By e-mail, fax & post

Our Ref.: C/COG(23), M7819 15 November 1999

Chairman,
LegCo Bills Committee on
Electronic Transactions Bill,
Legislative Council Secretariat,
3rd Floor, Citibank Tower,
No. 3 Garden Road,
Central, Hong Kong.

(Attn: Miss Salumi Chan
Clerk to Bills Committee)

Dear Sir,

Electronic Transactions Bill

Thank you for giving us the opportunity to present the Society's views on the above Bill at the Bills Committee meeting held on 12 November 1999. We indicated then that we would be sending you a more detailed reply to the Administration's response to our original submission. In that submission, we also mentioned that we would be referring some supplementary points to the Bills Committee. This letter covers both matters. Part 1 deals with the supplementary issues and Part 2 deals with the Administration's response to our submission to the Bills Committee of 1 November 1999.

If you require further elaboration on any of the points made in this submission, please contact Ms. Winnie Cheung or Mr. Peter Tisman in the first instance.

Yours faithfully,

LOUIS L. W. WONG
REGISTRAR
HONG KONG SOCIETY OF
ACCOUNTANTS

LW/WCC/ky
Encls.

c.c. Mr. Eric Li
ITBB (Attn: Mr. Alan Siu)

15 November 1999

HKSA Submission (Number 2) to the LegCo Bills Committee on Electronic Transactions Bill

Part 1 – Supplementary points

Use of the terms "audit" and "auditor"

1. We are concerned about the terminology used in clause 37 and believe that it may give a misleading impression. Cl.37(1) specifies the requirement for an audit of the performance of a recognised certification authority at least once every 12 months. Cl.37(2) requires the audit to be conducted by a person approved by the Director as being qualified for that purpose. The draft Code of Practice (in paragraph 3.13.2) further specifies that "all audits must be conducted by a qualified and independent "auditor" approved by the Director for this purpose."

   The term "auditor" is used in many Ordinances to mean a person who is a professional accountant holding a practising certificate under the Professional Accountants Ordinance (Cap. 50) that is, a Certified Public Accountant or CPA. We consider that it could create a false impression if the words "audit" and "auditor" were to be used in a sense that is different from this and which does not relate to statutory financial audits performed by CPAs.

   Currently, the term "audit" is not used to describe reports that can be distinguished from statutory audits of financial statements, even where they may be filed by auditors. Examples of these are reports filed to regulatory authorities for supervisory purposes that are stipulated under the Banking, Securities and Insurance Companies Ordinances and Ordinances of other regulated industries.

   Under the circumstances, we propose that clause 37 of the Bill be amended at the Committee Stage along the following lines:

   (1) A recognized certification authority must appoint a person to provide a report, at least once in every 12 months, at the expense of the recognized certification authority, for the purpose of assessing whether the recognized certification authority has complied with the provisions of this Ordinance applicable to a recognized certification authority and the code of practice.

   (2) A report under subsection (1) is to be prepared by a person approved by the Director as being qualified for that purpose."

Scope of the report under cl.19 and "audit" under cl.37

2. The draft Code of Practice recently published for public consultation has still not clearly defined the scope of the report required to be furnished by an applicant to become a recognized certification authority, or the person required to prepare such a report. The draft Code, in many cases, quotes from, rather than explains, the law's requirements.

As the draft Code is meant to provide the main regulatory framework for the operation of recognized certification authorities and will form the key part of the report and also the "audit" of a recognized certification authority under cl. 37, it needs to be sufficiently specific so as to leave no doubt as to what is expected of an authority or its "auditors". The "audit" scope also has to be clearly defined.

We also query the requirement under cl.19(3) (b) for a report which "certifies" that an applicant is capable of complying with the provisions of the Ordinance applicable to a recognized certification authority and any code of practice. We are not clear what it would mean to certify an applicant's capability, particularly where some of the requirements with which an applicant has to comply may not be verifiable by any objective benchmarks or by any practicable means. For example, a recognized certification authority is required under the draft Code of Practice (paragraph 3.1.1) to "comply with all the conditions of recognition including the conditions attached by the Director to the recognition granted under section 20 of the Ordinance". However, an applicant will not be in a position to know what these conditions may be at the time of the application. Again, a recognized certification authority is also required to "comply with the legislation currently in force in the Hong Kong Special Administrative Region" (draft Code of Practice, paragraph 3.1.2). This includes a huge body of primary and subsidiary legislation, much of which will have little direct relevance to a certification authority. How can a report "certify" that an applicant is capable of complying will the entire body of legislation in Hong Kong?

Clause 20: Overlapping requirements of the Ordinance and the Code of Practice

3. We note that there appears to be a considerable degree of overlap and repetition between the Ordinance and the draft Code of Practice that contributes to the problems referred to under item 2 above. For example, under clause 20(3) of the Bill, the Director of Information Technology Services must take into account a number of things in determining whether an applicant is suitable for recognition; amongst these are the following:

"(d) the report referred to in section 19(3)(b)(if applicable);
(e) whether the applicant and the responsible officers are fit and proper persons"

However, under paragraph 3.3.6 of the draft Code of Practice, there is already a requirement for a recognized certification authority to ensure that all its responsible officers are fit and proper and, as indicated under item 2 above, the report under clause 19(3)(b) must indicate, inter alia, whether an applicant is capable of complying with any code of practice. There are other examples of such duplications. It appears to us that the interaction between the Bill and the draft Code of Practice needs to be re-examined.

Security protection requirements

4. The term, "generally accepted security procedures" specified in the interpretation section is not commonly used and conveys the idea of a detailed guidance that may differ on a case by case basis. There is currently a wide range of security procedures in use:

   - some are based upon a set of standards (NIST, and BS7799 / AS4444 Information Security Management);
   - some are based upon performance of certain criteria (Visa / MasterCard);
   - some are based upon trust (Trusted Computing Security Evaluation Criteria (TCSEC) by the US Department of Defense);
   - some are based on a set of voluntary guidelines (HKMA Guideline 15.1.1);
   - some are based upon controls (ISACF Control Objectives for IT or CobiT);
   - some are based upon assessment of risk (Basle Committee risk management guide);
   - some are based upon the need for independent audit (CPA WebTrust);

   For this reason, we consider that the term "generally accepted security principles" would be a more appropriate description and would suggest that some generic "security principles" should be defined and applied. It is unlikely that core security principles will change although the application of these principles will differ depending on the circumstances. Specifying and establishing such principles up-front would provide the framework for parties to apply the appropriate level of security measures.

5. Although we referred in our submission to the WebTrust concept being developed in Hong Kong by the Society, we would emphasize that we are not suggesting the need to have specific types of security assurance services provided for in the law. However, the general expansion of e-commerce could be impeded significantly by legitimate concerns over security issues. In fact, the results of a number of recent surveys on e-commerce have indicated that security is of higher concern among Asian respondents than those in the U.S., Latin America or Europe. We believe that provision for the adoption of suitable security protection arrangements, as and when they are developed, could and should be introduced into the main body of the law.

Taxation implications

6. The Bills Committee should be aware of the potential tax implications of e-commerce particularly for a "source" based tax system. Clause 18 of the Bill stipulates when an electronic record is deemed to have been sent and received. Clause 18(4) and (5) make reference to the originator's and the addressee's "place of business" and the place of business "which has the closest relationship to the underlying transaction". It is not at all clear how the concept of "closest relationship" is to be interpreted but, more generally, an e-business provider can be registered in any place and can be linked to any internet portal or be copied onto different servers at different locations. This will present considerable challenges to a tax regime that bases liability on whether or not income has a Hong Kong source and which utilises factors such as where a particular underlying transaction was carried out to determine this issue.

Part 2 - The following points are made in response to the Administration's paper (LC Paper No.CB(1) 297/99-00(02) commenting on our earlier submission.

General considerations

7. Although it may be true that provisions exist in other legislation for that legislation to prevail over any inconsistent law, provisions of that type are in fact the converse of clause 15 of the Bill. Clause 15 provides that the Bill gives way to conflicting provisions in other legislation. The former type of provisions result in greater certainty by creating in effect a "superior" piece of legislation whilst clause 15 gives rise to more uncertainty because various pieces of legislation will prevail over the ETB and we do not know at this stage precisely what types of transaction will not be governed by the ETB. Hence our suggestion for a review of other legislation on which this may impinge to ensure consistency. In advocating this we note that submissions on the Bill from the Bar Association and a firm of solicitors have already pointed out that, as currently drafted, the Bill would have the effect of impinging upon one of the basic principles of contract law. This indicates the possible pitfalls of not examining the ramifications of the Bill on the existing legal framework.

   In relation to the reference in our submission to the WebTrust concept, see our comments in Part 1 above.

More detailed points

Interpretation

Definition of "trustworthy system"

8. We have explained in Part 1 the problem with the reference to "generally accepted security procedures" in the definition of "trustworthy system". Numerous references are also made to the test of reasonableness. We believe that further guidance could and should be given to the courts in terms of matters to be taken into account.

   Examples of similar provisions in other jurisdictions are quoted by the Administration in relation to this clause and others, in order to lend support to the Bill as drafted. However, the examples quoted are different in relation to different clauses of the Bill. In this instance, it is "Singapore, Malaysia, Utah, etc". Elsewhere references cited are Australia, United Nations Commission on International Trade Law, UK and Denmark. This rightly or wrongly creates the impression that various different approaches adopted in different jurisdictions have been amalgamated in the Bill. If this is in fact the case, it may not be conducive to the overall consistency and integrity of the framework.

Clause 7

9. In relation to the requirement under clause 7 for there to be a reliable assurance as the integrity of the information, the Administration's reply states that the test for whether a reliable assurance exists is essentially a matter of fact to be decided ultimately by the court having regard to the circumstances of the case. However, this clause concerns the fundamental issue of whether a rule of law requiring information to be presented or retained in its original form is satisfied by presenting or retaining the information in the form of electronic records. This may result in a good deal of uncertainty until such time as

a substantial body of case law is built up. Furthermore, no guidance is offered to the courts as how to determine the issues involved. If Hong Kong is at the forefront in implementing legislation of this type, then there will be few common law precedents for the Hong Kong courts to follow. This will result in the imposition of an onerous burden on what is a relatively small judiciary.

Clause 11

10. The response refers to the receipt of electronic information by the Government. However, it is not evident that this clause is intended to relate solely or primarily to government functions. We make two points by way of reply. Firstly, the Administration could specify explicitly in the legislation that in respect of acceptance of electronic submissions made to the Government certain procedures will be applied. These need not be applicable to all other types of transactions and why should they be if the concern is limited to acceptance of electronic transactions by the Government? Secondly, the issue of consultation with interested parties has not been addressed. The fact that the Administration may ultimately wish to retain the decision as to technical standards applying to submissions to the Government should not preclude consultation with parties who may be affected before any particular standards are specified.

Clause 18

11. It is not entirely clear that "designating an information system" does have an unequivocal meaning, because the meaning of the term "information system" itself may not be clear-cut. Could there, for example, be confusion between an information system and an element in an information system? The fact that an addressee has taken it upon himself to designate on information system would not necessary be the end of the matter if, because of uncertain terminology in the legislation, there were to be a significant risk of relevant parties getting their wires crossed.

    Regarding the reference to "comes to the attention" in clause 18(2)(a)(ii), the Administration's response could reflected more specifically in the legislation.

Clause 19

12. Closed network certification services, overseas certification authorities, etc. could be specifically excluded from some or all of the provisions of the Bill if a mandatory licensing scheme were to be preferred.

    Regarding references to overseas examples of similar provisions, see our comments in relation to the "Interpretation" section above.

    As indicated in Part 1 above, the draft Code of Practice recently published for consultation has not removed all our concerns in relation to clause 19(3)(b). In addition, the issue of the Director's discretion under clause 19(4) has not been referred to in the Administration's response.

Clause 29

13. We note that the Postmaster General is required to comply with most of the provisions of the Bill. However, the sanction provisions do not apply to him and it is not clear what action can be taken in the event of failures of compliance by the Post Office.

Clauses 35 and 38-39

14. We are considering the adequacy of the Draft Code of Practice in relation to these issues and will respond to the Administration separately from the consultation on the Bill if we have matters to raise.

Clause 41

15. Clause 41(2)(a) is very broad and vague. We are not entirely convinced that there is a reasonable balance between protecting the privacy of individuals and fulfilling the legitimate objectives of the legislation in respect of this part of the clause.