

FINAL VERSION

A Bill

entitled

“FIRST ATLANTIC COMMERCE LTD.

ELECTRONIC COMMERCE ACT 1999”

WHEREAS the Company has presented a Petition praying the enactment of certain provisions for the advancement of electronic commerce in these Islands and elsewhere, and for the clarification of the law in relation to the Company, its Clients and the Consumers wheresoever situate of the goods and services which they may acquire across the medium of the internet from the Clients of the Company, and for the protection of the rights of and the protection from harm of the Company, its Clients and Consumers;

AND WHEREAS the Company prays by its petition for the enactment of certain provisions having private effect, but which relate to the immediate conduct of the Company's business, the protection of Clients and Consumers and the advancement of electronic commerce generally in circumstances where no public legislation now exists to govern these matters;

AND WHEREAS it is deemed expedient to pass an Act to give effect to the prayer of the Petition;

NOW BE IT THEREFORE ENACTED by the Queen's Most Excellent Majesty, by and with the advice and consent of the Senate and the House of Assembly of Bermuda and by the authority of the same as follows:

PART I
Interpretation and Application

1. This Act may be cited as The First Atlantic Commerce Ltd. Electronic Commerce Act 1999.

2. In this Act, unless the context otherwise requires:

“Addressee” of a Data Message means a person who is intended by the Originator to receive the Data Message, but does not include a person acting as an Intermediary with respect to that Data Message;

“Authenticate” means to sign, or to execute or adopt a symbol or sound, or encrypt or process a Record in whole or in part, with intent by the authenticating party;

“Banking” means the conduct of banking business as defined in Section 1 (1) of the Banks Act 1969;

“Business” means electronically based data transactions for digitally based commerce of all types and between any parties including, but not limited to, financial settlements, web-based marketing, advisory and transactional services, database services and products, on-line services of all types, and all related data communication services, whether conducted by e-mail, document management, voice or data transmission, or otherwise;

“Certification Authority” means any person who, or entity which, in the course of its business, engages in issuing identity certificates in relation to cryptographic keys used for the purposes of Electronic Signatures;

“Certification Authority Data” means all communications passing through a Certification Authority;

“Client” means a person who enters into contractual relations with the Company in relation to the sale by the Client of their goods or services over the Internet through the medium of the Company's Facility;

“Companies Act” means the Companies Act 1981 together with all amendments thereto and regulations made thereunder, and all statutes enacted from time to time having specific application to companies incorporated, registered or permitted to trade in or from within Bermuda;

“Company” means First Atlantic Commerce Ltd;

“Consumer” means any person or company which enters into contractual relations with a Client of the Company for the purchase of goods or services over the internet through the medium of the Facility offered by the Company;

“Contract” and “Contracted” means an agreement, whether entered into orally, in writing or electronically, between two or more persons which creates an obligation to do or not to do a particular thing in exchange for a consideration;

“Courts of Bermuda” and “Court” mean the Magistrates Court, Supreme Court and Court of Appeal of Bermuda;

“Correspond” in relation to Private or Public Keys means to belong to the same Key Pair;

“Digital Signature” means a cryptographic transformation of the numerical representation of a Data Message, such that any person having the Data Message and the relevant Public Key can determine that the transformation was created using the Private Key corresponding to the relevant Public Key and that the Data Message has not been altered since the cryptographic transformation;

“Data Message” means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

“Directive” means legislation adopted by the European Parliament and Council which is to later be brought into effect in each member state of the European Union by means of its own national legislation;

“Electronic Signature” means digital code intended by the Originator to indicate assent;

“Encryption” means the process by which communications are kept private by the method of transforming data into an unintelligible form;

“EU Data Protection Law” means European Directive 95/46 E.C.;

“Facilities” or “Facility” means, inter alia, the programmes, networks, systems, servers, web sites, routers, firewalls, secure gateways, hardware, software, and any other thing having a function in relation to the conduct of Business;

“Functional Equivalent” means having an analogous effect regardless of the medium used;

“Information” means data, text, signs, signals, writing, images, sound, codes, computer programmes, software, data bases, and intelligence of any nature;

“Information System” means a system for generating, sending, receiving, storing or otherwise processing Information;

“Intermediary” with respect to a particular Data Message, means a person who, on behalf of another person, sends, receives or stores that Data Message or provides other services with respect to that Data Message;

“Invitation to Treat” means the web site of a Client, incorporating standard terms and conditions of Contract used to promote the sale of goods or services by a Client over the internet through the medium of the Company's Facilities;

“Investment Business” means investment business as defined in Section 2 of the Investment Business Act 1998;

“Key Pair” means a Private Key and its mathematically related Public Key, having the property that the Public Key can verify an Electronic Signature that the Private Key creates;

“Minister” means the Minister of Finance or such other Minister as may be responsible for the administration of the Companies Act;

“Originator” of a Data Message means a person by whom, or on whose behalf, the Data Message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an Intermediary with respect to that Data Message;

“Private Key” means the key of a Key Pair used to create an Electronic Signature;

“Public Key” means the key of a key pair which can verify an Electronic Signature that the Private Key creates;

“Public Key System” means a system of encryption that employs a Key Pair, being a Public Key which corresponds to a Private Key, thereby providing a method by which the identity of the Originator of a message may be identified;

“Record” means information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in comprehensible form;

“Registrar” means the Registrar of Companies appointed pursuant to section 3 of the Companies Act, or such other person as may be performing his duties under the Companies Act;

“Relevant Person” means any person who might reasonably be expected to rely on a Digital Signature, Electronic Signature or Record;

“Segregated Accounts” shall have the meaning assigned to that term by Schedule IV of this Act;

“Subsidiary” has the same meaning as assigned to that term by section 86(l) of the Companies Act.

3. This Act applies to the Business conducted by the Company, its Clients and Consumers.

PART II

The Advancement of Electronic Commerce

4. (1) Subject to the satisfaction of the provisions of subsection (3), a Contract shall not be denied legal effect, validity or enforceability by reason only that it has been negotiated, settled, executed, recorded or performed in electronic form, or by electronically manifest communications between the parties.

The On-line
Creation of
Legally
Enforceable
Obligations
- (2) For the avoidance of doubt, the ordinary law of contract shall apply in relation to Contracts governed by Bermuda law for the construction of the actions and intentions of the parties to any such Contract, save that where there is no equivalent in the ordinary law of contract to any action performed on-line, a Court shall have regard to the electronic consequences of such act and, save where there is manifest error or *bona fide* mistake at law, the Originator of such action shall be deemed to have intended that effect and the action shall take effect as the Functional Equivalent of the element at law which shall have been in dispute.
- (3) A Contract shall be deemed to have been formed electronically over the internet using the medium of the Company's Facilities in the event the following shall have occurred:
 - (a) An Invitation to Treat is extended by the Client, or by the Company on behalf of the Client;

- (b) The Consumer makes an offer to the Client, or to the Company acting on behalf of the Client, by the intentional performance of any action on-line which necessarily results in the transfer of cash or credit in exchange for goods or services; and
 - (c) The Client indicates its acceptance of that offer by the intentional performance of any action on-line which necessarily indicates a promise in respect of the delivery of goods or services, or the supply of information or other intellectual property in exchange for cash or credit.
 - (4) A Contract concluded in compliance with subsection (3) shall be deemed to incorporate the Client's or the Company's standard terms and conditions provided that the contracting party has reviewed, or has had an opportunity to review, those standard terms and conditions, prior to the formation of the Contract whether by posting such provisions for review on the web site or otherwise.
 - (5) For the avoidance of doubt, the actions contemplated by paragraphs 4(3)(b) and 4(3)(c) as indicating formal assent to a Contract shall include any act that would lead a reasonable person to conclude that an agreement had been reached, including without limitation by clicking on an icon that specifically indicates acceptance of, agreement to, consensus ad idem or approval of such Contract, or the enablement thereof.
 - (6) A Contract may be found in any circumstances or combination of circumstances which establishes that the parties are ad idem with the intention of being legally bound to certain terms, including, without limitation, part performance of the Contract which shall be deemed formal assent to, and evidence of, acceptance of the Contract.
5. (1) Information shall not be denied legal effect, validity or enforceability or admissibility into evidence by reason only that it is in the form of a Record or Electronic Signature or on the ground that it is not in its original form or is not an original.
- (2) Information in the form of a Record or Electronic

Electronic
Records

Signature shall be given due weight in evidence by the Court. In calculating such weight, the Court may consider the manner in which it was generated, stored, or communicated, the reliability of the manner in which its integrity was maintained, the manner in which its Originator was identified or the Record was signed and any other relevant information or circumstances.

- (3) In determining the reliability of the manner in which the integrity of a Record was maintained, the Court may have regard to the following considerations:
 - (a) by demonstrating that the Records have been made in the usual and ordinary course of business;
 - (b) the Records are a part of a complete record-keeping process, including input of entries, transmission of information, storage system, retrieval system, tangible presentation and system security;
 - (c) the Records are a result of a post entry/pre-storage data verification (data audit) system;
 - (d) without prejudice to Section 27E (3) of the Evidence Act 1905 data inherent in the Records have been recorded within a reasonable time, if not immediately;
 - (e) the business procedures and practice to create the Records have been followed as a matter of administrative routine and standard operation;
 - (f) the Records are those which the electronic commerce parties rely upon in making their day-to-day business decisions;
 - (g) without prejudice to Section 27E (C) of the Evidence Act 1905 the keeper of the Records can demonstrate that its information system can record, store, retrieve and reproduce business records fully and accurately;
 - (h) that the security features of the operating system prevent the Records from being

modified, sabotaged or otherwise tampered with in any way that would adversely affect their reliability; and,

- (i) that a senior officer of the Company is directly responsible for all aspects of Record creation, storage and retrieval.
- (4) Where a statutory provision or other law requires information to be “written”, or “in writing”, or to be presented in writing, or provides for certain consequences if it is not, a Record created or maintained by the Company, a Client or a Consumer satisfies that statutory provision or other law if the information contained therein is accessible so as to be usable for subsequent reference.
6. (1) Where a rule of law requires that certain documents, records or information be retained, that requirement is satisfied by retaining them in the form of Records if the following conditions are satisfied:
- (a) the Information contained therein remains accessible so as to be usable for subsequent reference;
 - (b) the Record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated by an expert to represent accurately the Information originally generated, sent or received; and
 - (c) such Information, if any, as enables the identification of the origin and destination of a Record and the date and time when it was sent or received, is retained.
- (2) An obligation to retain documents, records or information in accordance with subsection (6)(1)(b) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a Record 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 in paragraphs (a) to (c) of that subsection are complied with.
- (4) Nothing in this section shall:

- (a) apply to any rule of law which expressly provides for the retention of documents, records or information in the form of electronic Records;
 - (b) preclude the Minister from specifying additional requirements for the retention of Records that are subject to the jurisdiction of such Minister.
7. (1) A Digital Signature shall be effective for all purposes of law to confirm the authenticity and validity of a Record if it complies in respect of the Originator with the provisions of Section 10(1) *mutatis mutandis*, as if such Digital Signature were the Data Message referred to therein. Signatures
- (2) Where a statutory provision or other law requires a signature, or provides for certain consequences if a document is not signed, an Electronic Signature processed by the Company satisfies that statutory provision or other law.
- (3) An Electronic Signature may be proved in any manner, including, without limitation, by showing that it is a Digital Signature or that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that a Record is that of such party.
- (4) Where consequences in law would arise from the use of a signature, those consequences shall arise from an Electronic Signature.
8. A Record is presumed to have been signed if a Digital Signature is affixed to or logically associated with such Record.
9. An Electronic Signature is presumed to be that of the Originator from whom it purports to be generated, unless it is established that the Electronic Signature was applied neither by the Originator nor by a person who had the authority of the Originator. Authentication
10. (1) As between the Originator and the Addressee, a Data Message 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 in respect of that Data Message; or
 - (b) by an Information System programmed by or on behalf of the Originator to operate automatically.
- (2) As between the Originator and the Addressee, an Addressee is entitled to regard a Data Message as being that of the Originator if.
 - (a) in order to ascertain whether the Data Message was that of the Originator, the Addressee properly applied a procedure previously agreed to by the Originator for that purpose; or
 - (b) the Data Message as received by the Addressee resulted from the actions of a person whose relationship with the Originator or with any agent (or other person acting by authority) of the Originator enabled that person to gain access to a method used by the Originator to identify the Data Message as his own.
- (3) Subsection (2) shall not apply:
 - (a) from the time when the Addressee has both received notice from the Originator that the Data Message is not that of the Originator, and has had reasonable time to act accordingly;
 - (b) in a case within subsection (2)(b), at any time when the Addressee knew or ought to have known, had it exercised reasonable care or used any agreed procedure, that the Data Message was not that of the Originator; or
 - (c) if in the opinion of the Court, taking into account all the circumstances of the case, it is unconscionable for the Addressee to regard the Data Message as that of the Originator or to act on that assumption.
- (4) Where a Data Message is that of the Originator or is deemed to be that of the Originator, or the Addressee is entitled to act on that assumption, then, as between the Originator and the Addressee, the Addressee is entitled to regard the Data Message received as being what the

Originator intended to send, and to act on that assumption.

- (5) The Addressee is not so entitled when the Addressee knew or should have known, had the Addressee exercised reasonable care or used any agreed procedure, that the transmission resulted in an error in the Data Message as received.
 - (6) The Addressee is entitled to regard each Data Message received as a separate Data Message and to act on that assumption, except to the extent that the Addressee duplicates another Data Message and the Addressee knew or should have known, had the Addressee exercised reasonable care or used any agreed procedure, that the Data Message was a duplicate.
11. Where a Digital Signature is properly applied to a designated portion of a Record and indicates that the designated portion of the Record has not been changed since a fixed time it is presumed that the designated portion of the Record has not been changed since that time.
12. (1) Where a rule of law requires information to be presented or retained in its original form, or provides consequences for the information not being presented or retained in its original form, that rule of law is satisfied by a Record if there exists reliable assurance as to the integrity of the information from the time when it was generated in its final form, as an electronic Record or otherwise. Verification of Records
- (2) The criteria for assessing the integrity of a Record or a Data Message shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement or other information that arises in the normal course of communication, storage and display. The standard of reliability required to ensure that information has remained complete and unaltered shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.
13. The Company may employ Encryption devices, software and systems of any bit size which may lawfully come into the possession of the Company. Cryptography

PART III

Administration of the Company

14. Notwithstanding any statutory provision or other law to the contrary:
- Conduct of
Business
- (a) the Company shall have, inter alia, the powers and objects set out in the First and Second Schedules of the Companies Act save that the Company shall not engage in insurance business or mutual fund business without a licence from the business or mutual fund business without a licence from the Minister;
 - (b) the Company shall have the capacity to carry on the Business and to operate a Facility;
 - (c) the Company shall have the capacity to carry on and to issue, enter into, obtain, receive and perform its obligations under any lawful Contract; and
 - (d) Notwithstanding the generality of paragraphs (a) - (c), the Company shall not have power to conduct Banking business, Investment Business or facilitate collective investment schemes or to use its Facility for the purpose of a Client conducting any Banking business, Investment Business or facilitate collective investment schemes without the consent of the Bermuda Monetary Authority.
 - (e) Notwithstanding the generality of paragraphs (a) - (c), the company shall not have power to conduct insurance or reinsurance business without a licence pursuant to the Insurance Act 1978.
15. For the purposes of subsection (d) above, the expression “performed” shall mean the delivery of the goods or services Contracted for.
16. (1) The Company when acting as an Intermediary shall not be subject to any civil or criminal liability under any statutory provision or other law in respect of::
- Exclusion of
Liability
- (a) third-party material, namely Records to which the Company merely provides access, or in respect of any matter posted on a web site of a Client or posted to any web site hosted on the

Company's Facility by a Consumer in a chat room, news group or any other place on such web site, if such liability is founded on:

- (i) the making, publication, dissemination, or distribution of such materials or any statement made in such materials; or
 - (ii) the infringement of any rights subsisting in or in relation to such materials; or
- (b) the use of hypertext links from the web site of a Client, or from a web site operated by or hosted on the Company's Facility, to other web sites; or
 - (c) any harm, injury, damages or liability whatsoever that is caused to any of the Clients of the Company, or to Consumers, by any person other than the Company; or
 - (d) non-compliance with Part V hereof, where such non-compliance arises by reason of a Client's providing a Data Controller for the purposes of Section 33 and Schedule V.
- (2) Nothing in this section shall affect:
- (a) any obligation founded on Contract as between the Company and a Client or a Consumer; or
 - (b) any obligation imposed under any statutory provision or by a Court to remove, block or deny access to any material.
- (3) The Company shall not be liable to any person in the event that the Facilities shall be rendered inoperable or in the event of any interruption of service by the Company by reason of the failure of any third party to render services to the Company to enable the Company to provide the Facilities.
- (4) In this section:
- (a) "provides access" in relation to third-party material, means the provision of the necessary technical means by which third-party material may be accessed and includes the automatic

and temporary storage of the third-party material for the purpose of providing access;

- (b) “third-party”, in relation to the Company, includes a Client or Consumer or any person over whom the Company has no effective control.
- (5) The liability of the Company with respect to all electronic commerce transactions entered into by the Company shall be limited in respect of claims in contract or tort (including product liability).
- (6) The limitation of liability under subsection (5) shall be subject to a maximum aggregate liability in relation to claims arising out of any one occurrence or in any one year (whichever shall first arise) of \$100,000.
- (7) The Company shall have the power by Contract to vary the provisions of subsection (6).
17. (1) Without prejudice to the generality of Sections 14 and 15, the enactments set out in Schedule I shall have only such limited application to Clients as may be specified in Schedule I. Modified application of certain statutes
- (2) The Minister shall have power to add to, vary or rescind any modified provision as may be set out in Schedule I.
18. Unless the parties otherwise expressly agree, any Contract or agreement between the Company and a Client shall, be deemed to be formed in Bermuda and governed by and construed in accordance with Bermuda law.
19. Transactions of any type between the Company and any Client, and whether or not conducted across the Company’s Facilities, shall, unless expressly agreed otherwise, be deemed for all purposes of Bermuda law to take place in Bermuda and no Court shall enforce the judgment of any foreign court to the extent such enforcement is premised upon a finding of a situs other than Bermuda.
20. Without prejudice to section 14, any dispute which may arise in relation to the content of any web site operated or hosted by the Company, any communication and data transmissions to and from Bermuda by the Company, or any Contract between the Company and a Client shall, unless expressly provided to the Jurisdiction

contrary, be subject to the exclusive jurisdiction of the Bermuda Courts.

21. (1) The Bermuda Courts shall have exclusive jurisdiction to consider any matter touching upon the nature, capacity or authority of the Company and, without prejudice to section 14(c) the use and scope of the Company's Facilities.
- (2) No judgment, order, application or process documents of a foreign court shall be enforced to the extent that they go to the matters referred to in subsection (1).
22. (1) The protection afforded to the various forms of intellectual property under the following Acts: Protection of Intellectual Property
- (a) the United Kingdom Copyright Act 1956, the provisions of which were extended to Bermuda by the Copyright (Bermuda) Order 1962;
- (b) the Trade Marks Act 1974 and associated Regulations, including the Trade Marks and Service Marks Regulations 1993; and
- (c) the Patents and Designs Act 1930 and associated Rules;
- shall apply and the Company shall be afforded protection for, inter alia:
- (i) the copyright in web site design and content;
- (ii) the confidentiality of Data, Messages;
- (iii) the trade marks, service marks, goodwill and reputation of the Company; and
- (iv) multi-media works, which shall be protected as being all of a literary work, film, photograph and sound broadcast.
- (2) In relation to the protection afforded by (iii) above, the Company shall be entitled to control its brand and shall

be entitled to bring an action in the Courts of Bermuda against any party which engages in the tort of passing off in relation to its business get-up, trade or service marks.

- (3) In relation to the protection afforded by (i) above, it shall include protection for the look and feel of web sites, which means how the various elements of the web site are sequenced, structured and organised, as well as the visual appearance of such web sites.
23. (1) All Information, trade secrets, know-how and data of the Company shall be the sole and exclusive property of the Company and shall be held as confidential by the Company and by any third party coming into possession of such information, trade secrets, know-how or data. Confidentiality
- (2) The Company shall take reasonable care to ensure that any such information, trade secrets, know-how and data shall not come into the possession of any unauthorised party and shall not itself disclose such information, trade secrets, know-how or data to any person save where required by express provision of law.
- (3) Any persons coming into possession of any such Information trade secrets, know-how or data shall use their reasonable efforts to protect that property from any tampering, theft, modification, alteration, elimination, unauthorised access, unauthorised transmission, or unauthorised use or exploitation of any nature whatsoever.
24. Notwithstanding section 61 of the Telecommunications Act 1986, it shall be lawful for the Company to record and disclose to a person authorised by law to receive the same, any information tending to disclose the commission of a crime, a fraud or any other activity having effect in Bermuda (other than by reason of data transmission across the Facilities of the Company) which is contrary to Bermuda law or any international treaty to which Bermuda is subject. Recording of Transactions
25. (1) A Subsidiary of the Company may for the purposes of availing itself of the provisions of this Act, with the prior written consent of the Minister, by notice, apply to the Registrar to be registered under this section. Extension of this Act to Wholly-owned Subsidiaries
- (2) A notice referred to in subsection (1) of this section

shall be in the form set out in Schedule II.

- (3) The Registrar shall, upon receipt of the notice and the consent of the Minister, register the Subsidiary as being entitled to avail itself of the provisions of this Act and such entitlement shall be effective on the date of such registration.
- (4) Where a Subsidiary of the Company, being registered under this section, ceases to be a Subsidiary of the Company, it shall, within thirty days of ceasing so to qualify, or such later date as the Registrar may in his discretion permit, give written notice to the Registrar thereof in the form set out in Schedule III and the Registrar shall register that company as ceasing to be entitled to avail itself of the provisions of this Act and such cessation shall be effective on the date of such registration.
- (5) The Registrar shall maintain a public record of all registrations under this section, in such form and manner as the Registrar may in his discretion consider appropriate.

PART IV

Protection of Clients of the Company

- | | | |
|-----|---|---|
| 26. | For the protection of the separate interests of Clients, the Company may operate Segregated Accounts in accordance with the provisions of Schedule IV. | Segregated
Accounts |
| 27. | Any disclaimer posted on a web site operated by a Client or the Company shall be effective for all purposes of law if it is clearly visible or indicated and identified as a term of or condition precedent to any Contract. | Enforcement
of Web Site
Disclaimers |
| 28. | All web site disclaimers shall be governed by and construed in accordance with Bermuda law, and no Court in Bermuda shall enforce the judgment, order, application or process documents of any foreign court in so far as they purport to govern a web site hosted on a server belonging to the Company and located in Bermuda. | |
| 29. | (1) Subject to Section 24, the Company shall hold as confidential all Information, and any Record relating to a Client, and shall not disclose, divulge, furnish or make accessible to any person, any confidential information or proprietary information belonging to a Client, including but not limited to trade secrets, which | Client
Confidentiality |

may have been communicated to the Company by the Client.

- (2) This section shall apply to third parties who come into possession of web site material which relates to a Record belonging to any party using the Company's Facility, and shall also apply to third parties who have received confidential information or trade secrets from a Client or any other person.
 - (3) A Client shall be entitled to obtain injunctive relief in Bermuda to prevent the unauthorised use or disclosure of any confidential information or proprietary information.
- 30.
- (1) In the event that a Consumer shall learn that its Digital Signature has, without authorisation, been intercepted, altered or corrupted in any manner, the Consumer shall be bound to notify the Client forthwith.
 - (2) In the event a Consumer shall fail to notify a Client as provided in subsection (1), the Consumer shall be liable for all loss, damage or expense arising by reason of any misuse of the Digital Signature consequent on such interception, alteration or corruption.
 - (3) In the event that a Consumer shall give notice as provided in subsection (1), the Consumer shall not be liable as provided in subsection (2).
- 31.
- (1) Notwithstanding any provision of this Act or the Telecommunications Act 1986 it shall be lawful for the Company or a Client to access Records and any computer system under the control of a Client or a Consumer where there are reasonable grounds in the opinion of the Company or the Client or upon lawful instruction from the Minister for the suspicion of the commission or intended commission of a crime under the laws of any jurisdiction and provided that the Company or Client, as the case may be, has obtained a court order authorising such access.
 - (2) The Company shall have the power to waive its right under subsection (1) above with respect to its dealings with particular Clients or Consumers.
 - (3) Reference in subsection (1) above to court orders shall include orders granted on an *ex parte* basis.

PART V
Protection of the Consumer

32. Where an agreement so provides, Consumers shall be entitled to all of the protections as to the compilation, storage and dissemination of Personal Data as are set out in Schedule V, and the provisions of this section and of Schedule V shall apply to the Company, the Company Data Controllers, their employees and officers, and to all Clients who are not the Company's Data Controllers. Personal Data Protection
33. Where a Contract so provides, the Company shall be bound to carry on its Business in accordance with the terms of this Act, and to maintain its Facilities in compliance with Schedule V.
34. In the event that any Directive or other regulation or instrument shall be issued by the European Union limiting or reducing the requirements for personal data protection in respect of jurisdictions outside the European Union, the provisions of Schedule V shall be reduced or modified to like effect without any further action to be taken by the Company in respect of this Act, or any amendment of this Act being required or in respect of a Contract, the terms of which shall be modified accordingly.
35. (1) Without prejudice to the provisions of sections 31 and 32, all Records maintained by a Client in respect of a Consumer shall be treated as confidential and shall not be disclosed to any person for any purpose without the consent of the Consumer. Confidentiality
- A Consumer who may be aggrieved by a breach of the Client's duty under subsection (1) shall be entitled to injunctive relief in the Courts of Bermuda without demonstrating that he has suffered damage in consequence of the breach.
36. Unless the parties otherwise expressly agree, any Contract or agreement between a Client and a Consumer for the purposes of a transaction effected through the medium of the Facilities of the Company shall be deemed to be formed in Bermuda and governed by and construed in accordance with Bermuda law, and the provisions of the Sale of Goods Act 1978 shall be incorporated by reference therein. Governing Law
37. Unless the parties otherwise expressly agree, the situs of any transaction effected through the medium of the Facility shall for all purposes of Bermuda law, and as a limitation on the enforcement of any judgment, order, application or process documents of a foreign court, be deemed to be Bermuda. Situs

38. (1) Consumers shall be deemed to have submitted to the non-exclusive jurisdiction of the Bermuda Courts, and Consumers shall have standing to argue or respond to any matter connected with a Contract or a Client before the Bermuda Courts, whether or not such Consumer shall be a company subject to the Companies Act, or a natural person, partnership or firm who would otherwise not be subject to the jurisdiction of Bermuda. Jurisdiction
- (2) The Court shall not entertain an assertion of *forum non conveniens* by any person using the Facilities of the Company, or effecting a settlement through the medium thereof.

PART VI
Miscellaneous

39. In the event that there shall be enacted in these Islands any law of general application going to the provisions of sections 5,6,7,8,9,10,11,12,16 and 22, such law shall supersede the said provisions of this Act. Public Enactments to Supersede this Act
40. (1) The Minister may, in his discretion, on application by the Company extend part or all of the provisions of this Act to third parties connected with the Company for the provision of services to Clients. Extension of this Act to Authorised Third Parties
- (2) For the purposes of this section “connected with the Company for the provision of services to Clients” shall mean that there is a Contract between some person and the Company the subject matter of which is the provision of services of any nature to Clients, or, that the Company shall have less than a majority shareholding in a company and the commercial purpose of that other company and the Company taken together is to render services to Clients.
- (3) Any application pursuant to subsection (1) shall be supported by such documents as the Minister may require.
- (4) Any extension of this Act pursuant to subsection (1) which may be approved by the Minister, and the terms thereof, shall be gazetted.
41. The Minister shall have power to revoke any extension of this Act which may have been granted pursuant to section 40, save that where the Minister is minded to revoke any such extension the Company shall have the right to be heard in the matter.

42. (1) Any on-line dispute resolution system having the characteristics set out in subsection (2) and conducted between the Company and a Client, or a Client and a Consumer, shall be valid, binding and effective as if it had been conducted in accordance with the Arbitration Act 1986 or the Bermuda International Conciliation and Arbitration Act 1993 as the case may be. On-line Alternative Dispute Resolution
- (2) Without prejudice to the generality of subsection (1), any on-line dispute resolution system which has the following characteristics:
- (a) a web-based document filing system allowing parties to submit instantaneously any number of documents over any distance;
 - (b) an automated document management system which is capable of processing, storing and archiving documents submitted to the arbitrator or arbitrators;
 - (c) facilities which allow for the on-line review of any documents submitted to the arbitrator or arbitrators by parties with the required access rights on a 24-hour basis from anywhere in the world;
 - (d) appropriate audio and video facilities which allow for the conduct of meetings or hearings on-line;
 - (e) applicable procedures in cases of challenges to the authenticity of documents or parties; and
 - (f) facilities allowing for the writing and signing of documents on-line for the purposes of party communications and for any award made by an arbitrator or arbitrators;
- shall be effective for the resolution of any dispute going to a Contract or arising out of any provision of this Act, other than a provision relating to an offence, and any award made pursuant to any such on-line dispute resolution system shall be deemed to be an award for the purposes of the Arbitration Act 1986 or the Bermuda International Conciliation and Arbitration Act 1993, as the case may be.
43. To the extent that reciprocal facilities are made available by any Governmental authority of Bermuda, it shall be lawful and effective for all purposes that the Company or any Client shall file any document, submission, statement, declaration or return Electronic Filings

by way of a Record delivered electronically.

44. Nothing contained in this Act shall be construed to affect the rights of Her Majesty, Her heirs and successors or of any body politic or corporate or of any other person or persons except such as are mentioned in this Act, and those claiming by, from or under them.

Saving of
Rights of
Crown

SCHEDULE I

Statutes Having Limited Application

“None”

SCHEDULE II

**Form of Notice of Wholly-owned Subsidiaries
First Atlantic Commerce Ltd. Electronic Commerce
Act 1999
("the Act")
NOTICE PURSUANT TO SECTION 25(1)**

I, [name and address of person giving notice] a duly authorized representative of [name of Subsidiary] hereby give you notice pursuant to Section 25(1) of the Act that [name of Subsidiary] is a subsidiary of First Atlantic Commerce Ltd. and desires to be registered under the said section. Attached hereto is evidence of receipt of the Minister of Finance's consent approving such registration, as required under the said section.

Yours faithfully,

[signature of the person giving notice]

Date of Notice: [day, month and year]

SCHEDULE III

**Form of Notice of Companies Ceasing to be
Subsidiaries
First Atlantic Commerce Ltd. Electronic Commerce
Act 1999
("the Act")
NOTICE PURSUANT TO SECTION 25(4)**

I, [name and address of person giving notice] a duly authorized representative of [name of former Subsidiary] hereby give you notice pursuant to Section 25(4) of the Act that [name of former Subsidiary] ceased to be a subsidiary of First Atlantic Commerce Ltd. on [day, month and year].

Yours faithfully,

[signature of the person giving notice]

Date of Notice: [day, month and year]

SCHEDULE IV**Segregation of Accounts**

1. (1) “Segregated Account” means each account established or recorded pursuant to Section 2 of this Schedule, which shall be evidenced in the records of the Company and may be composed of sub-accounts and where there are sub-accounts, the expression “Segregated Account” shall mean also each sub-account.
- (2) Where required under, and in accordance with, the terms of a Contract, the Company shall pursuant to the provisions of this schedule establish and maintain a Segregated Account.
- (3) Subject to the provisions of this Act, rights and interests in assets and property standing to the credit of a Segregated Account shall be determined by the terms of the related Contract and no other rights or interests which might exist in such assets and property shall be recognized, notwithstanding any statutory provision or rule of law to the contrary.
- (4) The Company shall maintain separate books and records for each Segregated Account, in accordance with such generally accepted accounting principles consistently applied with any amendments thereto and any additional principles, as may be determined from time to time by the Company.
- (5) The Company shall credit to the relevant Segregated Account all capital, assets, income, expenses and liabilities as may be attributable to the Client pursuant to the Contract and in accordance with generally accepted accounting principles.
- (6) Subject to the terms and conditions of a Contract to which a Segregated Account relates, the Company may invest and deal with the assets, investment income and other property credited to that Segregated Account in such manner as the Company thinks fit.
- (7) All income, interest, or other gains earned from investing or dealing with the assets, investment income and other property belonging to or concerning a Segregated Account shall be credited to that Segregated

Account.

- (8) All expenses relating to the Segregated Account or incurred from dealing or investing the assets, investment income and other property belonging to or concerning a Segregated Account shall be charged against that Segregated Account.
2. The assets and property standing to the credit of a Segregated Account shall, after deduction of all amounts payable in accordance with subsection 1 (7), be held by the Company subject to the provisions of this Act, for the benefit of the related Client pursuant to the Contract and no other person shall have any right or interest in such assets.
3. (1) Notwithstanding any statutory provision or any rule of law to the contrary, but subject to subsection (2):- Restrictions on Winding Up Company
- (a) No petition shall be presented to the Court for the winding up of the Company by any person; and
- (b) The Company shall not be voluntarily wound up, without the consent of the Registrar, which consent shall not be granted until the Company has paid all amounts due under all Contracts or until seventy-five percentum of the number of Clients consent in writing to the proposed petition or to the Company being wound up (as the case may be).
- (2) The Registrar may, in addition to any power he may have under the Companies Act, present a petition for the winding up of the Company in circumstances where he may determine, after representations made by the Company or on its behalf or by any Client, that it is expedient in the public interest that the Company be wound up.
- (3) Where a petition for the winding up of the Company is presented by a person other than the Registrar, a copy of the petition shall be served on the Registrar, and he shall be entitled to be heard on the petition.
4. Notwithstanding any statutory provisions or any rule of law to the contrary, on the commencement of proceedings to wind up the Company: Obligations of Liquidator

- (a) the liquidator shall be bound to recognize the separate nature of each Segregated Account and the Contracts pursuant to the provisions of this Act and shall not apply the property identified as the property of any one Segregated Account (including any interest in a mixed fund or converted or combined property where property may have been commingled) to pay the claims of general creditors of the Company;
- (b) if required under the terms of a Contract, the liquidator shall preserve the property in such Segregated Account and ensure, where applicable, the assets therein held are permitted to mature as required for the benefit of the related Client;
- (c) the liquidator shall be bound to observe, and shall have no power to vary or cancel, the terms of any Contract nor any deed, contract or agreement between the Company and any other person with respect to any Contract or, Segregated Account;
- (d) transfers of property from a Segregated Account to the Client to whom the Segregated Account relates, whether pursuant to a Contract, the bye-laws of the Company, or otherwise, shall not constitute nor be deemed to be a fraudulent preference or a fraudulent conveyance, nor constitute business of the Company being carried on with intent to defraud creditors of the Company or creditors of any person or for any fraudulent purpose, for the purposes of any statute or law relating to bankruptcy or insolvency; and
- (e) to the benefit of the relevant Client the remedies of tracing in law and in equity shall apply to the property and the proceeds of the property of any Segregated Account where such property or proceeds may have been commingled.

SCHEDULE V
DATA PROTECTION

1. Interpretation

“Data” means representations of information or of concepts in any form;

“Data Controller” means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed;

“Data Processor” means, in relation to Personal Data, any person (other than an employee of a Data Controller) who processed that data on behalf of such Data Controller;

“Data Protection Authorities” means the authorities in a member state of the European Union responsible for regulating compliance with EU Data Protection Law;

“Data Protection Officer” means the individual who shall be an officer of the Company appointed as the Data Protection Officer for the purposes of this Schedule;

“Data Protection Principles” means the principles set out in Part I of this Schedule;

“Data Subject” means an individual who is the subject of Personal Data;

“Directive” means legislation adopted by the European Parliament and Council which is to later be brought into effect in each member state of the European Union by means of its own national legislation;

“Onward Data Controller” means another Data Controller to whom the Data Controller has forwarded Data as permitted by the Directive;

“Personal Data” means Data which have been sent (whether transmitted directly or indirectly by third parties) by an EU Data Controller to the Company and that were received by the Company and which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, the Data Protection Officer, and includes any expression of opinion about the individual and any indication of the intentions of the EU Data Controller or any other person in respect of the individual.

The Data Protection Principles are to be interpreted in accordance with Part 2 of this Schedule.

Part 3 of this Schedule (which applies to all Personal Data) and Part 4 of this Schedule (which applies only to Sensitive Personal Data) set out conditions applying for the purposes of the first principle; and Part 5 of this Schedule sets out cases in which the eighth principle does not apply.

Subject to section 13(l), it shall be the duty of the Company's Data Controller to comply with the Data Protection Principles in relation to the processing of Personal Data.

2. (1) The Company shall appoint a suitably qualified Officer to the post of Data Protection Officer, and shall take such steps that are necessary from time to time to ensure that such post is not vacant.
- (2) The Data Protection Officer shall be responsible for ensuring that the Company's Data Controller complies with the Data Protection Principles and other obligations imposed in this Schedule. The Data Protection Officer
- (3) The Data Protection Officer shall represent the Company with regard to the processing by it and all Data Controllers of Personal Data and will be responsible for liaising with Data Protection Authorities, EU Data Controllers and Onward Data Controllers in respect of the Company's obligations under this Schedule. The Company shall ensure that all such persons are made aware of the address (postal address and internet protocol address) and identity of the Data Protection Officer.
- (4) The Data Protection Officer shall represent the Company (including for the avoidance of doubt, all the Company's Data Controllers) with regard to the performance of its obligations to Data Subjects under this Schedule.
- (5) In relation to the Company's Data Controllers, the Data Protection Officer shall:
 - (a) maintain an accurate register in accordance with section 6 below;
 - (b) notwithstanding the legal force and effect of the obligations imposed on Clients of the

Company that are the Company's Data Controllers by virtue of this Act, ensure that all such Data Controllers are adequately bound to comply with all obligations hereunder having regard to the lawful and secure processing of Personal Data and the availability of remedies to the Company and/or any EU Data Controller and any Data Subject in the event of non-compliance with this Part by such Data Controllers;

- (c) monitor the activities of the Company's Data Controller and ensure that regular reviews of the processing of Personal Data by the Company's Data Controller is undertaken in order to audit continuing compliance with the Company's obligations hereunder;
 - (d) advise the Company's relevant Data Controller as far as is practicable of any measures to which certain EU Data Controllers are subject under EU Data Protection Law that may have a bearing on the Company's compliance with section 5; and
 - (e) promptly and appropriately exercise the powers granted to him under section 7 in the event of a breach by the Company's Data Controller of its obligations hereunder.
- (6) For the purposes of compliance with subsection (5)(b) the Company's Data Controller shall be deemed to be adequately bound if an appropriate undertaking is provided in a Contract with a Client.
- (7) For the purposes of subsection (3) the Data Protection Officer shall be responsible for approving the terms on which Onward Data Controllers are to be contractually obliged to protect any Personal Data which has been transmitted by the Company's Data Controller. Such terms must provide an adequate level of protection for Personal Data having regard to the eighth principle of the Data Protection Principles and the Data Protection Officer shall ensure that such terms are reviewed in the light of any requirement of an EU Data Controller or guidance received from an EU Data Controller or a Data Protection Authority.

3. (1) Where a Client is pursuant to a Contract acting as a Data Controller

Data Controller such Client shall appoint an appropriately qualified employee or agent who shall be responsible for ensuring that such Client complies with their obligations under this Schedule and this Act.

- (2) The identity of the employee or agent appointed pursuant to subsection (1) shall be notified to the Data Protection Officer and such employee or agent shall be responsible for liaising with the Data Protection Officer with regard to the processing of Personal Data by the relevant Client and such employee or agent shall promptly notify the Data Protection Officer of any breach, whether actual, suspected or anticipated of the obligations under this Schedule of such Client.
 - (3) The Data Controller shall promptly provide all information and assistance required by the Data Protection Officer in his performance of all obligations imposed on the Company in this Schedule.
 - (4) The Data Controller will ensure that all processing of Personal Data is undertaken in accordance with requirements of the EU Data Controller who disclosed such Personal Data and shall abide by any restrictions on the processing of such Personal Data issued by such EU Data Controller.
 - (5) The Data Controller will ensure that any Onward Data Controllers including but not limited to Clients, who receive Personal Data from the Company enter into Contracts with the Company on terms approved by the Data Protection Officer under section 1(7).
 - (6) Without prejudice to the foregoing it shall be a term of any Contract between the Company and a Client that any Client will fully compensate the Company for all loss and damage (whether caused directly or indirectly), expenses (legal or otherwise) and third party claims flowing from any breach by such Client of its obligations imposed by this Schedule.
4. If a Data Controller fails to comply with the Data Protection Principles, or any provision of this Part, and a Data Subject or an EU Data Controller suffers damage as a result of such non compliance by such Data Controller, the Data Subject or EU Data Controller shall have a claim against the Company for such non compliance; provided however, that with regard to all such claims the provisions relative to limitation of liability set out in Section 16 of the Act shall apply to any such claim and

Right to
Compensation

the relevant person liable for these purposes shall be the Client by whom the Personal Data was processed in breach of the provisions of this Schedule.

- | | | | |
|----|-------|---|----------------------------------|
| 5. | (1) | All rights conferred on a Data Subject under this Act may be exercised by the EU Data Controller who disclosed to the Company the Personal Data containing information regarding such Data Subject. | Rights of EU
Data Controllers |
| | (2) | The Company will provide, upon request, reasonable assistance to any EU Data Controller who requests assistance of the Company in ensuring that such EU Data Controller is in compliance with EU Data Protection Law, in relation to Personal Data disclosed by such EU Data Controller to the Company. | |
| 6. | (1) | The Data Protection Officer shall maintain or cause to be maintained a register in relation to each of the Company's or any Client's Data Controller which shall comprise: | Data Register |
| | (i) | a general description of the Personal Data to be received by the Company from an EU Data Controller; | |
| | (i) | the category or categories of Data Subject to which the Personal Data to be received from each EU Data Controller relates; | |
| | (ii) | a description of the purpose or purposes for which the Personal Data are being or are to be processed; | |
| | (iii) | description of any recipient or recipients to whom the EU Data Controller intends or may wish the Company's Data Controller to disclose the Personal Data; | |
| | (iv) | the names or description of any countries outside the European Economic Area (other than Bermuda) to which the EU Data Controller intends the Company's relevant Data Controller to directly or indirectly transfer the Personal Data. | |
| | (2) | Where the Company enters into a contract with an EU Data Controller which requires the EU Data Controller | |

to provide to the Company or any Client the information required under subsection (1), the Company will be entitled to assume that such information is accurate and complete for the purposes of subsection (1) except to the extent that the relevant Data Controller is, or ought reasonably to be, aware that such information is inaccurate or incomplete.

7. (1) Notwithstanding the provisions of any Contract with a Client, the Company may require a Data Controller to take appropriate measures to comply with the Data Protection Principles, and the rights conferred on EU Data Controllers and Data Subjects under this Act. Powers of the Data Protection Officer
- (2) If a Data Controller fails to comply with an instruction from the Data Protection Officer under subsection (1), the Company shall be entitled to terminate and suspend the operation of the relevant Contract (if any) and, if the non-compliance by the relevant Data Controller continues for more than 10 days following the suspension of the operation of the Client Contract, to terminate the Contract.
- (3) Notwithstanding the terms of any Contract, if the relevant Data Controller fails to comply with any obligation imposed on it under this Schedule, the Company is empowered to take all necessary steps to fulfil the obligation on behalf of the relevant Data Controller.
- (4) A Data Protection Officer shall be responsible for ensuring that the obligations imposed on the Company or a Client (as the case may be) under this Schedule are performed in respect of all Personal Data processed by the relevant Data Controller (including Personal Data processed by the Company on behalf of a Client) and in the event of non-compliance shall be entitled to take all necessary steps to ensure compliance without recourse to such Data Controller or the Company.
8. (1) Subject to the following provisions of this section and to section 9 a Data Subject is entitled: Right of access to Personal Data
- (a) to be informed by the Company or the Client (as the case may be) whether Personal Data of which that individual is the Data Subject are being processed by or on behalf of the appointed Data Controller of the Company or

the Client (as the case may be).

- (b) if that is the case, to be given by the relevant party a description of:
 - (i) the Personal Data of which that individual is the Data Subject;
 - (ii) the purposes for which they are being or are to be processed; and
 - (iii) the recipients or classes of recipients to whom they are or may be disclosed.
 - (c) to have communicated to him in an intelligible form:
 - (i) the information constituting any Personal Data of which that individual is the Data Subject; and
 - (ii) any information available to the Company or the Client (as the case may be) as to the source of those data; and
 - (d) where the processing by automatic means of Personal Data of which that individual is the Data Subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the Company or the Client (as the case may be) of the logic involved in that decision-taking.
- (2) Neither the Company nor the Client is obliged to supply any information under subsection (1) unless it has received a request in writing or by way of an electronic Record.
 - (3) Neither the Company nor the Client is obliged to comply with a request under this section unless it is supplied with such information as he may reasonably require in order to satisfy itself as to the identity of the person making the

request and to locate the information which that person seeks.

- (4) Where the Company or a Client cannot comply with the request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless:
 - (a) the other individual has consented to the disclosure of the information to the person making the request; or
 - (b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual.
- (5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request and that subsection is not to be construed as excusing the Company from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by the omission of names or other identifying particulars or otherwise.
- (6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular to:
 - (a) any duty of confidentiality owed to the other individual;
 - (b) any steps taken by the Company with a view to seeking the consent of the other individual;
 - (c) whether the other individual is capable of giving consent; and

(d) any express refusal of consent by the other individual.

(7) A Data Subject making a request under this section may, specify that his request is limited to Personal Data of any description.

(8) Subject to subsection (4), the Company shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.

(9) In this Section:

“the prescribed period” means forty days or such other period as may be prescribed;

“the relevant day”, in relation to a request under this section, means the day on which the Company receives the request or, if later, the first day on which the Company has the information referred to in subsection (3).

9. (1) The obligation imposed by section 8(1)(c)(i) must be complied with by supplying the Data Subject with a copy of the information in permanent form unless:
- (a) the supply of such a copy is not possible or would involve disproportionate effort; or
- (b) the Data Subject agrees otherwise;
- and where any of the information referred to in section 8(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.
- (2) Where the Company has previously complied with a request made under section 8 by an individual, the Company is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.
- (3) In determining for the purposes of subsection (2) whether requests under section 8 are made at

Provisions
Supplementary
to Section 8

reasonable intervals, regard shall be had to the nature of the Data, the purpose for which the Data are processed and the frequency with which the Data are altered.

- (4) Section 8(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in any decision taking if, and to the extent that, the information constitutes a trade secret.
 - (5) The information to be supplied pursuant to a request under section 8 must be supplied by reference to the Data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.
 - (6) For the purposes of Section 8(4) and (5) another individual can be identified from the information being disclosed if he can be identified from that information, or from any other information which, in the reasonable belief of the Company, is likely to be in, or to come into, the possession of the Data Subject making the request.
10. (1) Subject to subsection (2), a Data Subject is entitled at any time by notice in writing to the Company to require the Company's Data Controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any Personal Data in respect of which he is the Data Subject, on the ground that, for specified reasons:
- (a) the processing of those Data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another; and
 - (b) that damage or distress is or would be unwarranted.
- (2) Subsection (1) does not apply in a case where any of the conditions in paragraphs 1 to 4 of part 2 is met.
- (3) The Company must within twenty-one days of

Right to prevent processing likely to cause damage or distress

receiving a notice under subsection (1) (the “Data Subject Notice”) give the individual who gave it a written notice:

- (a) stating that it has complied or intends to comply with the Data Subject Notice; or
 - (b) stating its reasons for regarding the Data Subject notice as to any extent unjustified and the extent (if any) to which it has complied or intends to comply with it.
- (4) The failure by a Data Subject to exercise the right conferred by subsection (1) or section 11 (1) does not affect any other right conferred on him by this Part.
11. (1) A Data Subject is entitled at any time by notice in writing to the Company to require the Company’s Data Controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing Personal Data in respect of which he is the Data Subject. Right to prevent processing for purposes of direct marketing
- (2) In this section “direct marketing” means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.
12. (1) A Data Subject is entitled at any time, by notice in writing to the Company, to require the Company to ensure that no decision taken by or on behalf of the Company's Data Controller which significantly affects that Data Subject is based solely on the processing by automatic means of Personal Data in respect of which that Data Subject is the Data Subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct. Rights in relation to automated decision-taking
- (2) Where, in a case where no notice under subsection (1) has effect, a decision which significantly affects a Data Subject is based solely on such processing as is mentioned in subsection (1):
- (a) the Company must as soon as reasonably practicable notify the Data Subject that the decision was taken on that basis; and

- (b) the Data Subject is entitled, within twenty-one days of receiving that notification from the Company, by notice in writing to require the Company's Data Controller to reconsider the decision or to take a new decision otherwise than on that basis.
- (3) The Company must, within twenty-one days of receiving a notice under subsection (2)(b) ("the Data Subject Notice") give the Data Subject a written notice specifying the steps that he intends to take to comply with the Data Subject notice.
- (4) A notice under subsection (1) does not have effect in relation to an exempt decision; and nothing in subsection (2) applies to an exempt decision.
- (5) In subsection (4) "exempt decision" means any decision in respect of which the condition in subsection (6) and the condition in subsection (7) are met.
- (6) The condition in this subsection is that the decision:
 - (a) is taken in the course of steps taken:
 - (i) for the purpose of considering whether to enter into a contract with the Data Subject;
 - (ii) with a view to entering into such a contract;
 - (iii) in the course of performing such a contract; or
 - (b) is authorised or required by or under any statutory provision.
- (7) The condition in this subsection is that either:
 - (a) the effect of the decision is to grant a request of the Data Subject; or
 - (b) steps have been taken to safeguard the legitimate interests of the Data Subject (for example, by allowing him to make representations).

13. (1) References in any of the Data Protection Principles set forth in Part I or any provision of this Schedule to Personal Data or to the processing of Personal Data do not include references to data or processing which by virtue of this Part are exempt from that principle or other provision. Exemptions
- (2) In this section and sections 14 and 15 “the subject information provisions” means:
- (a) the first Data Protection Principle to the extent to which it requires compliance with paragraph 2 of Part 2; and
- (b) Section 9.
- (3) In this section and in sections 14 and 15, “the non-disclosure provisions” means the provisions specified in subsection (4) to the extent to which they are inconsistent with the disclosure in question.
- (4) The provisions referred to in subsection (3) are:
- (a) the first Data Protection Principle, except to the extent to which it requires compliance with the conditions in Parts 3 and 4;
- (b) the second, third, fourth and fifth Data Protection Principles; and
- (c) section 10.
14. Personal Data are exempt from: Information available to the public by or under enactment
- (a) the subject information provisions;
- (b) the fourth Data Protection Principle; and
- (c) the non-disclosure provisions;
- if the Data consist of information which the Company is obliged by or under any statutory provision to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.
15. (1) Personal Data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by an order of the Disclosures required by law or made in

court.

connection with
legal proceedings etc

- (2) Personal Data are exempt from the non-disclosure provisions where the disclosure is necessary:
- (a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings); or
 - (b) for the purpose of obtaining legal advice;
- or otherwise necessary for the purposes of establishing, exercising or defending legal rights.

PART I
THE DATA PROTECTION PRINCIPLES

1. Personal Data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
 - (a) at least one of the conditions in Part 3 is met; and
 - (b) in the case of Sensitive Personal Data, at least one of the conditions in Part 4 is also met.
2. Personal Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal Data shall be accurate and, where necessary, kept up to date.
5. Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal Data shall be processed in accordance with the rights of Data Subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or lawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.
8. Personal Data shall not be transferred to a country or territory outside the European Economic Area (except in Bermuda where such transfers (transferors and recipients) are governed by the provisions of this Act) unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.

PART 2
INTERPRETATION OF THE PRINCIPLES IN PART I

The first principle

1. (1) In determining for the purposes of the first principle whether Personal Data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed. For these purposes the relevant Data Controller shall be entitled to rely on appropriate assurances provided by an EU Data Controller.
- (2) Subject to paragraph 2, for the purposes of the first principle Personal Data are to be treated as obtained fairly if they consist of information obtained from a person who:
 - (a) is authorised by or under any enactment to supply it; or
 - (b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on Bermuda or a member state of the European Union.
2. (1) Subject to paragraph 3, for the purposes of the first principle Personal Data are not to be treated as processed fairly unless:
 - (a) in the case of Data obtained from the Data Subject, the relevant Data Controller ensures so far as practicable that the Data Subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3); and
 - (b) in any other case, the relevant Data Controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the Data Subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).
- (2) In sub-paragraph (1)(b) “the relevant time” means:

- (a) the time when the relevant Data Controller first processes the data; or
 - (b) in a case where at that time disclosure to a third party within a reasonable period is envisaged:
 - (i) if the Data are in fact disclosed to such a person within that period, the time when the Data are first disclosed;
 - (ii) if within that period the relevant Data Controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the relevant Data Controller does become, or ought to become, so aware; or
 - (iii) in any other case, the end of that period.
 - (3) The information referred to in sub-paragraph (1) is as follows, namely:
 - (a) the identity of the relevant Data Controller;
 - (b) the purpose or purposes for which the Data are intended to be processed; and
 - (c) any further information which is necessary, having regard to the specific circumstances in which the Data are or are to be processed, to enable processing in respect of the Data Subject to be fair.
3. Paragraph 2(1)(b) does not apply where either of the following primary conditions are met:
- (a) that the provision of that information would involve a disproportionate effort; or
 - (b) that the recording of the information to be contained in the Data by, or the disclosure of the Data by the Company Data Controller is necessary for compliance with any legal obligation to which the relevant Data

Controller is subject, other than an obligation imposed by contract.

The second principle

4. The purpose or purposes for which Personal Data are obtained may in particular be specified in a notice given for the purposes of paragraph 2 by the relevant Data Controller to the Data Subject.
5. In determining whether any disclosure of Personal Data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the Personal Data are intended to be processed by any person to whom they are disclosed.

The third principle

6. Personal Data shall not be treated as used or disclosed in contravention of this principle unless-
 - (a) used otherwise than for a purpose of a description registered under this Schedule in relation to the data; or
 - (b) disclosed otherwise than to a person of a description so registered.

The fourth principle

7. The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in Personal Data which accurately record information obtained by the relevant Data Controller from the Data Subject or a third party in a case where:
 - (a) having regard to the purpose or purposes for which the data were obtained and further processed, the Relevant Data Controller has taken reasonable steps to ensure the accuracy of the data; and
 - (b) if the Data Subject has notified the Relevant Data Controller of the Data Subject's view that the data are inaccurate, the data indicate that fact.

The fifth principle

8. Any question whether or not Personal Data are accurate shall be determined as for the purposes of this Schedule but, in the case of such data as are mentioned in Section 6 (2), this principle shall not be regarded as having been contravened by reason of any inaccuracy in the information there mentioned if the requirements specified in that subsection have been

complied with.

The sixth principle

9. The Company (and for the purposes of Section 7(1), the relevant Company Data Controller) is to be regarded as contravening the sixth principle if, but only if:
 - (a) it contravenes section 9 by failing to supply information in accordance with that section;
 - (b) it contravenes section 10 by failing to comply with a notice given under subsection (1) of that section to the extent that the notice is justified or by failing to give a notice under subsection (3) of that section;
 - (c) it contravenes section 11 by failing to comply with a notice given under subsection (1) of that section; or
 - (d) it contravenes section 12 by failing to comply with a notice given under subsection (1) or (2)(b) of that section or by failing to give a notification under subsection (2)(a) of that section or a notice under subsection (3) of that section.

The seventh principle

10. Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to:
 - (a) the harm that might result from such unauthorised or unlawful processing, or accidental loss, destruction or damage as are mentioned in the seventh principle; and
 - (b) the nature of the data to be protected.
11. The Relevant Data Controller must take reasonable steps to ensure the reliability of any employees of his who have access to the Personal Data.
12. Where processing of Personal Data is carried out by a Data Processor on behalf of the relevant Data Controller, the Data Controller must in order to comply with the seventh principle:
 - (a) choose a Data Processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and

- (b) take reasonable steps to ensure compliance with those measures.

13. Where processing of Personal Data is carried out by a Data Processor on behalf the relevant Data Controller, the relevant Data Controller is not to be regarded as complying with the seventh principle unless:

- (a) the processing is carried out under a contract:
 - (i) which is made or evidenced in writing; and
 - (ii) under which the Data Processor is to act only on instructions from the Data Controller, and
- (b) the contract requires the Data Processor to comply with obligations equivalent to those imposed on the relevant Data Controller by the seventh principle.

The eighth principle

14. An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to:

- (a) the nature of the Personal Data;
- (b) the country or territory or origin of the information contained in the Data;
- (c) the country or territory of final destination of that information;
- (d) the purposes for which and period during which the Data are intended to be processed;
- (e) the law in force in the country or territory in question;
- (f) the international obligations of that country or territory;
- (g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases); and
- (h) any security measures taken in respect of the Data in that country or territory.

15. The eighth principle does not apply to a transfer falling within

any paragraph of Part 5.

16. (1) Where:
- (a) in any proceedings under this Act any question arises as to whether the requirement of the eighth principle as to an adequate level of protection is met in relation to the transfer of any Personal Data to a country or territory outside the European Economic Area; and
 - (b) a Community finding has been made in relation to transfers of the kind in question;

that question is to be determined in accordance with that finding.

- (2) In sub-paragraph (1) “Community finding” means a finding of the European Commission, under the procedure provided for in Article 31(2) of the European Commission Directive 95/46/EC (as amended from time to time), that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of Article 25(2) of that Directive.

PART 3
CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The Data Subject has given his consent to the processing.
2. The processing is necessary:
 - (a) for the performance of a contract to which the Data Subject is a party; or
 - (b) for the taking of steps at the request of the Data Subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligations to which the Data Controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interest of the Data Subject.
5. The processing is necessary:
 - (a) for the administration of justice;

- (b) for the exercise of any functions conferred on any person by or under any enactment;
 - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or
 - (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. The processing is necessary for the purposes of legitimate interests pursued by the relevant Data Controller or by the third party or parties to whom the Data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the Data Subject.

PART 4
CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST
PRINCIPLE:
PROCESSING OF SENSITIVE PERSONAL DATA

1. The Data Subject has given his explicit consent to the processing of the Personal Data.
2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the Data Controller in connection with employment.
- (2) The processing is necessary:
 - (a) in order to protect the vital interests of the Data Subject or another person, in the case where:
 - (i) consent cannot be given by or on behalf of the Data Subject; or
 - (ii) the relevant Data Controller cannot reasonably be expected to obtain the consent of the Data Subject; or
 - (b) in order to protect the vital interest of another person, in a case where consent by or on behalf of the Data Subject has been unreasonably withheld.

3. The processing:
 - (a) is carried out in the course of its legitimate activities by any body or association which:
 - (i) is not established or conducted for profit; and
 - (ii) exists for political, philosophical, religious or trade union purposes;
 - (b) is carried out with appropriate safeguards for the rights and freedoms of Data Subjects;
 - (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and
 - (d) does not involve disclosure of the Personal Data to a third party without the consent of the Data Subject.
4. The information contained in the Personal Data has been made public as a result of steps deliberately taken by the Data Subject.
5. The processing:
 - (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
 - (b) is necessary for the purpose of obtaining legal advice; or
 - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
6. The processing is necessary:
 - (a) for the administration of justice;
 - (b) for the exercise of any functions conferred on any person by or under an enactment; or
 - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
7. (1) The processing is necessary for medical purposes and is undertaken by:

- (a) a health professional; or
 - (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
- (2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
8. The processing:
- (a) is of Sensitive Personal Data consisting of information as to racial or ethnic origin;
 - (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and
 - (c) is carried out with appropriate safeguards for the rights and freedoms of Data Subjects.

PART 5
CASES WHERE THE EIGHTH PRINCIPLE DOES NOT
APPLY

1. The Data Subject has given his consent to the transfer.
2. The transfer is necessary:
 - (a) for the performance of a contract between the Data Subject and the relevant Data Controller; or
 - (b) for the taking of steps at the request of the Data Subject with a view to entering into a contract with the relevant Data Controller.
3. The transfer is necessary:
 - (a) for the conclusion of a contract between the relevant Data Controller and a person other than the Data Subject which:
 - (i) is entered into at the request of the Data Subject; or

- (ii) is in the interests of the Data Subject; or
 - (b) for the performance of such a contract.
- 4. The transfer is necessary for reasons of substantial public interest.
- 5. The transfer:
 - (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
 - (b) is necessary for the purpose of obtaining legal advice; or
 - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- 6. The transfer is necessary in order to protect the vital interests of the Data Subject.
- 7. The transfer is part of the Personal Data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.