Explanatory Memorandum
Electronic Transactions Policy and Bill

Introduction

The Ministry of Public Administration and Information (MPAI), through extensive consultation with the public sector, the private sector and academia, developed ***fastforward***, the National Information and Communications Technology (ICT) Strategy for Trinidad and Tobago. Electronic commerce ("e-commerce") has been identified as an important strategic driver for economic growth, particularly in developing countries. In order to take full advantage of the opportunities for business and consumers that is offered by e-commerce, we must have a clear and predictable legal environment that can be trusted by citizens, institutions and businesses. Two key areas in which legislation is required are Data Protection and Electronic Transactions. The Electronic Transactions Policy forms the basis of the Electronic Transactions Bill, which will be the first stage of the legislative renewal required to fully achieve the objectives of ***fastforward***.

Legislative Approach

Governments around the world have taken common approaches to dealing with the issue of recognizing the validity of electronic documents. Generally speaking, all legislation dealing with electronic transactions or electronic documents states that no document, record or transaction will be found to be invalid solely because it is electronic. The legislation creates **media neutrality**. It is important to note that a transaction may invalid for other reasons—a contract that was entered into under duress will be no more valid if electronic than it were written on paper. A document that is irrelevant to a legal proceeding will be excluded as evidence by a court whether it is electronic or paper. The provisions regarding validity do not grant any greater evidentiary weight to electronic documents than to paper documents. The Bill does not give electronic documents any greater certainty than paper documents and basic contract law is not changed by electronic transactions legislation.

Governments have also adopted the basic concept of **functional equivalence** found in the United Nations Commission on Trade and International (UNCITRAL) Model Law on Electronic Commerce: where statutory language assumes the use of a paper document or paper-based transaction (e.g., by using a term such as "signature" or requiring the retention of records), the electronic transactions legislation will set out the criteria or tests that have to be met for electronic technology to fulfill the functions of the paper-based requirement. For example, one of the functions of providing individuals with paper copies of transactions is so they can review, re-read, and store them for future reference. If electronic technology allows for retention and storage for future reference and allows an electronic document to be printed, then it is functionally equivalent. Also following the UNCITRAL Model Law, most electronic transactions legislation is **technologically neutral**. While it may set out criteria to determine functional equivalencies, it does not state what technology will satisfy the criteria since this may change as time goes by.

Most of the provisions of the Policy and Bill are *enabling*: they allow for a particular legal effect but do not impose regulatory requirements. People have a choice as to whether they will use electronic transactions, conduct business electronically, negotiate contracts through e-mail, or use e-government portals to download forms or file electronic documents with the government. Nothing in the Policy or the Electronic Transactions Bill changes the basic law of contract. The essential objective of the Policy and Bill is to allow individuals and businesses to use electronic communications for personal and commercial purposes while knowing that their communications and transactions will have the same protections in court as paper documents.

In some cases, however, the Bill does create regulatory requirements that impose duties and responsibilities on certain persons dealing in the electronic environment of e-commerce. There are regulatory provisions with respect to:

- Certified electronic signature providers;
- Accredited electronic signatures;
- Persons doing business with consumers online;
- Internet service providers and other intermediaries; and
- Persons who send unsolicited electronic communications ("spam") with a connection to Trinidad and Tobago.

Generally speaking, the Policy and Bill embody a "light touch" co-regulatory approach. **Co-regulation** is a form of regulation where both government and private sector parties (e.g., industry, industry organizations, consumer groups, and other interested parties) have roles to play in achieving the objectives of regulation. It is based on the premise that both government and the private sector have different, but often complementary, strengths, and that the most effective regulatory regime draws on all the resources available.

Thus, government has available the power of the law, including the power to impose regulation, set regulatory requirements and enforce the law. Private industry, on the other hand, knows more about the capacities and nature of the industry—in some cases, such as in the high tech industry, the cutting edge expertise needed to completely understand the technical issues involved in a particular matter simply may not be available within government. To look only to government as a source of monitoring for compliance with regulatory requirements would mean that the important job of enforcement would be badly done, with a negative impact on not only the regulatory regime but also on the reputation and integrity of government as a whole. Also government alone may not be the best source of the development of legally enforceable rules in highly technical matters, such as appropriate security requirements for electronic signatures.

Many of the areas where some form of co-regulation (or supervised self-regulation) has developed are those where government lacks the capacity for a full-fledged regulatory system and must rely, as a practical matter, on industry to take a co-operative and complementary enforcement role. The securities industry is a prime example where self-regulatory organizations, such as stock exchanges, share regulatory responsibilities with specialized government oversight bodies, a securities commission.

Experience has also shown, however, that government must maintain a monitoring capacity and the willingness to take enforcement action in a co-regulatory regime. Co-regulation does not mean that government abdicates responsibility for the achievement of public policy objectives. The regulatory structures described in the Policy and set out in the Bill have complementary roles for government and the private sector. The private sector, for example, will be expected to do the following:

- Work with government and interested stakeholders (e.g., consumers, suppliers, community groups or others) to develop codes of conduct that will guide behaviour in a much more detailed way than would be provided in the legislation and that would be tailored to the particular circumstances of the industry and the needs of stakeholders. Codes of conduct may cover such matters as information to be provided to customers, dispute resolution mechanisms, service standards and remedies.
- Work with government and interested stakeholders to identify good business practices and promote them within the business community.
- Educate the industry in the requirements of the law and, in particular, provide a source of advice to small business that may be disadvantaged in dealing with a co-regulatory system that imposes responsibilities on business.
- Work with government and interested stakeholders to educate consumers about their rights, about what they should expect in terms of good business practices, and how disputes may be resolved in a less formal forum than the courts.
- Develop internal compliance and reporting systems and promote good governance within their own companies to ensure that the requirements of the law and industry codes of conduct, including best practices, are met.

Government would continue to have responsibility for monitoring compliance with the law, enforcing the law through prosecutions if appropriate, and promoting compliance with the law through education and capacity building. In some cases, the government may have to work with industry leaders to build and strengthen industry organisations to take over a strong co-regulatory role. It should be noted, however, that government will not overlook any anti-competitive behaviour that might be thought to be encouraged by the prospect of industry members working together to establish industry organisations and play a regulatory role. Government will continue to be alert to this possibility and keep the concept of the public interest in the forefront when working with industry to develop codes of conduct and establish the capacity for industry monitoring and enforcement of compliance with codes. In most cases, government anticipates that codes of conduct will be voluntary in nature, although the courts may look to industry codes as evidence of appropriate behaviour in an industry when interpreting the law. In some cases, codes of conduct may have a particular legislative base, such as a code dealing with Internet service providers and intermediaries, with legal consequences for failure to comply with the requirements set out in the code.

Consumers, suppliers, employees and other stakeholders have roles to play in a co-regulatory scheme and government may have to work with these stakeholders to improve their capacities to participate effectively. In particular, identifying good business

practices and establishing reputable mechanisms to settle disputes may require input and active participation from stakeholders who are outside of industry.

In sum, co-regulation is intended to take advantage of the strengths, expertise and resources of industry and other stakeholders. It is not to be confused with self-regulation where there is no legislative base for regulatory requirements (although industry members may by contract impose requirements on themselves) or where government does not have the ultimate responsibility and power to set legal requirements and enforce the law.

Principles of the Policy and the Bill

Principle 1: General Provisions

1.1 Definitions

The definitions of "addressee," "originator" and "intermediary" are linked in that the intention is to make clear that activities of an intermediary, such as an Internet service provider, are separated from the intentions and activities of those who originate an electronic communication or transaction and those to whom it is addressed or receive it. In this sense, the intermediary may be thought of as analogous to a common carrier who merely transmits information but who cannot be considered as being intended to receive it or send it for its own communications purposes.

"Certificate" is the terminology that refers to the attestation that "certifies" that particular data is linked to a signatory of an electronic signature and consequently verifies that the signatory is the source of the electronic signature—i.e., "signed" the signature.

The definition of "consumer" is intended to capture the concept of a person who purchases for use rather than to sell again. It is broader than the EU definition, which is limited to an individual or a natural person, since it seems advisable to consider the situation of business buying supplies for its own use. Where a major business is dealing with a large supplier, the provisions would likely be redundant since the larger business would doubtless be aware of the address and contact information of its supplier. A smaller business dealing on the internet, however, would be in essentially the same position as an individual purchasing an item for personal use. The language is drawn from the definition used in the Saint Vincent and the Grenadines *Electronic Transactions Act, 2004*. That Act does limit the definition to a natural person. It should be noted, however, that the Saint Vincent and the Grenadines legislation embodies a more complete code of consumer protection that deals with matters that in Trinidad and Tobago are the subject of a separate legislative initiative. In light of the limited purposes of the consumer information provisions in the Electronic Transactions Policy and Bill, the broader definition is appropriate.

The definition of "electronic" is deliberately broad and is based on the New Zealand (and indirectly, the Australian) legislation. It includes technologies that might not initially be considered as electronic, such as optical, biometric, and photonic technologies. The goal is to avoid limiting the application of the Policy and the Bill inappropriately.

An “electronic agent” is not related to the law of agency as it has no legal personality; it is a machine or program using a machine (e.g., computer) that performs a particular communication function without review by an individual at the time it happens. For example, when an individual programmes his email function to send an email automatically replying to an incoming email and stating that the individual is away on holiday, an electronic agent is being used.

“Electronic record” should be read in conjunction with “information” and transaction. The intention is that substantially all electronic transactional/communication activities should be covered by the broad usage.

The term “electronic signature” deals with the basic functions of electronic signatures. In some jurisdictions, there are qualifiers that in this Policy and Bill are placed in the text to indicate criteria of reliability and integrity, but which are not in themselves necessary for a definition. By not including them in the definition, the essential concept of an electronic signature maintains the flexibility to allow persons to choose the level of reliability and integrity that suit their purposes, subject to legal requirements.

The terms “originator,” “addressee” and “intermediary” are drawn from the UNCITRAL Model Law and are reflected in language used in a number of jurisdictions. See commentary above regarding “addressee.”

“Information” and “record” are also defined broadly and intended to capture all forms of electronic communication.

The concept of a “public authority” is drawn from legislation in Ontario, Saint Vincent and the Grenadines (“public authority”) and the Trinidad and Tobago *Freedom of Information Act. 1999*, and indicates that both the clarifications provided by the general enabling provisions and the authority provided by Principle 7 in this Policy and Bill apply to non-private entities broadly. Thus an agency or corporation or other entity that is not part of a ministry but that operates in a more independent and arm’s length fashion would have the benefit of the legislative protections and authorizations. The intention is that the definition could be further refined by order of the Minister to ensure clarity, for example, where a mixed enterprise corporation was created. The specific language is drawn almost entirely from the *Freedom of Information Act, 1999*. Inclusion of the courts provides specific authority to introduce case management and IT tools that will improve efficiency and effectiveness of adjudication and the court process.

“Signatory” relates to a natural person who signs an electronic signature. Like a handwritten signature, it is done by a human being, although it may be done on behalf of a corporation or other form of person (e.g., a trust, partnership, other body corporate) by an authorized natural person. This allows the linkage of authenticity and authorization to continue, although in a technical sense one might assign an electronic signature to a corporation or other institution or even to an electronic agent since the physical act of signing and the physical attributes of a handwritten signature are absent. At this point in time of the evolution of electronic signatures, however, it seems advisable to continue the

human linkage to better protect the integrity of the process, although the technical neutrality will continue since this does not otherwise limit the technology to be used.

The term “transaction” is broad, but not so broad as to include all possible activities and interactions. It deals with both commercial and non-commercial or personal transactions and the language is based on the New Zealand and Australian legislation. The UNCITRAL Model Law was focused on commercial transactions, but the trend in more recent legislation (e.g., since 2000) has been to deal with both commercial and non-commercial transactions since there did not seem to be any compelling reason to exclude non-commercial transactions or communications from the ambit of the certainty and protection provided by the legislation.

1.2 Binding the State

It is important that the Policy and the Bill apply to the Government of Trinidad and Tobago. The Government will be one of the most important users of electronic documents, not only in the conduct of its own affairs, but also in its role as prosecutor and enforcer of the law in the courts. Effective regulatory systems will use electronic record keeping more often in the future, as well as relying on electronic systems to identify compliance trends. In addition, there are particular provisions (Principle 7) that specifically authorize government to do business electronically, thus enabling the introduction of e-government.

1.3 Exclusions

There are some areas where it may not be appropriate to replace paper documents with electronic documents. Generally, these deal with matter where it may be important to have only one original copy of a document or where the formality of affixing a signature to a document may be considered important, or both. For wills and trusts and powers of attorney, both are important. For centuries the unique character of land as a form has been recognized by requirements that contracts dealing with the sale and transfer of land should be in written form. This provision does not exclude the possibility, however, that an electronic land titles system might be developed—as has been done in a number of jurisdictions (e.g., Ontario, Canada) where the land registry is kept electronically. Even in these jurisdictions, the actual contracts of purchase and sale of real property are written and hand-signed.

Wills or other testamentary documents, powers of attorney and documents dealing with the sale or transfer of real property or land are common exclusions in a number of jurisdictions. Some jurisdictions also include other matters, such as notices to disconnect utilities (particularly in jurisdictions with harsh weather conditions where lack of heat or electricity, for example, could cause extreme hardship or death) or documents dealing with adoptions or domestic agreements (e.g., divorce settlements or separation agreements). The provisions dealing with citizenship, immigration and passport documents are not yet common in legislation of this nature, but have become a matter of concern in light of recent developments with terrorism and identity theft. The emphasis here is then on the ability to produce original paper documents.

An additional exclusion that may be of importance is one that is found in several jurisdictions (e.g., Saint Vincent and the Grenadines, Ontario and British Columbia in

Canada, and Singapore): negotiable instruments. The Guide to Enactment of the UNCITRAL Model Law does note that the requirement that cheques be in writing is subject to the Geneva Convention 1931 on a Uniform Law for Cheques. It was felt at this time that this matter deserved some particular attention and consultation and that the provision that would allow the Minister to amend the list of excluded matters would be sufficient safeguard to allow for future refinements, such as the addition of negotiable instruments.

Other matters that are excluded in some jurisdictions include documents dealing with domestic contracts (e.g., pre-nuptial agreements, marriage contracts, divorce and separation agreements and documents relating to adoption). This is another area where additional consultation may be required to determine whether the list should be expanded by regulation.

1.4 Removals from the exclusion list

The intention of the Policy and Bill is that maximum flexibility be retained. Future technology or social change may make the proposed list of exclusions inappropriate and a relatively simple approach to changes, accompanied by appropriate safeguards, maintains that objective.

1.5 Voluntary use of electronic transactions

The general purposes of the Policy and Bill are to enable the use of electronic communication and encourage e-commerce. This provision makes clear that this use is voluntary and while private parties to a transaction may require electronic communication, it is not required by law. In some legislation, there are specific provisions that government may not require electronic communication by citizens with government. This would appear to be redundant in light of the clear provisions that electronic transactions are voluntary and such a provision would not bind future parliaments.

1.6 Consent may be inferred

Consent to communicate electronically need not be explicit but may be inferred from the circumstances. For example, if an individual writes by e-mail or sends a fax to another individual or a company asking for some information, it would be reasonable to infer that the individual has consented to receiving the information electronically. If they send a handwritten letter but provide an e-mail address in the letter, it may also be reasonable to infer that a reply may be sent by e-mail. Allowing consent to be inferred not only eliminates the need for unnecessary communication but also reduces the opportunities for after-the-fact bad faith repudiation. This provision is found in a number of statutes, including Ontario, British Columbia and the Federal Government in Canada, New Zealand and Australia.

1.7 Express consent required for government

E-government is an important part of the ***fastforward*** strategy and an important part of this Policy and Bill are the provisions that give authority to Government to conduct business electronically. In practice, e-government in the sense of providing services and interacting actively with citizens will be implemented over time. The provision that

express consent is required for government is included so that there will be no confusion about when government is "ready to do business" in a particular area electronically. Citizens will not be able to argue that because government places information on a website about licensing requirements for a new business (as it should as quickly as possible), that it should be in a position to take applications for a licence electronically (as it eventually will be able to do). There will be no question that the provision of information could be considered to imply the ability to do more electronically until government is in a position to positively state that fact. This thus allows government to incrementally implement electronic service delivery and to have greater control over the format with which it will communicate interactively with citizens. This technique of express consent has been used in Canada federally and in Ontario, although the means of communicating willingness to do business electronically have differed. This approach is also used in Saint Vincent and the Grenadines, and Bermuda (in terms of drafting, this provision in Bermuda is associated with the provision binding the Crown, similar to Principle 1.2, above). The Federal Government in Canada will add statutes to a schedule by order as it becomes possible to do business electronically pursuant to those statutes. Since more than one government programme may be authorized by a particular statute, it may be advisable to simply make particular services available online as capacity evolves.

New Zealand is an example of a jurisdiction that has not used this approach but instead has suggested that government departments and other recipients of statutory communications should issue guidelines regarding the form and format of the electronic communications they would be prepared to receive; it could then be inferred that they would not receive communications that did not conform to the guidelines. This approach appears to be less precise than the provisions requiring explicit consent and would place pressure on government ministries to produce guidelines prior to the enactment of legislation.

1.8 Certain legal requirements continue

There are some legal provisions that expressly prohibit electronic communication or that require the display or posting of information in written form. For example, government may require that certain information about the law or about health and safety procedures in the workplace be physically posted in a prominent place. Having this information available in electronic form would not meet the policy objectives of education and readily available information that are provided by a poster. Neither the Policy nor the Bill would change this. Similarly, some legislation might require certain notices to be given to the public in a particular way (e.g., by advertisement in a newspaper). This also would continue. This provision is found in legislation in Ontario and British Columbia in Canada; a similar provision is found in the New Zealand legislation, although the legal requirements that continue in force are scheduled in the legislation.

Principle 2: Requirements for Legal Recognition

This Principle is essentially based on the media neutrality and functional equivalence provisions of the UNCITRAL Model Law and form the core of modern electronic transactions legislation. All the jurisdictions that were examined and formed the basis of

this Policy and the Bill use some form of this language, as well as jurisdictions that were not actively used in the preparation of this Policy and Bill.

The Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce sets out the rationale for the functional approach:

> The Model Law is based on the recognition that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication….[C]onsideration was given to the possibility of dealing with impediments to the use of electronic commerce…by way of an extension of the scope of such notions as "writing", "signature" and "original", with a view to encompassing computer-based techniques. …[T]he electronic fulfillment of writing requirements might in some cases necessitate the development of new rules….(para. 15)
>
> The Model Law thus relies on a new approach, sometimes referred to as the "functional equivalent approach", which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions served by a paper document could be fulfilled through electronic-commerce techniques….(para. 16)

2.1 Legal recognition of electronic transactions

This principle states that an electronic document, record or information may have legal effect; that is, the mere fact that it is electronic does not deny it legal effect. It should be noted that this provision does not give any greater importance, security, authority or authenticity to an electronic document, record etc. than might be given to a paper one or to transactions consisting of paper records. Thus, an electronic document may not be admissible in court because its authenticity cannot be proven or the court may determine that the electronic information is otherwise unreliable: it is possible to lie electronically as well as in writing. Similarly, an electronic record may be excluded from evidence because it is not relevant to the proceeding, just as a paper document would be in the same circumstances.

2.2 Writing

A basic function of writing is memory. If an electronic document or record is accessible and can be used for subsequent reference, then it performs the same memory-like function of a paper document or record. The user can retrieve the document, read it, print it, store it, etc. It may be noted here that the electronic record is not necessarily better than a paper one: the Policy or the Bill do not state how long the electronic information has to be usable, although a reasonableness element may be inferred. Just as paper may decay, so may an electronic record. If there are other retention requirements, however, that relate to the electronic document in question (e.g., archival requirements, business record retention requirements), then the electronic record would have to satisfy that rule too to be considered compliant with principle 2.2.

The UNCITRAL Guide to Enactment also notes that writing can be considered the lowest point on a hierarchy of documents that may also be subject to legal requirements for signatures, witnessed signatures and so on. These matters are dealt with in other provisions of the Policy and the Bill, with an emphasis on flexibility for parties to

themselves decide what higher level of security or authenticity they require or for government to define its requirements more precisely in the electronic context.

2.3 Provision of information

This provision deals with sending of information (to a person who consents to receive information electronically, either explicitly or implicitly) and notes that this requirement can be met through the electronic provision of information. It also provides an elaboration on the provisions of principle 2.2 in that the information must be capable of being retained. It is not enough to refer someone to an electronic source of the information if there is otherwise some legal obligation to provide the information. The main reason for this latter point is that the information on a website may not necessarily be "saveable," printable or otherwise capable of being retained and it also shifts the responsibility that has been imposed by law to search and provide information to the user, who may or may not be able to access the correct information.

2.4 Specified non-electronic form

The emphasis here is on form or format (rather than on public posting as, for example, in the requirements noted in 1.7). Again, remembering that willing to receive the information in electronic form is consensual, the point is to maintain the functional equivalence of the format as well as meeting the retention requirements that are functionally equivalent for a written record (principle 2.2). It should be noted that this provision should not be considered as preventing the use of formatting codes, which are common in electronic data interchange systems. Information can be transmitted as economically as possible by electronic means. The actual display of the information to a human reader, however, should be recognizably the same as the format required by law.

2.5 Original form

The requirements for retention echo those for functional equivalence of a written record (principle 2.2). If "original" is defined as a medium on which information is fixed for the first time, it would be impossible to speak of an "original data message." Multiple originals can be created; hence the principle 2.8, above, that allows one electronic document to serve the function of several paper copies. Again, one looks to the function of the requirement for original documents. In some cases, where there is truly a need for a single document that is an "original," the Policy and Bill exclude those documents from the application of the Policy or Bill (e.g., wills). In other cases, however, the requirement for an original has stemmed from a need to ensure that the information in a document is unchanged and therefore reliable. In a paper-based environment, original documents are demanded in order to lessen the likelihood that they have been altered in some fashion, which is easier to detect in an original document. There are, however, technical means of ensuring the integrity or "unalterability" of an electronic document or record. These specific technical means are almost certain to evolve and, following the requirement for technical neutrality, the Policy and Bill only look to the functional equivalent or outcomes. These are elaborated below in the next two principles for greater certainty and reflect, among other matters, some existing caselaw dealing with the introduction into courts of electronic documents or records.

2.6 Whether information or a record is capable of being maintained

This principle is fairly clear; a record or information must be, for example, "saveable" or "downloadable" and "printable." There is no specific technical requirement, however, consistent with technical neutrality, so the concepts of "saving" and so on are not specifically enshrined in the Policy or Bill. How the user of the information chooses to maintain it may depend on other requirements, such as record retention rules.

2.7 Criteria for integrity and reliability

Integrity refers to the information or the record not being altered or having data missing and emphasizes the importance of integrity of information for consideration of its originality. Reliability refers to the capacity of persons, including the courts, to rely on a record or information for various purposes. As with real life transactions, different levels of reliability serve different purposes: an individual will be far more concerned with the reliability of his bank account statement than with less important documents and the standards of appropriate security, assurances that the right information is attached to his identity and so on will be higher with financial records than they might be of a record of a video store rental, for example.

In drafting terms, the elaboration of the criteria for integrity and reliability may sometimes be found within the provisions relating to originality. The separation of the provisions is used in several Canadian jurisdictions, such as Ontario, and makes for easier reading of the concepts.

2.8 Copies

This provision simply reflects that fact that the recipient of an electronic record can print out as many copies as he or she chooses: to push the "send" button several times is unnecessary for the person who is providing the copies, as would be mailing multiple copies of an electronic disk.

2.9 Electronically signed message deemed to be original document

The media neutrality principle of the Model Law is not intended to change the substance of existing law. It is only intended to ensure that the law is equally applicable to paper and electronic records. In the Model Law, and in some jurisdictions, this provision includes the requirement that the signature must be as reliable as appropriate in the circumstances. At common law, signatures did not in themselves have to meet a particular test of reliability—a signature could be a handwritten name, a mark, a fingerprint etc. Parties to a transaction had the freedom to determine the appropriate form of a signature that might be required in a given transaction and this type of freedom is established for most situations in the provisions dealing with electronic signatures, below.

It is also important to distinguish between basic legal requirements, such as may be established by the Bill, and prudent business practices. The common law and the Bill would allow considerable freedom in determining the form and type of electronic signature that might be required for a given transaction. Parties to a contract, however, may have very distinct views about what may be appropriate, as may financial institutions and other suppliers of goods and services. Banks may be appropriately reluctant to allow people to sign cheques with a penciled X, and may want to have a more elaborate form of electronic signature for certain electronic transactions. While PIN numbers—a form of electronic signature--suffice for bank machines when combined with

a type of “smart card”—another potential form of electronic signature, there is a limit to the amount of withdrawal that may be made from an account. The provisions dealing with electronic signatures allow for more reliable and secure forms of signatures that can be required as appropriate.

This provision should also be read in conjunction with the definition of “electronic signature,” above. If the association with a person is demonstrated and the intent to sign is demonstrated, the signature will be valid, as is true with a handwritten signature or mark on a paper document. These elements have to be shown in order to meet the definition of “electronic signature.”

2.10 Retention of electronic records

This provision is consistent with the media neutrality of the Policy and Bill. It has no effect on time provisions etc. in the current law.

2.11 Admissibility and evidentiary weight of electronic records

This provision provides greater certainty with respect to the media neutrality of the law regarding electronic records and expands on the concepts set out in principle 2.1.

Principle 3: Contract Formation and Default Provisions

Most of the provisions of Principle 3 are also drawn from the UNCITRAL Model Law, although some matters, such as place of residence, are not since it reflects the broader scope of the Policy and Bill to include non-commercial transactions. In fact, businesses are already actively engaged in e-commerce, but these provisions provide greater certainty and set out default rules that may be useful in particular circumstances. Parties to a contract are free, of course, to set out their own rules regarding time and place of communications, means of communications, the jurisdiction under whose laws the contract is to be interpreted or enforced, arbitration clauses and so on. The default provisions are intended to apply only when parties have failed to include these matters in their agreements.

3.1 Formation and validity of contracts

This is simply a more specific expression of the principle set out in 2.1 and is consistent with the media neutrality of the Policy and Bill. It covers not only the actual terms of the contract but also the representations and other information that might be exchanged in the course of negotiating a contract. This provision does not mean that an electronic contract is automatically valid, but only that it will not be invalid merely because it is electronic. It may still be invalid due to any of the reasons that a paper-based contact may be invalid. Indeed, there may even be some situations in which the use of electronic communication may contribute to invalidity, e.g., using a hyperlink to communicate a vital and material fact may not be considered a sufficiently clear communication, depending on the situation, sophistication of parties and so on. But the underlying issue of contract law dealing with the basic agreement on the terms of the contract is not changed.

3.2 Electronic expression of offer or acceptance

This provision deals with one of the real issues in electronic contract formation: what type or form of electronic signal may be sufficient to indicate offer and acceptance. While a written offer in an e-mail may provide a fairly clear cut example, it is also possible to express agreement to an offer or acceptance of an offer through some other form of electronic signal, such as touching a computer screen, clicking an icon, responding to a voice recognition device

3.3 Involvement of electronic agents

Electronic agents (a defined term) can initiate an action or respond to an electronic communication without human intervention at the time of initiation or response. It is possible for two or more electronic agents to communicate and carry on a transaction. It is important to note that the term “agent” has nothing to do with the law of agency; as machines, they have no legal personality. The term is, however, well established. Principle 3.3 makes it clear that it is possible to form a valid contract using electronic agents on one or both sides.

3.4 Errors that occur while dealing with electronic agents

This provision is intended to deal with “keystroke” errors. Electronic agents, being only machines, may often not recognize keystroke errors. Very often to prevent such an error, individuals communicating with an electronic agent are asked to confirm their action—for example, clicking on an “OK” button on the bank machine or clicking an “I agree” icon on a computer or re-entering the information a second time to confirm it. The Policy and the Bill do not set out any particular form of correction that should be made available since that depends on the situation and will certainly depend on present and future technology. But since in most case an electronic agent cannot recognize an “oops,” it is appropriate to provide some form of correction mechanism or protocol. If the procedures set out to correct the error are followed, then the contract made in error is not enforceable. If, however, the party making the error has benefited from the contract by, for example, accepting and using a product, then the contract would be enforceable since that party would be considered to have adopted the terms of the contract even if originally made in error.

If there is no mechanism or protocol to correct the error, then the contract is unenforceable—again, unless the party making the error has received a material benefit from the contract.

3.5 Attribution of electronic records

Implicit in this provision is the concept of authorisation: the person sending the record electronically either did it personally or authorised the sending of the record. This essentially reflects existing law of contracts and agency. The provision is a simplified version of the language of the UNCITRAL Model Law, which in turn was based on the UNCITRAL Model Law on International Credit Transfers, which defines the obligations of the sender of a payment order. The provision is intended to apply when there is a question of whether a data message was really sent by the person indicated as being the originator. In the case of paper-based communication, the issue would arise as a question of a forged signature. In electronic communications, an unauthorized person may send the communication, but the authentication by code or encryption (e.g., electronic signature) may be accurate. The purpose of this provision is not to assign responsibility but to provide a rebuttable presumption that in certain circumstances a data message is considered the message of the originator.

3.6 Acknowledgement of receipt of electronic records

Electronic transmissions can often not indicate a guaranteed receipt of record. Parties may wish to request or require acknowledgment of receipt. It should be noted, however, that acknowledgment in and of itself does not guarantee that the communication has not been altered in some fashion either deliberately or accidentally. Secure communications are a separate issue, as is the difference between acknowledgment of receipt and agreement with the contents of a communication. Acknowledgment of receipt of an offer and acceptance of the offer are a matter of contract law and are not intended to be changed by this provision.

3.7 Time of sending of electronic records

Electronic communication is treated as being sent when it leaves the control of the originator, that is, when the originator can no longer prevent the transmission of the record or information. For example, an individual using email attached to dial-up or high-speed connection to the Internet would send an email when hitting the “send” button and the message leaves the computer. When a computer is attached to a corporate network, the record or information is sent when the email leaves the relevant network; this is typically when it leaves the corporate mail server and enters an Internet Service Provider’s server. If the originator and addressee are on the same system (e.g., within an office), then the record is deemed sent when it becomes capable of being accessed by the addressee.

3.8 Time of receipt of electronic records

Electronic communication is treated as being received when it enters the computer system that the addressee has designated for receiving messages or that is generally used for messages of that type. If, for example, a company has a particular email address for dealing with customer complaints and another for dealing with orders for goods, then the message is treated as received when it reaches the appropriate address.

It may be noted again that these are default rules and do not necessarily represent prudent business practice or the approach that many people take in doing business. It continues to be good business (and personal) practice to ask that the addressee acknowledge receipt of a communication when the matter is important; see principle 3.6.

It should also be noted that this provision does not require that the electronic record be necessarily intelligible to the addressee. There are situations in which an encrypted message may be sent and considered as received even though decryption may occur later or not at all (the Model Law mentions some circumstances in which encrypted data is transmitted to a depository for the sole purpose of retention in the context of intellectual property disputes).

A data message should also not be considered as sent if it cannot enter the system; an addressee is not under an obligation to keep a system functioning at all times.

3.9 Place of sending and receipt

This default rule is important since it may not be obvious from where a communication is sent. The basic rule is that a communication is sent from a place of business. This provision also clarifies a situation when an employee of a company may travel and send emails from any number of locations. Those various locations, or the locations of a server or other intermediary, are not relevant to determining the place of sending and receipt.

3.10 Place of business

This provision further clarifies the rule regarding place of business as the place of sending and receipt. Where an address has more than one place of business, then the place of business associated with the underlying transaction is the location. The "underlying transaction" is intended to refer to both an actual commercial transaction and one that may not be completed. As an example, if the Port of Spain-based subsidiary of a US company entered into a contract or negotiated with a supplier in Grenada, the place of sending or receipt with respect to the Port of Spain company's communications would be Port of Spain, although the company may have multiple locations across North America and the Caribbean. If there is no transaction as such, but merely a communication, then the location of the principle place of business of the originator or receiver of the communication is the place of sending and receipt. For a corporation, the principle place of business generally refers to the head office.

3.11 Habitual residence

The Policy and Bill are intended to deal with transactions and communications that are non-commercial, as well as those between consumers and businesses. Where there is no place of business on at least one side of the communication or transaction, then a residence becomes the relevant criterion.

Principle 4: Electronic Signatures

4.1 Electronic signature

Electronic signature is a defined term and the definition used in the Policy and Bill is a straightforward explanation of the technical nature of an electronic signature. Thus, the definition itself does not impose any qualifications on the reliability or security of the signature and allows persons the flexibility to choose the level of reliability and security they prefer—taking into account the fact that a court may find that the form of signature chosen was inappropriate in the context if they wish to enforce the agreement to which the signature attests.

4.2 Minimum standards for electronic signatures

The provisions in principle 4.1 set out the flexible criteria that may be applied when the law requires a signature. In some legislation (e.g., the Canadian Federal Act dealing with electronic documents), the different situations, such as a witnessed signature, a notarized signature and so on are set out in sections with the accompanying reliability and security requirements. The format chosen here is more flexible and more easily allows for both distinctions in the forms of signatures, the nature of future technology and an expansion of categories of records to which particular forms of signatures might be attached. This provision should be read in context with Principle 4.3, below and the provision in Principle 4.4 that allows the Minister to require particular forms of signatures for specific legal documents.

4.3 Reliability and integrity of electronic signatures

This provision elaborates the concepts of reliability and integrity in the context of electronic signatures. These provisions are used widely in jurisdictions throughout the world that use a technology-neutral approach. In this Policy and Bill, these characteristics are associated at their strongest with a more secure type of signature designated through the provision of an "accredited certificate," below at Principle 4.4.

4.4 Regulations regarding electronic signatures

This provision provides the government with the flexibility to determine what form of electronic signature may be appropriate in particular circumstances and to adjust the situations in which the "law requires" a particular form of signature, i.e., the flexibility for parties to choose their own form of signature is pre-empted. This may be used particularly in cases where the signatures are required for filings to government to fulfill regulatory or other requirements and is thus an important element in the capacity to effectively implement e-government.

4.5 Electronic signature associated with an accredited certificate

Some forms of electronic signature are more reliable and secure than others and offer greater proof and certainty regarding authenticity. Currently, the more commonly used secure form of electronic signature is the digital signature, which is based on a public key infrastructure (PKI) or public key cryptography. Usually algorithmic functions are used to generate two different, but mathematically related, "keys." One key, known as the "private key," is used to create the signature and the other, the "public key," is used to

verify the signature. The signatory must keep the private key secret since that is the basis for authenticity, although the signatory does not need to know the key but can use, for example, a "smart card" to sign. The public key can be held by a number of people, including public institutions. Attaching the private key to a particular individual or verifying or certifying the relationship between the public key and the private key (and hence a particular individual) is a necessary part of the structure; this function is usually performed by a "trusted third party" who issues a certificate (certification service providers, see below). This is, therefore, the link between the signature verification data and a signatory, and confirms the identity of the signatory. This allows strangers to communicate and authenticate their communications.

In certain cases, such as where digital signatures are used, the certificate will attest to the use of a technology that has a relatively high level of security and reliability. In this case, the certificate is designated an "accredited certificate." This term is taken from the legislation of Bermuda; other jurisdictions speak of "qualified certificate" (Norway); or a secure or enhanced signature (e.g., Singapore) or an "advanced" electronic signature (Denmark). The meaning is generally the same: a level of signature whose technology provides a high level of security and reliability. Consistent with the approach of technical neutrality, the Policy and the Bill do not define the specific technology that meets these requirements (unlike, for example, Singapore which has focused on digital signatures), but only sets out the characteristics of the signature (e.g., ensuring that the communication cannot be altered without detection).

Since an accredited certificate is associated with a more secure form of signature, the responsibilities of those who provide these certificates are more onerous.

Principle 5: Certification Service Providers

Certification service providers are in the business of providing electronic signatures and, in particular, of providing the certificates that link signatures with signatories. The regulatory regime described in Principle 5 is co-regulatory and places responsibilities on certification service providers to fulfill certain responsibilities and maintain certain standards of technological and business practice as the reliance on their services increases. In other words, the provider of an accredited certificate, which implies a more secure level of signature, is obliged to meet more stringent requirements. The regulatory structure set out in this Principle is drawn from those used in Sweden, Denmark and Norway. Among other matters, it reflect the reality that the technical capacity to realistically regulate in a quickly changing and technically sophisticated environment is almost certainly lacking in government. To pretend otherwise is to court a finding of liability for regulatory negligence and to undermine the credibility of the regulatory structure in general.

5.1 registration

Under this regulatory scheme, there are no onerous regulatory requirements imposed those who wish to offer the service of certifying electronic signatures. This is consistent with the approach taken by the European Union (EC Directive on a community framework for electronic signatures) and is also consistent with the elements of the Electronic Transactions Policy that seek to avoid the imposition of non-tariff trade barriers and unnecessary regulatory requirements in the provision of certification

services. It also reflects the reality that there currently exist a number of less secure forms of electronic signature, such as PIN numbers or passwords, that are used in a variety of minor transactions, such as checking the number of points in an airline plan or purchasing an item on eBay. There is no intention in the Policy or Bill to impose unnecessary regulatory requirements in these situations.

Where, however, a person wishes to set up in the business of providing electronic signatures in Trinidad and Tobago, that fact should be registered. The type of information required is intended to be minimal and include such matters as address, names of officers and directors if it is a corporation, and other contact information. The Minister by order can specify what information should be required for a registry.

The registration may be done with the Minister (i.e., the Ministry) or with a body to which this responsibility is delegated by the Minister by order. The intention is to provide flexibility in the choice of institution to which this responsibility is assigned. For example, it may be appropriate that the Telecommunications Authority of Trinidad and Tobago carry out this responsibility. It may also be appropriate that if an Office of a Data Commissioner or an Information and Privacy Commissioner is established pursuant to the Policy and Bill dealing with Data Protection (which will complement this Policy and Bill), that organisation would be appropriate locus of responsibility. Or it is possible that at some point industry organizations may develop that are sufficiently sophisticated, well-funded and credible to take on these responsibilities. In any event, the Policy and Bill allow for flexibility as the environment, and perhaps the nature of the responsibilities, change.

5.2 Registry of certification service providers

The registry is intended to be a public document. At the most minimal, it provides the public—potential users of the services—with some basic information about the service providers. Where the certification service providers provides an accredited certificate and has therefore filed the information requirements listed below at 5.3, that fact should also be noted. This provides an element of consumer protection by allowing the user of the services to know that the service provider has at least met certain minimal regulatory requirements. It does not, however, indicate that they continue to be in compliance with these requirements and the fact of the registry does not imply that the Government warrants in some way that they are.

5.3 Requirements for a certification service provider that provides an accredited certificate

These requirements are a compilation of the minimal requirements to ensure the integrity, security and credibility of a more secure level of electronic signature. These are found in legislation in a number of jurisdictions, including Bermuda. These can be elaborated by order of the Minister. For example, in Bermuda, the “Certification Service Providers (Relevant Criteria and Security Guidelines) Regulations 2002” provide 50 pages of technical requirements that, among other matter, require compliance with the IETF (Internet Engineering Task Force) and European ETSI/CEN standards, in addition to various ISO/IEC standards, including the best practices management systems standards such as ISO/IEC 17799. These matters can be considered by the Minister pursuant to the Policy and Bill, but may initially also be suitable for a code of conduct developed by

either industry organizations or adopted from existing codes of conduct and application of the ISO/IEC quality management standards. Compliance with ISO and other quality management standards is usually certified by an independent third-party and the Minister may want to further follow the Scandinavian model by requiring a third-party audit of compliance and the filing of the outside auditor's report with the information required under 5.3.

5.4 Self-certification of compliance with the requirements for a certification service provided of an accredited certificate

Self-certification of compliance is commonly used in European regulatory systems, although it can be found in some other areas, including transportation safety, occupational health and safety and environmental regulation. In all cases, it must be backed by a serious enforcement and sanction structure dealing with false or misleading filings. In effect, the regulatory bargain is: "we will give you the freedom and flexibility to ensure compliance and certify compliance and will reduce the regulatory burden on you; in exchange, if you betray the trust placed in you, the sanctions will be sure and heavy." It will be an offence (see below) to provide false or misleading information in self-certifying compliance with regulatory requirements.

The reason this approach was chosen in the Policy and Bill is essentially practical, although it also is consistent with the general approach of encouraging business and not imposing unnecessary constraints on competition or innovation. The practical point is lack of capacity, which has been behind various forms of self-regulation or self-certification in a number of situations, primarily the financial services industry. In discussing its regulatory approach (which is similar to that chosen here), the Danish Government notes:

> The reasons for organising the regulation as an audit-based system in which a major part of the practical regulation is carried out by the external auditor at the certification authorities, are first of all to make use of the experience and competence in the performance of systems audits that already exist in the audit sector. Expert knowledge is required to be able to understand and assess the advanced technology used by a certification authority and the National Telecom Agency does not possess that knowledge today.
>
> Secondly, it will take a great deal of resources to build up extensive governmental regulation, and it is assumed that these will be paid for by the companies subject to regulation. This might deter certification authorities from issuing qualified certifications [note: accredited certificates], which might mean that the quality of the market created for electronic signatures might be insufficient to inspire confidence among consumers, authorities, and companies. [1]

The Danish legislation requires the statement of self-certification to include the management and system auditor of the certification authority, a declaration from the certification authority's management stating that its overall data, system and operation security must be regarded as adequate and in compliance with the rules laid down in the

[1] Bill on Electronic Signatures—Bill No. L 229, Ministeriet for Videnskab Teknologi og Udvikling

Act, and a declaration from the system auditor that these are also to be regarded as adequate. The self-certification structure is therefore underlaid by a third-party independent audit.

5.5 Notification of compliance must be renewed annually
This is also based on the Scandinavian model and ensures that the information held by the Ministry is up-to-date.

5.6 Audit by Minister
A regulatory system that relies on a heavy degree of self-regulation through the implementation of internal compliance systems and reporting must be backed by the potential of a government response. Some call this the "shadow of government." The late American Supreme Court Justice, William O. Douglas, called it the "loaded shotgun behind the door" when he was the second Chairman of the U.S. Securities and Exchange Commission [in reference to his relationship with the New York Stock Exchange]. Whether the Minister or his delegate (see discussion above) undertakes an audit for compliance in response to a complaint or on a random basis, the power to examine the certification service provider regarding the accuracy of the self-certification, the integrity of the compliance systems and the quality of service being provided to clients is crucial. An audit could also be used to ensure that the information provided in the registration is accurate and up-to-date, although this is unlikely to be an enforcement priority.

5.7 Responsibility to co-operate with audit
The audit by the Minister or his delegate plays an important role in maintaining the integrity of the self-certification system. The certification service provider must provide all reasonable co-operation with the audit, which would include making information available, allowing interviews of staff, review of documents, internal compliance systems, software and so on. Providing false or misleading information in this context, as with original and annual self-certifications, would be an offence. In addition, obstructing an audit would also be an offence.

5.8 Confidentiality
Anyone, whether a government official or an expert consultant, who is involved with an audit of a certification service provider of an accredited certificate will have access to sensitive information. They may have access to information about the clients, the certificates themselves, the security precautions used by the provider, the backgrounds of employees of the provider and other information that should not be divulged except in very narrow and specialized circumstances (primarily in enforcement proceedings—and even then may be treated as an *in camera* matter with confidentiality). This provision is intended to impose an obligation on these individuals and breach of this obligation would be an offence under the Bill.

5.10 Powers of the Minister to deal with failure to meet requirements
The main powers of the Minister when a certification service provider has failed to meet requirements—for example, has not maintained satisfactory standards or has failed to self-certify on time—relate to ordering either a cessation of business or the taking of remedial action. For example, a service provider who had become slack on security matters might be forbidden to continue to offer accredited certificates until corrective

action had been taken. What that action might entail might be identified by the order. These provisions are complemented by the offence provisions relating to provision of false or misleading information or failure to co-operate with an audit. In those cases, the emphasis would be less remedial and more on sanctioning illegal behaviour.

5.11 Recognition of external certification service providers

This provision establishes a regime of international recognition and co-operation that will be important for Trinidad and Tobago since, in a practical sense, a competitive certification service provider industry may be slow to develop within the country. It also ensures the reciprocal structure that is necessary in the global economy of e-commerce.

5.12 Pseudonyms

Electronic signatures are intended to perform the functions of a handwritten signature and the functional approach identified as a key theme of the Policy and Bill indicates that there should be no more restrictions on the use of pseudonyms for electronic signatures than there would be for handwritten signatures. The service provider itself would have the necessary information regarding the signatory's true name and, if a pseudonym were being used for fraudulent or other illegal purposes, other legislation deals with the matter.

5.13 Additional responsibilities of certification service provider

The addressee who receives the document with the electronic signature needs to be able to know that the information about the signatory is accurate and up to date. Signatories of electronic signatures, like those who sign handwritten signatures, may have limitations placed on their authority. It is common for individuals in business or government to have "signing authority" up to a certain amount or for a certain purpose. Similarly, the certificate for an electronic signature may be limited. The directory sets out that information.

5.14 Immediate revocation upon request

Signatures have a meaning and persons using signatures wish to be assured of their on-going validity and credibility. Just as users of credit cards or bank cards rely on the credit card company or bank to respond immediately to requests for cancellation for lost or stolen cards, the signatory will want to be assured that the potential for misuse of a signature is limited by immediate response by the certification service provider.

5.15 Liability of certification service provider issuing an accredited certificate

Where it can be shown that the certification service provider has failed to meet the standards required—for example, by failing to have adequately trained or skilled staff or using current security standards—that service provider will be prima facie liable for any damages or loss that occurred to anyone relying on the certificate.

5.16 Release from liability

Even if a certification service provider has failed to meet the requirements and is in a position of being prima facie liable to anyone who relied on the certificate, the service provider may be exempted from liability by showing that the injury or loss was not caused by negligence. Thus, if the provider took all reasonable precaution to ensure that

only qualified people were hired and had no reason to believe that an employee was not competent, then the provider would very likely to not be held liable because it turned out that an employee did not meet the standards for experience and training (e.g., perhaps he had misled the employer).

5.17 Same
The practical effect of this section is to create an incentive for a certification service provider to make a due diligence investigation of the qualifications of any other certification service provider that it guarantees. The paramount objective of ensuring the security, integrity and authenticity of the signature and consequent protection of the those who rely on them is not undercut by a system of indirect guarantees with no real substance.

5.18 Costs and fees
Cost recovery is appropriate for this type of service. Recovery of the costs of audits is also an incentive for co-operation and, ideally, for maintaining a reputation that will reduce the likelihood of an audit.

Principle 6: Intermediaries and Internet Service Providers

6.1 Liability of intermediaries and Internet service providers
For Internet service providers and intermediaries, there is a separation of content from the service of providing carriage for content. Where the common carrier concept of mere carriage or provision of a conduit applies, the ISPs, like the telcos, will not be held responsible or liable for content. There is a limitation, however. Where the ISP or intermediary becomes aware or where judged by the objective standard of whether a reasonable person in that position would be aware (to avoid willful blindness) that there is a likelihood of civil or criminal liability regarding the content being carried by the ISP or intermediary, certain obligations are triggered. These are dealt with in the section Principle.

6.2 Procedure for dealing with unlawful, defamatory etc. information
In some jurisdictions (e.g., Bermuda, Singapore), and ISP or intermediary who becomes aware of content that has a likelihood of attracting civil or criminal liability, that ISP or intermediary must remove the content from the system immediately. While this approach has the attraction of quick and seemingly decisive action, it has problems. Who is to determine whether there is a "likelihood of attracting civil or criminal liability"? Admittedly in some cases, such as child pornography or a "snuff" film, the matter would be clear to almost anyone. But there are many matters that are not so clear: defamatory material is not always even clear to the courts. Political or social commentary, even of a rude or stringent nature, should not be discouraged. The line between art and obscenity is one that shifts, depends on community values, and is constantly being re-defined. It is difficult to say that it is so clear that the burden should be placed wholly on the ISP for taking action that itself could trigger problems and even liability. For example, if someone complained about commercial material on a website because to that individual it

was offensive and the ISP closed down the website, there could be resulting losses of profits. And perhaps the individual who complained was overly sensitive, or perhaps even a competitor. Should the ISP have to make those judgments?

The approach taken in the Policy and Bill is to require the ISP or intermediary to take action to report the matter. The basic reporting responsibility would be to report to the Telecommunications Authority of Trinidad and Tobago. A provision also allowing the option to report to law enforcement authorities was included so that where the content appeared to be so egregious (e.g., the child pornography mentioned above), immediate reporting to law enforcement would be possible—even outside of regular business hours.

The ISP or intermediary may be required to remove the content from the server or close down the website or divulge information about the customer, but only in response to lawful authority. This might be a court order, a warrant or a provision in legislation. In any event, the ISP or intermediary is not required to act without some form of authority.

6.3 Role of the Telecommunications Authority of Trinidad and Tobago

This provision complements the requirements for the ISP or intermediary to notify the TATT. The Authority is obligated to take such action as it considers reasonable—which might, in some circumstances, be no action at all. If the ISP, for example, has received a complaint that appears frivolous, vexatious or overly sensitive, it may report the matter to the Authority out of an abundance of caution but TATT may, upon examining the matter, close the file. TATT may also report the matter to the authorities. In the rare circumstance where TATT is of the view that immediate action should be taken but, for whatever reason, law enforcement authorities have not responded, TATT is authorized to apply to a court for whatever orders the court determines are appropriate.

6.4 Codes of conduct and service standards for intermediaries and Internet service providers

The commercial behaviour and business reliability of intermediaries and Internet service providers will be important elements in ensuring trust in e-commerce. TATT has the mandate to require the development of a code of conduct, which might cover such matters as provision of information to clients, offering "spam" filters or allowing blocking of certain content, and establishing a protocol for reporting concerns about objectionable content to TATT. Codes of conduct, whether voluntary or whether adherence is mandated by law, define good business practices in an industry. As a consequence, courts often look to codes of conduct to determine due diligence and standards of care in determining liability.

Principle 7: Government and Other Public Bodies

The objective of this Principle is to ensure that the Government has the necessary authority it will require to "do business" electronically; in other words, to implement the e-government provisions of ***fastforward***. Much of the legislative language is taken from the legislation of the Province of Ontario. Principle 7.2 complements the provisions of Principle 1.6 that express consent is required for Government and recognizes that this

may also be granted by the provision of specific instructions regarding electronic filings, forms, etc. Principle 7.3 recognises the regulatory authority of the Central Bank and the need for particular expertise to deal with this issue. It is possible that additional and more specific authority may be required for electronic business with respect to particular legislative provisions, but the Ministry is undertaking a Legislative Review to ensure that there are no additional legislative barriers to the implementation of ***fastforward.***

Principle 8: Consumer Protection

In some jurisdictions, electronic transactions legislation provides a fairly complete code of consumer protection (e.g., Saint Vincent and the Grenadines). In some other cases (e.g., Ontario, Canada), modernization of consumer legislation has included provisions to deal with e-commerce. Other work is being done within the Government of Trinidad and Tobago to improve consumer protection, including the development of a Code of Conduct for E-Commerce. An array of initiatives are truly needed, including education and provision of more information to consumers about the opportunities and risks presented by the new electronic environment (e.g. risks of identity theft). This Policy and Bill, however, provide an opportunity to put forward some basic consumer protection provisions that are closely linked to the subject matter of the Policy and Bill. In all respects, these initiatives should be viewed as an early step in the development of comprehensive approaches to consumer protection and the fight against unwanted communications, which are putting the viability of the Internet and e-commerce at risk and damaging not only consumers, but also inhibiting legitimate business communications and imposing costs on business and Internet service providers.

8.1 Minimum information in e-commerce

When a consumer operates in a face-to-face environment, or even deals with a supplier over the telephone or through the mail, the consumer often has certain information about the supplier—where the supplier is located and how to contact that supplier. In the e-commerce environment, the supplier is often in another—unidentified—country and the consumer may have little knowledge of how to contact or deal with the supplier. The consumer cannot examine the goods and may have little opportunity to confirm the nature of the services beyond the description available on a website. Assurances of good business practices on the part of the supplier may be even more important in e-commerce when the consumer may have little recourse or opportunity to seek redress because of lack of information. Indeed, the consumer may not really have the opportunity to exercise a truly informed choice about purchase because of the lack of information. The provision in principle 8.1 is intended to address these deficiencies and provide a model for good business practices in general.

8.2 Minimum information regarding e-signatures

This provision is essentially a list of information that an informed consumer of e-signature services should know or would want to know. Since this is an evolving industry, requiring the information will ensure that good business practices are part of e-commerce in Trinidad and Tobago from the beginning.

8.3 Unwanted commercial information ("spam")

Spam is proving to be a genuine menace to the viability of the Internet and e-commerce; as such it presents a threat to the economic development that many countries, including

Trinidad and Tobago, are hoping to achieve through e-commerce and the introduction of modern communications technology. The fight against spam will be international and must be co-operative and take advantage of a number of tools—the criminal law, technological solutions, consumer protection, good business practices, codes of conduct, education and other approaches. This provision is only a part of a concerted and comprehensive policy and legislative approach that must be developed. It does, however, provide consumers with one tool they can use to limit unwanted communications. As such, it is important to provide consumers with this tool at the earliest opportunity. The focus here is on email, although unsolicited mobile and fax communications are an emerging problem and will be dealt with as part of a broader policy.

8.4 Right of recission

Where a consumer has not been provided with the minimum information required by principle 8.1, the consumer will have the right to rescind the contract, provided that the consumer has not received any material benefit from the contract. If, for example, the consumer has received and used the product or the service that was the subject of the contract, then the contract cannot be rescinded. Any supplier in e-commerce who fails to provide the required information, however, runs the risk of having a contract cancelled.

Principle 9: Enforcement

Most of the provisions of the Policy and Bill are enabling: they do not impose regulatory requirements. In some cases, there are requirements; and in other cases, while there are choices about entering into agreements or undertaking activities, there are requirements for fair dealing and honest communication. The offence provisions reflect this. There are not, of course, offences for failure to abide by a Policy, but the Bill will provide for these offences when provisions become mandatory.

9.1 Failure to provide required information to consumers

In addition to allowing the consumers to rescind their contracts when the necessary information is not provided, it will be an offence to fail to provide the information.

9.2 False or misleading information

Providing consumers with false or misleading information will also be an offence. This provision is also necessary to back up the co-regulatory approach of self-certification. As noted above, there is a certain degree of flexibility available to the provider of the information but that does not extend to providing misleading, let alone false, information. To provide adequate deterrence, the penalties should be high and the response swift.

9.3 Obstruction of an audit

Like the provisions under Principle 9.2, the effectiveness of the co-regulatory approach depends on co-operation and the ability of government and the business sectors to work together. While audits will in most cases likely be on a complaint-driven basis, they form the core of the monitoring and enforcement system. Lack of co-operation should be treated with severity.

9.4 Directors and officers

This provision states the liability of directors and officers who direct, authorise etc. misconduct. In that sense, it is not an unusual section. It does clarify that it is not necessary that the corporation itself be convicted (since different evidentiary issues might apply and, indeed, a director or officer may have authorized misconduct that never was successfully completed by the corporation but that may still incur liability on the director's or officer's part, e.g., for obstruction). It also raises the profile relating to liability of directors and officers to state the matter specifically rather than require exploration of issues of vicarious liability.

9.5 Duties of directors and officers

Studies regarding compliance have shown that probably the most important single element in ensuring that there is a "culture of compliance" in place within a company is the attitude and message given from the top. Where directors and officers take their responsibilities seriously regarding ensuring that the necessary systems and reporting arrangements are in place within a company, the employees understand that these things genuinely matter—it is not just words or window dressing. In a practical sense, many of these matters will apply to certification service providers, and particularly those who provide accredited certificates. The requirements imposed on them relating to security, conduct of the business, activities of employees and so on will require on-going internal awareness and surveillance of compliance. Placing specific duties on officers and directors to ensure that these systems are in place will make compliance more likely and raise the profile of compliance activities.

9.6 Breach of confidentiality

The confidentiality provisions are important not only because of the major breach of trust that would occur but also because of the potential for large damages, both pecuniary and non-pecuniary. Backing these provisions with a sanction emphasizes their vital importance.

9.7 Penalties

Specific penalties should be subject to discussion, although it is important to distinguish between individuals and corporations and adjust sanctions accordingly.