as the case may be, commits an offence and is liable on summary conviction to a fine of five hundred thousand dollars and if the offence is a continuing one to a further fine of one hundred thousand dollars for each day the offence continues.

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

## PART IX

## OFFENCES IN RELATION TO

## RECEIPT, PAYMENT AND TRANSFER OF MONEY

False statement to procure a card.

61. (1) A person commits an offence where the person makes or causes to be made, either directly or indirectly, a false statement as to a material fact in writing, knowing it to be false and with intent that it be relied on, respecting –

(a) the person's identity or that of any other person; or

(b) the person's financial condition or that of any other person,

for the purpose of procuring the issuance of a card to the person or another person.

(2) A person who commits an offence under subsection (1) is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

Theft by taking or retaining possession of card.

62. (1) A person commits an offence where the person takes a card from the possession, custody or control of –

(a) the cardholder; or

(b) a person holding or having possession of the card with the consent of the cardholder,

without the cardholder's or the person's consent with intent to use, sell, or transfer it to a person other than the issuer or the cardholder.

(2) A person commits an offence where the person, with knowledge that a card has been taken from the possession, custody or control of –

(a) the cardholder; or

(b) a person holding or having possession of the card with the consent of the cardholder,

without the cardholder's or the person's consent, receives the card with intent to use, sell, or transfer it to a person other than the issuer or the cardholder.

(3) A person who commits an offence under subsection (1) or (2) is liable on –

(a) summary conviction to a fine of one million dollars and to imprisonment for three years; or

(b) conviction on indictment to a fine of two million dollars and to imprisonment for five years.

(4) For the purpose of this section, taking a card without consent includes obtaining it by any conduct defined or known as larceny or fraud, or by obtaining property by false pretence, or by extortion.

Card theft.

63. (1) A person commits an offence where the person receives a card that the person knows or ought to reasonably know to have been lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder and

who retains possession with intent to use, sell, or to traffic it to a person other than the issuer or the cardholder.

(2) A person who commits an offence under subsection (1) is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

Dealing in card of another.

64. (1) A person, other than the issuer, commits an offence where the person receives and retains possession of two or more cards issued in the name or names of different cardholders, which cards he has knowledge were taken or retained under circumstances which constitute a card theft.

(2) A person who commits an offence under subsection (1), is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

Purchase or sale of card of another.

65. A person other than an issuer who sells a card or a person who buys a card from a person other than an issuer commits an offence and is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

Obtaining control of card as security.

66. A person who, with intent to defraud the issuer, a creditor, or any other person, obtains control over a card as security for a debt commits an offence and is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

Forgery.

67. (1) A person commits an offence where the person –

(a) with intent to defraud an issuer, a creditor, or any other person, falsely makes, embosses, or alters in any manner a card or utters such a card; or

(b) with intent to defraud, has a counterfeit card or any invoice, voucher, sales draft, or other representation or manifestation of a counterfeit card in his possession, custody, or control.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of one million dollars and to imprisonment for three years; or

(b) conviction on indictment to a fine of two million dollars and to imprisonment for five years.

(3) A person, other than an authorised manufacturer or issuer, who possesses a counterfeit card is presumed to have the intent to defraud as required under subsection (1).

(4) A person falsely makes a card when he makes or draws in whole or in part a device or instrument which purports to be the card of a named issuer but which is not such a card because the issuer did not authorise the making or drawing, or when he alters a card which was validly issued.

(5) A person falsely embosses a card when, without the authorisation of the named issuer, he completes a card by adding any of the matter, including the signature of the cardholder, which an issuer requires to appear on the card before it can be used by a cardholder.

Signing a card of another.

68. A person, other than the cardholder or a person authorised by him, who, with intent to defraud the issuer or a creditor, signs a bank card, credit card or debit card commits an offence and is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

Fraudulent use of card.

69. (1) A person commits an offence where the person, with intent to defraud an issuer or a creditor –

(a) uses, for the purpose of obtaining money, goods, services, or anything else of value, a card obtained or retained fraudulently or a card which he knows is forged; or

(b) obtains money, goods, services, or anything else of value by representing –

(i) without the consent or authorisation of the cardholder, that he is the holder of a specified card; or

(ii) that he is the holder of a card and such card has not in fact been validly issued.

(2) A person who commits an offence under subsection (1) is liable –

(a) summary conviction to a fine of one million dollars and to imprisonment for three years; or

(b) conviction on indictment to a fine of two million dollars and to imprisonment for five years.

Fraud by person authorised to provide goods, services, etc.

70. (1) A creditor commits an offence where the creditor, with intent to defraud the issuer or the cardholder, furnishes goods, services, or anything else of value upon presentation of a card which he knows is obtained or retained fraudulently or illegally or a card which he knows is forged, expired or revoked.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of one million dollars and to imprisonment for three years; or

(b) conviction on indictment to a fine of two million dollars and to imprisonment for five years.

(3) A creditor commits an offence where the creditor, with intent to defraud the issuer, or the cardholder, fails to furnish goods, services, or anything else of value which he represents in writing to the issuer or the cardholder that he has furnished.

(4) A person who is –

(a) authorised by a creditor to furnish goods, services, or anything else of value upon presentation of a card or a card account number by a cardholder; or

(b) an agent or employee of a person who is authorised by a creditor to furnish goods, services, or anything else of value upon presentation of a card or a card account number by a cardholder,

commits an offence where the person authorised, or the agent or employee of a person authorised, with intent to defraud the issuer or the cardholder,

presents to the issuer or the cardholder, for payment, a card transaction record of sale, which sale was not made by that person, his agent or employee.

(5) A person commits an offence where the person –

(a) without the creditor's authorisation, employs, solicits or otherwise causes a person who is authorised by the creditor to furnish goods, services or anything else of value upon presentation of a card account number by a cardholder; or

(b) employs, solicits or otherwise causes an agent or employee of a person who is authorised by the creditor to furnish goods, services or anything else of value upon presentation of a card account number by a cardholder,

to remit to the creditor a card transaction record of a sale that was not made by the authorised person or the agent or employee of an authorised person.

(6) A person who commits an offence under subsection (3), (4) or (5) is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

Receipt of money, etc., obtained by fraudulent use of card.

71. A person who receives money, goods, services or anything else of value obtained in breach of section 70 knowing or believing that it was so obtained commits an offence and is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

General offence for fraudulent electronic fund transfer.

72. (1)A person commits an offence where the person, in the course of an electronic fund transfer, with intent to defraud an issuer or a creditor –

(a) uses the personal or financial data or credit account numbers or card of another; or

(b) obtains money, goods, services or anything else of value by using without authorisation the personal or financial data or credit account numbers or card of another or by representing that he is another.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of one million dollars and to imprisonment for three years; or

(b) conviction on indictment to a fine of two million dollars and to imprisonment for five years.

Alteration of card invoice.

73. A person who, with intent to defraud another person, falsely alters any invoice for money, goods, services or anything else of value obtained by use of a card after that invoice has been signed by the cardholder or a person authorised by him commits an offence and is liable on summary conviction to a fine of one million dollars and to imprisonment for three years.

Card lists prohibited.

74. (1) Subject to subsection (2), a financial institution shall not make available, lend, donate or sell any list or portion of a list of any cardholders and their addresses and account numbers to any person without the prior written permission of the cardholder.

(2) A financial institution may make available to another financial institution, which seeks to determine only the cardholder's credit rating, any list or portion of a list of any cardholders and their addresses without the permission of the cardholder but must, within seven working days, give written notice of the disclosure to the cardholder.

(3) A financial institution which breaches subsection (1) commits an offence and is liable on summary conviction to a fine of two million dollars.

Obtaining goods, etc., by use of false, expired, or revoked card.

75. (1) A person commits an offence where the person with knowledge, unlawfully obtains credit or purchases any goods, services or anything else of value –

(a) by the use of any false, fictitious, counterfeit or expired card, card number or other credit device;

(b) by the use of any card, card number, or other credit device of another person without the authority of that other person to whom such card, number or device was issued; or

(c) by the use of any card, card number, or other credit device in any case where such card, number or device has been revoked

and notice of the revocation has been given to the person to whom it was issued.

(2) A person who commits an offence under subsection (1) is liable on –

(a) summary conviction to a fine of one million dollars and to imprisonment for three years; or

(b) conviction on indictment to a fine of two million dollars and to imprisonment for five years.

(3) For the purpose of this section, knowledge of revocation shall be presumed to have been received by a cardholder seven clear days after such notice has been sent to him by post at his last known address.

Trafficking in counterfeit card.

76. (1) A person who is found in possession of three or more counterfeit cards, invoices, vouchers, sales drafts, or other representations or manifestations of counterfeit cards, or card account numbers of another person is deemed to have the same for the purpose of trafficking, and unless the contrary is proved, the burden of proof being on the accused, the person commits an offence.

(2) A person who commits the offence of trafficking under subsection (1) is liable on summary conviction to a fine of two million dollars and to imprisonment for five years.

Possession of card-making equipment.

77. A person who receives, possesses, transfers, buys, sells, controls, or has custody of any card-making equipment with intent that such equipment be used in the manufacture of counterfeit cards commits an offence and is liable on summary conviction to a fine of two million dollars and to imprisonment for five years.

Defences not available.

78. It shall not be a defence to a prosecution for an offence under this Act that a card that is not a counterfeit card is offered for use or sale as a counterfeit card, and a person, other than the defendant, who has breached this Act has not been convicted, arrested, or identified.

Liability for misuse of card.

79. (1) A cardholder shall not unless he acts in collusion with another person be liable to the issuer for any loss arising from use of the card by any person not acting, or to be treated as acting, as the cardholder's agent.

(2) Subsection (1) does not prevent the cardholder from being made liable to the extent of [one hundred dollars] for loss to the issuer arising from use of the card by another person during a period beginning when the card ceases to be in the possession of any authorised person and ending when the card is once more in the possession of an authorised person.

(3) Subsection (1) does not prevent the cardholder from being made liable to any extent for loss to the issuer from use of the card by a person who acquired possession of it with the cardholder's consent.

(4) Subsections (2) and (3) shall not apply to any use of the card after the issuer has been given notice within two days of discovering that the card is lost, stolen, or is for any other reason liable to misuse.

(5) Subsections (2) and (3) shall not apply unless the issuer provides the cardholder with particulars of the name, address and telephone number of a person stated to be the person to whom notice is to be given under subsection (4).

(6) Notice under subsection (4) takes effect when received, but where it is given orally, it shall be confirmed in writing within fourteen clear days.

(7) Any sum paid by the cardholder for the issue of the card, to the extent, if any, that it has not been previously offset by use made of the card, shall be treated as paid towards satisfaction of any liability under subsection (2) or (3).

(8) The cardholder, issuer or any person authorised by the cardholder to use the card shall be authorised persons for the purpose of subsection (2).

Territorial scope of offences under this Part.

80. (1) Subject to subsection (2), this Part shall have effect in relation to any person, whatever his nationality or citizenship, outside as well as within Guyana; and where an offence under this Act is committed by a person in any place outside of Guyana, he may be dealt with as if the offence had been committed within Guyana.

(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question –

(a) the accused was in Guyana at the material time;

(b) the card, computer or data was in Guyana at the material time;

(c) the card was issued by a financial institution in Guyana; or

(d) the damage occurred within Guyana, whether or not paragraph (a), (b) or (c) applies.

## PART X

## MISCELLANEOUS

Liabilities of directors and officers.

81. Where a body corporate commits an offence under this Act, any officer, director or agent of the body corporate who directed, authorised, assented to or participated in the commission of the offence is a party to and commits an offence and is liable to the punishment provided for the offence.

General penalty.

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

(a) summary conviction to a fine of one million dollars and to imprisonment for three years; or

(b) conviction on indictment to a fine of two million dollars and to imprisonment for five years.

(2) Where the offence under this Act is committed by a body corporate for which no penalty is provided, the body corporate is liable on –

(a) summary conviction to a fine of two million dollars; or

(b) conviction on indictment to a fine of five million dollars.

Jurisdiction of the Courts.

83. The Courts shall have jurisdiction to hear, determine and make Orders in relation to –

(a) applications for any Order which the Court considers appropriate to facilitate the enforcement of any provisions of this Act; or

(b) upon an application pursuant to this Act, cases involving any contravention of the provisions of this Act.

Regulations.

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

(2) In particular and without prejudice to the generality of subsection (1), the Minister may make regulations with respect to any matter that is required to be prescribed under this Act.

(3) Regulations made under this Act may provide that a contravention of a specified provision of the Regulations shall be an offence liable to summary conviction, and the penalty to be prescribed by the Regulations for the commission of an offence shall not exceed a fine of two million dollars and imprisonment for five years.

**SCHEDULE** s. 4

**DOCUMENTS AND TRANSACTIONS**

1. Creation or transfer of interest in movable or immovable property.
2. Negotiable instruments.
3. Documents of title.
4. Wills and other testamentary instruments.
5. Trusts.
6. Powers of attorney.

*Passed by the National Assembly on the 3rd August, 2023.*

*S.E. Isaacs, A.A.,*

Clerk of the National Assembly.

**(BILL No. 9/2023)**