By post & e-mail

Our Ref.: C/LC, M1784 9 March 2001

Securities & Futures Commission,
12/F., Edinburgh Tower,
The Landmark,
15 Queen's Road Central,
Hong Kong.

(Attn: Mr. Andrew Procter, Executive Director)

Dear Sirs,

Consultation Paper on the Regulation of On-line Trading of Securities and Futures

In response to your letter of 14 December 2000 requesting for comments on the captioned Consultation Paper, I have pleasure in submitting herewith the Hong Kong Society of Accountants' comments on the proposals contained in the Consultation Paper.

We are grateful for the extended deadline granted to us for making our submission and apologise for any inconvenience that it may cause.

If you have any questions in connection with any points contained in our submission, we shall be very pleased to discuss them with you. Please contact Ms. Winnie Cheung, our Director of Professional Development, in the first instance.

Yours faithfully,

LEE KAI-FAT
REGISTRAR
HONG KONG SOCIETY OF ACCOUNTANTS

KFL/WCC/ky
Encl.

Hong Kong Society of Accountants

Comments on

"A CONSULTATION PAPER ON THE REGULATION OF ON-LINE TRADING OF SECURITIES AND FUTURES"

issued by the Securities and Futures Commission

Regulatory Approach and Guidance Note Definitions

[62. When the Guidance Note was published in 1999, the Commission set out its regulatory approach "that the fundamental principles of regulation for activities over the Internet are not premised on the use of a particular medium of communication or delivery". In particular, ***the Commission has taken the view that it will apply its principles and its rules in a technologically neutral manner. Those who provide electronic media for trading will not be presented with additional hurdles that disadvantage them when compared to those who use traditional media****...]*

(1) While we would agree with this principle, it is also true that the provision of electronic media for trading does present broking firms with additional risks, such as security risks associated with the use of the Internet; the risks of disclosure of private investor information; the risk of system breakdown or unavailability, etc. Broking firms should therefore be required to establish appropriate measures to adequately manage these risks if the end users - the investing public - are to be adequately protected. It would not be appropriate to view such requirements as "additional hurdles".

[63. Recommendation 1: The title and contents of the Guidance Note should refer to "Electronic Trading" rather than the "Internet". "Electronic Trading" should be defined to accommodate the use of any electronic medium, including the Internet, WAP or a combination of them. In addition, it is suggested that a pop-up box be used to display "a prominent warning message" at the time the relevant website is accessed, to meet the prominent disclosure requirement.]

(2) Given the recognition of different electronic medium for access to be provided in the definition, the requirements to display "prominent warning message" in a pop-up box may not be practical: e.g. there would be technical difficulties in displaying or downloading risk warnings, disclaimers, user agreement information, etc., via a mobile phone. Given such practical implications, the Commission may wish to re-consider and refine this recommendation.

(3) Examples of "Prominent Warning Message" may be published for the references of industry practitioners and for investor education. The Prominent Warning Message may include a link to SFC or eIRC websites to provide further opportunities to investors or Internet users to learn more about the underlying risks and issues of e-Trading.

Client Identification

*[67. Issues of how accounts should be opened in an on-line environment and how clients can be properly identified to satisfy the "Know Your Client Rules" (as detailed in sections 5.1 and 5.4 of the Code of Conduct) were discussed ... one major concern is whether a **face-to-face** approach for account opening should be required as part of this guidance.*

Recommendation 2: Client Identification

(i) It is recommended that the applicable sections of the Guidance Note be amended to indicate how a registered person might establish the true and full identity of their client.

*These options might **stipulate** that account opening either takes place:*

*(a) In a **face-to-face meeting** between the client and a person who is registered as a dealer's representative of the relevant firm; or*

*(b) A **reliable third party** verifying the true and full identity of the client (e.g. a Justice of the Peace, a notary public, a solicitor, a bank manager); or*

*(c) **Using certification services that are recognized by the Director of Information Technology Services** as detailed in the Electronic Transaction Ordinance. Currently, the only certification service recognized is the one available from the Hong Kong Post, who issues recognized certificates to support digital signatures for the authentication of the identity of Internet users; or*

(d) Using other identification services as the Commission should determine on a case by case basis as technology continues to develop.]

(4) In addition to the Code of Conduct referred in the text, section 4.1 of the Guidance Notes on Money Laundering issued in July 1997 also states that "... whenever possible the prospective customer should be interviewed personally ...". These requirements seem to suggest that a face-to-face identification will be required in order to satisfy the existing requirements. Thus even though transactions can be conducted on-line, the investors would still need to open an account with the brokers in person. In this context, the reference to reliable third parties (paragraph 67(i)(b)), such as notary public, solicitors, etc., would be superfluous: the instances where a broker need to rely on such third parties as an alternative to face-to-face identification would seem very limited indeed.

(5) For banks or other financial institutions that also provide stock broking services, the concept of relying on somebody else to perform the verification can be applied. The investor may have already undergone some form of identification process when they opened the original account. The Registered Person may therefore be able to place reasonable reliance on such verification that was performed by staff in other divisions. It may be more difficult for a Registered Person to rely on a third party to perform this task, and clear guidance, or even a code of practice, will need to be provided.

(6) Regarding the recommendation on the use of certification services in paragraph 67(i)(c), there appears to be a fundamental flaw in the assumptions: neither the Electronic Transactions Ordinance nor the Code of Practice for Recognized Certification Authorities specifically require Recognized Certification Authorities to perform face-to-face identification of their subscribers. Indeed, current commercial CAs are known to have issued certificates to subscribers without performing face-to-face authentication. Naturally, these certificates would have a lower 'trust level' compared to those that are issued after face-to-face authentication. However, the fact that a CA is recognized under the ETO does not automatically imply that a face-to-face identification is performed, which is what seems to be implied here. This is a significant issue because if the SFC takes this approach, then it effectively sets additional requirements for recognized CAs, which is beyond the remit of the SFC. The SFC can, however, determine a set of model Certificate Policy (CP) that is appropriate to support electronic trading activities, e.g. requiring face-to-face authentication as a mandatory identification mechanism. A CA can then decide, base on its own business model, whether or not to support this CP and if so to describe this in its Certificate Practice Statements (CPS).

(7) As regards client identification, the Guidance Note refers only to the use of certification services that are recognized by the Director of Information Technology Services. There is very little discussion about the use of digital certificates issued by other international CAs . Since the direction of HKSE is towards the development of a continuous global market and cooperation with other major overseas exchanges, the use of other recognized and regulated certification authorities is an important area which warrants further studies.

(8) Besides, industry practitioners may have proprietary means for client identification (e.g. user ID, password, login Tokens, etc.), which are also relevant considerations.

Client Agreements

[69. Recommendation 3 : Registered persons are required to ensure clients can readily access or obtain a copy of the Client Agreements on the Website]

(9) It should be advisable for Client Agreements published by dealers electronically to investors to be digitally signed by the dealer to ensure the integrity of the agreement content.

(10) The Commission may wish to alert Registered Persons to the potential difficulties in the display of certain character sets, e.g. Traditional vs Simplified Chinese, and to recommend that Registered Persons should made available such Client Agreement in both HTML and PDF formats (or any other formats that the Commission deems appropriate).

Suitability

[73. Recommendation 4: ... Registered persons are reminded that suitability requirements arise when they give advice or make recommendations to their clients. They must first ascertain the client's financial situation, investment experience, objectives and any other information disclosed through the due diligence process to the broker. They should only give advice or make recommendations that are suitable for the client, based on this information. Advice and recommendations will include outright solicitations or offerings, and may also include more ***subtle approaches****. The Commission takes the view that* ***in general, any offer, solicitation or notice****, which has been* ***individually customised*** *for the client,* ***will constitute a recommendation.****]*

(11) It is not unusual that on-line merchants will seek to 'customise' their interface to individual customers to provide so-called 'personalised experience'. In the case of an on-line broker, it is conceivable that it may wish to provide such features on its web-site, such as through the use of cookies or other mechanisms, to track individual users preferences, and customise the interface accordingly, e.g. to show those stock categories that an investor is interested in. The SFC may wish to consider this aspect, and provide clearer interpretation on what it consider as "subtle" and what would constitute a "recommendation" (e.g. whether providing price movement analysis / alerts to a known day-trader would constitute a recommendation).

Client Priority

[78. The SFC has been advised that it is technically feasible for an on-line dealer to prepare exception reports that highlight orders which were not processed according to the time sequence in which they were received. This is a useful tool for the dealers to ensure compliance with the client priority requirement.

Recommendation 6: ... In line with requirements 3.1 and 3.4 of the Code of Conduct, it is recommended that the Guidance Note be amended to ***require that dealers' systems have the capability to generate reports that highlight exceptions****. A* ***time sequence*** *for orders that were received, placed and executed is considered to be a minimum requirement of these reports. On-line broker's systems should be able to* ***differentiate orders in terms of fractions of a second (which would generally be at six decimal places) and assign unique reference numbers to each order for the exception reports****.]*

(12) While this is technically feasible, in practice it may be difficult to achieve. In essence, the actual feasibility depends on the design of the on-line trading system itself, and on the amount of information that it collects. It is important to understand that there are a number of time sequences relating to each trade, and the underlying reliability of these timestamps. For example,

the time that an order is input by the investor may be 'unreliable' in that the on-line broker will have no control over the setting of the system clock in the computer used by the investor. The next point of capture is when the order is received by the broker's own system. This time is controlled by the broker and can therefore be used, providing that the broker periodically synchronise/re-set the system clocks of its servers, etc, against a reliable reference source. This is particularly important if there are several channels for orders to be submitted. Further, the FIFO principle may be difficult to implement, for example if the broker uses straight through processing, or if an order is incomplete and therefore requires manual 'repair' prior to its release/execution.

(13) In addition, having the capability to generate exception reports may not be enough. There may also be a need for a way to ensure that such exception reporting routines are in fact operating as designed, as well as an effectively mechanism to review such reports and follow up unusual incidents. We recommend that the Commission should further refine recommendation 6.

Chat Rooms

[79. Recommendation 7(g): ... It is recommended guidelines should be put forward to the industry for consultation in relation to chat rooms provided and operated by licensed persons. The Guidance Note might be amended to reflect these guidelines.

(i) General disclosures

At a minimum, the operator of a chat room should post clear procedures detailing how the chat room operates and how activities are monitored.

(ii) Disclosures to people who read materials posted in the chat rooms

Users of material in chat rooms should be clearly alerted to the risks of relying upon on-line discussion forums or chat rooms for investment decisions. A "warning page" with full disclaimers should be inserted in a web area, prior to access to a chat room or bulletin board. The warning page should alert investors to the dangers of relying on this material to make investment decisions as it is not professional investment advice. The "warning page" should also inform the investor entering the chat room whether the opinions posted in the chat room are the opinion of the operator of the chat room.

(iii) Warnings to people who post material in the chat rooms

People who post materials in chat rooms should also be clearly warned that they are personally responsible for the accuracy and authenticity of the material they post in the chat room. They should also be warned that if their postings contain any misleading or deceptive information, persons acting on such information may take action against them. They should also be ***asked to state whether they have any interest in the securities*** *to which their postings relate, and if so, what their interests are.*

(iv) Obligations of the chat room operator

The operator of a chat room should be obliged to advise the SFC whether they are operating within the proposed chat room guidelines. The operator should also ensure that the chat room contains all the disclosures and warnings required and should provide a link to the SFC website and the SFC Electronic Investors Resource Centre

Only registered persons should be allowed to make postings about any securities or issuers on behalf of the firm or the chat room operator.

It is also proposed that the operators of chat rooms offer the SFC free access to their chat room, their members' information and postings. It would be helpful if the chat room had a suitable search function (e.g. search by key words, user and company names and dates of postings).

The chat room operator is ***expected to monitor the traffic*** *within the chat room. Chat room operators should certify to the SFC that they have reasonably adequate procedures and mechanisms to* ***properly identify persons making the postings****. They should also* ***monitor whether postings appear to be misleading or deceptive****, or likely to amount to illegal or unauthorised activities (e.g. market manipulation, unauthorised offering of securities), It is proposed that chat room operators be required to remove such postings and withdraw the access rights of the persons making those postings.*

It is proposed that operators of chat rooms notify the SFC immediately of any complaints they receive about suspicious postings and provide whatever information they may have of the identity of the persons responsible for the postings. Chat room operators would be expected to ***retain information about postings and the identity of the persons making the postings****, as well as other information which may be appropriate,* ***for a period of six months.****]*

(14) First, it is assumed that only licensed persons may operate such chat rooms. In reality, there exists a variety of chat rooms where information on stock is posted. There exists a possibility that particular chat rooms may be outside the regulatory powers of the SFC.

(15) Second, the recommendations set out the obligation of chat room operators in relation to the monitoring of the chat room traffic, their contents (whether they appear to be misleading or deceptive, etc.), the persons making the postings, and the storage of such information together with the identity of the persons making the posting for a period of six months. In reality, depending on the popularity of the chat room, the volume of postings may make such monitoring impractical from a cost point of view. It would be far easier for the SFC to simply discourage licensed persons from running chat rooms.

(16) Chat Room services may take up significant system resources and may even impact the availability of the core trading facilities. Guidance should be provided on how to monitor or mitigate the impact of this potential operational problem. At the least, the Chat Room network should be segregated from normal trading network to safeguard availability and security of on-line Trading system.

Record Keeping

[Recommendation 8: ... It is recommended that the Guidance Note should be amended to require that brokers maintain both audit logs and outage and delay logs.

Audit logs should document the order process and transaction flow through the trading systems ...

… The documentation and logs should be diligently maintained and be made available to the SFC upon request. It is important that the logs be reviewed regularly for detecting potential problems and planning preventive measures.]

(17) The volume of audit information could make this recommendation impractical, particularly with respect to the requirement for regular review of logs. There needs to be further consideration of the proper mechanism / framework to implement the control, review and reporting objective of this record keeping requirement.

System Integrity

[84(i). The Commission has stated its expectations in the Guidance Note (section 6.2) that registered persons must put in place additional operational measures if they intend to conduct on-line trading activities. The discussions with the Working Group, the results of the SFC survey and interviews indicate that there are a number of operational issues in relation to on-line brokers in Hong Kong ...]

(18) We agree that "system integrity" is key to protecting investors and preserving market integrity. As already indicated, system integrity covers a wide variety of aspects. However, this is an area that is traditionally weak - in the sense that it is not typically focused upon by management across a broad spectrum of industries. There is a concern that so long as the overall awareness of controls in respect of system integrity remains weak, there will be weaknesses within the policy and controls framework (the governance framework) of brokers. In this respect, the SFC may need to consider prescribing a set of objective, minimum requirements in order that broker firms

can follow. International standards, such as WebTrust, SysTrust, the ISO 17799, can be a useful set of generic guidelines in this respect.

Security

[84(i)(a). Recommendation 11(iii): Recommends the use of password equal to or longer than 8 characters or digits without setting a maximum limit.

(19) An unnecessary long password may lead to practical problem in usage and may even create the adverse effect such as users writing down their password, thereby weakening security. A password length that addresses the risks of the underlying processing environment is considered acceptable. The usual practice is to encourage the use of between 6~8 alphanumeric character passwords.

(20) The list seems too "Low level". For a "Low level" list, anti-virus countermeasures should definitely be one of the requirements.

The following additional areas may also be included:

- the number of password history to be kept (eg 6) in order to restrict the reuse of previous passwords
- the maximum number of invalid login attempts (eg 3) before automatic lockout of an user ID
- automatic time-out after a certain period of inactivity
- regular review of user profiles and access rights granted.

(21) Consideration should be given to address the need to and criteria for assessing service organizations if the dealer is employing the services of outside service providers.

Contingency plan

[84(i)(d). Recommendation 14: Both onsite and offsite backup copies should be maintained]

(22) Periodic restore and backup testing should also be recommended to ensure that data in backup media is recoverable in case of emergency data restoration.

IT Competency

[84(ii) In some cases, due to the aggressive development and implementation schedules of on-line trading systems, ***some firms may not have ensured that the necessary infrastructure is in place*** *so that they have the Information Technology ("IT") as well as Human Resources competence to manage the on-line trading operations. Senior management should recognise that they carry the responsibilities that arise from the launch of on-line trading, the ongoing operations, and with that the management of IT capability. This leads to the whole issue of integration of the IT functions into a firm's regulatory and compliance control procedures. The IT department now has a key role to play in delivering compliance services and satisfying regulatory requirements. From a regulatory point of view,* ***there is a real need to be satisfied of IT competence as part of the "fit and proper" assessment for a registered firm engaged in on-line trading****.]*

(23) We concur with the observation that some firms may not have the necessary infrastructure: the people, process and technology, needed to support the on-line trading operation. Looking at just the people element, we are of the view that competent IT personnel are in short supply, and shall remain so at least for the immediate future. Historically, there had not been any specification of IT competency, and if the SFC were to proceed with this recommendation, then we feel that this requirement would effectively present "additional hurdles" to those providing electronic media for trading, at least in the short term, which is what the SFC seeks to avoid. The SFC should therefore carefully consider the implementation timeframe of this recommendation, as well as working with the interested parties to define a set of "recognised" IT qualifications.

Standards and Independent Reviews

[Recommendation 10: System Integrity ... As system integrity lies at the heart of both investor protection and integrity of the market, it can be argued that regulators should set detailed minimum standards. The implementation of this would of course have to be supervised. In many instances, ***regulators may not have the resources or the expertise*** *for this approach. Moreover,* ***a "one size fits all" set of standards may be inappropriate*** *as different types and level of service may require different standards ...*

… The Commission notes that the Hong Kong Monetary Authority on 6 July 2000 issued a Guidance Note on the "Management of Security Risks in Electronic Banking Services". In September 2000, the HKMA then issued a new Guidance Note entitled "Independent Assessment of Security Aspects of Transactional E-banking Services" which supplemented the July 2000 Guidance Note. In this later Guidance Note, the HKMA has called for ***independent assessments to be carried out by trusted independent experts*** *which may also include independent parties within the firm (such as an Internal Audit Department) before the launch of the e-banking services. Such assessments will be conducted thereafter* ***generally at least once a year, or whenever there are substantial changes to the risk assessment of the services or in the major security breaches****. The assessments should cover the following topical areas: information security policies and practices, system and network security, business continuity management.*

The Commission is also considering a second initiative; whether it should require a registrant to obtain an independent certification of its systems...

… The Commission recognises that if the requirement for certification is implemented, this will represent additional costs to the industry. However, based on the special inspections conducted, the Commission believes system integrity is an issue that many brokers have not come to grips with ... the Commission believes that this area should be periodically reviewed and that reviews by ***qualified independent assessors*** *may be the most appropriate way to achieve this. The Commission specifically invites comments on the desirability of* ***independent certifications of systems****.]*

(24) The issues of standards and independent assessment are discussed under "system integrity". Firstly, on the subject of standards, we agree that a "one size fits all" set of minimum standards may not be appropriate. However, it is possible to establish a set of controls principle that all brokers that provide on-line trading should adhere to. Although these will be at a higher level, the onus will be on the individual brokers to assess the specific risks that they are exposed to under each of the principles, and then to demonstrate that an appropriate controls framework has been establish to manage the risks.

(25) Secondly, while we support the idea of independent assessment, it is essential for the SFC to work with the potential reviewers (internal auditors, external auditors, IT professionals) who may be conducting such assessments. It is essential that a consistent approach is taken in respect of the scope of the assessment, and the basis for evaluating / reporting any findings. Issues such as independence, professional standards / practices, etc., should also be considered.

(26) Finally, the subject of independent certification of system is a complex one. The fundamental difficulty is in determining what it is that needs to be certified. In this context, "system integrity" is too vague a term to be of much use; there need to be clear criteria established. Here lies a further complication: how to balance the cost of the certification against the level of comfort / assurance desired by the SFC. While this idea is potentially workable, it would be a lengthy process to define the scope for certification that is both acceptable to the SFC (from a scope perspective) and the industry (from a cost perspective). Once the scope is defined, then the SFC can proceed to determine who would be best qualified to conduct the independent assessment / certification.

[Recommendation 10: System integrity.…… The first initiative the Commission is considering is a requirement that registered persons complete a checklist and provide a standard declaration of system integrity that is approved and signed off by senior manager.]

(27) Completion of a standard check list and standard declaration obviously gives little comfort of the overall system integrity. Dealers' environment will be different, and one checklist will not fit all. There may also be different interpretation being placed on the questions being asked by the checklist. Further, the checklist approach will easily be turned into a routine process which will further reduce the effectiveness of the assurance that it is hoped to provide. We do not believe that a checklist approach would achieve the intended objective.