POLICIES ON DIRECT ELECTRONIC ACCESS

Consultation Report

TECHNICAL COMMITTEE
OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FEBRUARY 2009

This paper is for public consultation purposes only. It has not been approved for any other purpose by the IOSCO Technical Committee or any of its members.

Foreword

IOSCO is pleased to publish the consultation report prepared by the Technical Committee in relation to policies on direct electronic access. This consultation report sets forth elements regarding possible principles pertinent to direct electronic access, including those that address pre-conditions for direct electronic access, information flow, and adequate systems and controls. Comment is sought on these three topics. In addition, we encourage commenters to address any issue they deem relevant to the issue of direct electronic access as described in this consultation report.

How to Submit Comments

Comments may be submitted by one of the three following methods **on or before 20 May 2009**. To help us process and review your comments more efficiently, please use only one method.

1. E-mail

- Send comments to Greg Tanzer at DEAReport@iosco.org.
- **The subject line of your message should indicate "Policies on Direct Electronic Access."**
- Please do not submit any attachments as HTML, GIF, TIFF, PIF or EXE files.

OR

2. Facsimile Transmission

Send a fax for the attention of Mr. Greg Tanzer, using the following fax number:
+ 34 (91) 555 93 68.

OR

3. Post

Send your comment letter to:

Mr. Greg Tanzer
IOSCO General Secretariat
C / Oquendo 12
28006 Madrid
Spain

Your comment letter should indicate prominently that it is a "Public Comment on Policies on Direct Electronic Access."

Important: All comments will be made available publicly, unless anonymity is specifically requested. Comments will be converted to PDF format and posted on the IOSCO website. Personal identifying information will not be edited from submissions.

POLICIES ON DIRECT ELECTRONIC ACCESS

I. Introduction

In April 2007, the Technical Committee (TC) of the International Organization of Securities Commissions (IOSCO) approved a mandate on direct electronic access (DEA) to exchanges and other markets submitted by the Technical Committee's Standing Committee on the Regulation of Secondary Markets (TCSC2) to: (1) conduct a fact-finding survey of direct electronic access models in TCSC2 member jurisdictions; (2) compile the survey results and compare and analyze the various access models and the rules that apply; and (3) determine whether it is appropriate to give guidance regarding direct electronic access.

As TCSC2 undertook its work, it became clear that work related to intermediary practices should also be taken into account. Accordingly, in November 2007, the TC approved a related project mandate for its Standing Committee on the Regulation of Market Intermediaries (TCSC3) to survey intermediaries with respect to how they permit direct electronic access to markets. The mandate approved by the TC authorized TCSC3 to summarize those responses, highlight relevant issues, and coordinate and work with TCSC2 as necessary in determining whether IOSCO should publish guidance with respect to DEA. This Report reflects the work of both TCSC2 and TCSC3.

The Report sets forth elements regarding possible principles pertinent to DEA, including those that address pre-conditions for DEA, information flow, and adequate systems and controls. Comment is sought on these three topics. In addition, we encourage commenters to address any issue they deem relevant to the issue of direct electronic access as described in the Report.

II. Background and Purpose

As the way in which exchanges and other markets operate has evolved, so too has the means of access to these markets.[1] Securities and derivatives exchanges are overwhelmingly electronic, which has facilitated their operations globally through various forms of communication. Spurred by the increasing demand by customers[2] for access to global markets, the means to access markets has evolved through continual innovation.

There are divergent understandings of the term "direct electronic access" (DEA). Nonetheless, there is general agreement that DEA falls into two key categories: intermediated and non-intermediated.

For purposes of this Report, "intermediated" DEA generally refers to:

(a) Customers being given direct access to the market through a registered intermediary's system/infrastructure, *i.e*. automated "order routing;" or

(b) Customers of an intermediary being given direct access to the market without going through the intermediary's system/infrastructure, *i.e*., "sponsored" access.

In either case, however, the order is sent to the market as the intermediary's order, *i.e*., using the intermediary's trading ID (aka mnemonic). The intermediary therefore retains full responsibility for the order.

Non-intermediated direct access generally refers to markets providing direct access to non-intermediaries (*i.e*., parties other than registered brokerage firms), as market-members and in that capacity connecting directly to the market, without going through an intermediary. The Report refers to this type of DEA as direct access by non-registrant/non-intermediary market-members.

Thus, DEA, as used in this Report, refers to automated order routing systems, sponsored access, and direct access by non-registrant/non-intermediary market members. We recognize that the latter category may not always raise the same issues when compared to the other two. For example, there may be less of a concern with regard to compliance with market rules. Nonetheless, as noted later in this report, *credit risk* is a key concern raised by DEA arrangements and the non-registrant/non-intermediary market-member poses potentially substantial credit risk to the clearing firm that is also a member of the market.

The ability to transmit orders directly to a market in real time gives DEA users greater control over their trading decisions and reduces latency of execution time. Overall, the different means of accessing markets electronically has facilitated the establishment of a globally competitive market, and has greatly benefited market participants and their Customers by permitting them to transact complicated investment and hedging strategies on a global basis in a matter of

---

[1] For purposes of this Report, the term "market" refers to exchanges and alternative trading facilities.

[2] See definition in Appendix I

milliseconds. The use of electronic systems also has regulatory benefits, such as the generation of electronic audit trail data, and the enhancement of both trade transparency and the ability of markets, intermediaries and other market members to develop and apply automatic risk management controls.

Nonetheless, the work undertaken by TCSC2 and TCSC3 has identified areas of concern where market authoritie[3] may determine that guidance is appropriate. For example, DEA has introduced several regulatory challenges to markets, intermediaries and their regulators. Although the nature of the challenges varies depending upon the type of DEA, they include:

- Allowing users to access markets outside of the infrastructure and/or control of market intermediaries, which challenges intermediaries' traditional risk management approaches and may make rule compliance and monitoring more difficult; for instance regarding market manipulation and insider dealing

- The creation of incentives for intermediaries/Customers to gain execution advantages based on the type and geographic location of their connectivity arrangements, which raises potential "fairness;" and

- Facilitating algorithmic trading through automated systems, which raises issues of capacity and the potential need for rationing bandwidth. Indeed, some "black box" trading systems are capable of transmitting several thousand order messages to a market in less than a second.

This Report describes current DEA arrangements, as well as the regulatory approaches of TCSC2 and TCSC3 member jurisdictions. It also identifies the commonalities and differences in approaches as they relate to the controls imposed by intermediaries on Customers' direct access to the market for purposes of placement of orders and intermediaries' ability to review trades on a pre- or post-execution basis[4]. However, the Report does not attempt to describe in technical

---

[3] The term "market authority" is used to refer to the authority in a jurisdiction that has statutory or regulatory powers with respect to the exercise of certain regulatory functions over a market. The relevant market authority may be a regulatory body, a self-regulatory organization and/or the market itself.

[4] Broader issues raised by screen based trading systems (*e.g.*, issues of system integrity and capacity) were addressed previously by the Technical Committee and thus are not the focus of this Report. *See* IOSCO *Principles for the Oversight of Screen-Based Trading Systems*, Report of the Technical Committee of IOSCO, June 1990 (Screen-Based Principles Report); and *Principles for the Oversight of Screen-Based Trading Systems for Derivative Products-Review and Additions*, Report of the Technical Committee of IOSCO, October 2000, at p. 5, section III, Part 1, available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD111.pdf (2000 Report). In the 2000 Report, the Technical Committee adopted four additional principles that encouraged regulatory authorities to develop cooperative arrangements to address risks that arise from cross-border derivatives markets, to share relevant information in an efficient and timely manner, to maintain a transparent framework for regulatory cooperation, and to take into account a jurisdiction's application of the IOSCO Objectives and Principles of Securities Regulation. *See also*, *Policies on Error Trades*, Report of the Technical Committee of IOSCO, October 2005, available at http://www.iosco.org/library//pubdocs/pdf/IOSCOPDF207.pdf.

detail the specific features of the multitude of DEA systems in existence.[5] Indeed, the technical nature of electronic access systems is complex, varied and constantly changing. It is hoped, however, that publication of this report will facilitate a better understanding of the different ways that direct access is regulated and how markets address the relevant issues.

The Report identifies and discusses the benefits, potential risks and concerns that are associated with the use of DEA arrangements that permit Customers of intermediaries and non-intermediary market-members to enter orders directly into a market's trade matching system for execution. It also evaluates the information obtained from markets, intermediaries, and market authorities, both in response to written questionnaires and presentations.

III. Relevant DEA Arrangements

TCSC2 and TCSC3 were confronted by a diversity of terminology used to describe the specific arrangements of DEA in various jurisdictions and markets (*e.g.,* "direct access", "direct market access", "pure direct market access", "intermediated access", and "sponsored access"). It was learned that these terms of art may be understood by market participants in a particular jurisdiction as having a specific meaning in relation to local market structures. These terms, however, may either not reflect the DEA arrangements that exist in *other* jurisdictions or, even if used, have a different meaning. Both TCSC2 and TCSC3 attempted to manage this problem and avoid confusion by adopting similar definitions within their surveys. *See Appendix 1.*

However, for both surveys (and thus also for this Report), the trading model of a Customer calling the intermediary or sending an internet order to the intermediary was not considered to be "direct access."[6]

---

[5] In general, the basic technical variations in electronic access range from the "restricted" model of a market providing dedicated communication lines to the trading system as well as all trading software and hardware, to more "open access" models where the market permits access through a combination of means, such as dedicated lines and internet, and allows connections using proprietary market software and hardware, proprietary brokerage software and hardware, third-party vendor software and hardware solutions. In this regard, the responses indicate that most markets generally do not restrict the type of end-user technology. In all cases, each market requires that any direct connections to its trading system meet such market's standards.

[6] In these instances, only the intermediary, who is member of the market, has the capacity to communicate electronically with the market through a messaging system to place an order directly into the market's trading system. Other distinguishing characteristics between this arrangement and the DEA arrangement described in this Report may include:

•DEA excludes human intervention, including retail orders placed over the Internet that may involve some human intervention.

•Retail Customers do not have access to electronic messaging formats that communicate DEA orders, such as the Financial Information eXchange ("FIX") protocol. The retail Customer can only send orders through the intermediary's website.

•The retail Customer does not enter into a DEA agreement with the intermediary and/or the market (such agreements are described later in the summary).

•The retail internet Customer does not have access to an electronic order management system.

A Customer calling the intermediary or sending an internet order to the intermediary is not considered to be DEA because although the Customer's trading is intermediated, it is not "direct access." Although the

For the purposes of this Report, DEA is defined as the following three major pathways:

- **Automated Order Routing Through Intermediary's Infrastructure (AOR)**

  This describes a situation where an intermediary, who is a market-member, permits its Customers to transmit orders electronically to the intermediary's infrastructure (*i.e.*, system architecture, which may include technical systems and/or connecting systems), where the order is in turn automatically transmitted for execution to a market under the intermediary's market-member ID (mnemonic). In this case, the intermediary retains the ability to monitor internally and, if necessary, stop an order before it is executed. Such access is often referred to as "automated order routing."

- **Sponsored Access (SA)**

  This describes a situation where an intermediary, who is a market-member, may permit its Customers to use its member ID (mnemonic) to transmit orders for execution directly to the market without using the intermediary's infrastructure. In this case, the intermediary is not able to use the internal controls applied with respect to AOR (*e.g.*, does not have a real time view and cannot stop an order).

- **Direct Access by Non-Intermediary Market-Members**

  This describes a situation where an entity that is not registered as an intermediary, such as a hedge fund or proprietary trading group, becomes a market-member, and in that capacity connects directly to the market's trade matching system using its own infrastructure and member ID (mnemonic). Such non-registrant members are generally not eligible to become a clearing member of the market and must enter into a clearing arrangement with and become a Customer of a clearing member intermediary.

IV. Description of DEA Arrangements

A. Introduction

The various permutations of DEA described above, and in particular AOR and SA, could widen the class of persons able to enter orders directly into a market's trade matching system. In addition, although TCSC2's survey revealed that some markets continue to require that their members be registered intermediaries, other markets permit a broader class of entities to become

---

intermediary itself may connect directly to the exchange, the requirements for, and the risks that may flow from direct access trading by registered intermediaries is not the focus of the mandate. Moreover, broader issues raised by screen based trading systems (*e.g.,* issues of system integrity and capacity) have been addressed previously by the Technical Committee. *See* Screen Based Principles Report, *supra* note 4 and 2000 Report, *supra* note 4 at p. 5, section III, Part 1.

DEA participants/ market-members, *e.g.,* non-intermediaries. A majority of markets responding to the TCSC2 survey believe that the way they permitted DEA does not introduce unmanageable risks.

B. Intermediated Direct Access (automated order routing/sponsored access)

(1) Introduction

Although the use of DEA continues to increase, the number of DEA Customers appears to be relatively small as a percentage of all Customers.

Intermediaries in five of the ten responding jurisdictions permit SA. However even in North America, where the extent of SA is greater than in many other jurisdictions, a number of intermediaries indicated that they do not permit such access at all.

In some jurisdictions, "service bureaus" play a significant role in DEA. Service bureaus are technology companies that provide order-routing and connectivity services for both intermediaries and institutional Customers[7]. The service bureaus enter into agreements with markets that authorize their electronic connections. In essence, they function as the electronic front end that directs orders to a particular market, and can under some circumstances be viewed as an extension of the technology infrastructure of intermediaries. The use of service bureaus by intermediaries can be seen as an outsourcing of functions that are normally performed internally (possibly including pre-trade controls). Service bureaus may be used in both AOR and SA.

(2) Qualifications of Customers

AOR and SA are granted by the intermediary; however, the specific approval of markets may also be required. Where such specific approval is not required, the market and/or market authority generally requires the market-member to ensure that the Customer has, *e.g.*, the appropriate financial resources, familiarity with the rules of the market, and knowledge of the trading system and proficiency in the use of that system. These requirements may differ between AOR and SA arrangements. For example, in SA arrangements, some markets restrict Customer access to certain types of institutional investors (including portfolio managers and financial institutions).

In general, market-members who are intermediaries have discretion over which of their Customers are given direct market access, provided such Customers meet certain terms and conditions outlined below, which are typically set in written contractual agreements (see V.B.2 below). Intermediaries generally use a vetting process to determine on a case by case basis which of their Customers will be permitted to have DEA. A key element of this vetting process is an analysis of the entire risk profile of the potential DEA Customer, particularly with regard to sponsored access. The Customer's internal systems of monitoring their own risk are closely reviewed by the intermediary, including whether the Customer has adequate systems and

[7] Service bureaus, because of their different revenue model, generally are not in competition with exchanges, Electronic Communication Networks, Alternative Trading Systems or broker-dealers.

controls to monitor orders and trades on a real-time basis. In addition, intermediaries report that they review closely some or all of the following factors before granting DEA to their Customers:

- Familiarity with market rules;
- Degree of financial experience;
- Prior sanctions for improper trading activity;
- Evidence of a proven track record of responsible trading and supervisory oversight;
- Ability to meet appropriate credit and risk guidelines;
- Minimum thresholds for assets under management; and
- Proposed trading strategy and associated volumes.

Intermediaries in approximately half of the responding jurisdictions grant direct access to markets only for Customers that are financial institutions, such as broker/dealers, asset managers, banks, introducing brokers, or other types of entities that are supervised or regulated as a financial institution within the jurisdiction. But even where an intermediary permits non-financial institutions to have DEA, it will nonetheless require a certain minimum level of investor sophistication.

Few intermediaries stated that they would permit retail participation.

Some markets permit sub-delegation of a Customer's DEA access to another party, *i.e.,* where a DEA Customer is permitted to delegate its access privileges directly to another Customer. This is used primarily to accommodate structures of the market-member whose affiliates have DEA Customers outside of the jurisdiction. There are rarely any specific market rules to regulate the sub-delegation.

(3) Identification of DEA orders

Markets assign each market-member a mnemonic (identifier or "designated code"); and users must input a username and password to access the market trading system. However, most markets' electronic systems do not identify through the market member's IP address or mnemonic the specific Customers of market-members using AOR or SA, *i.e.*, their systems do not support sub-user identifiers or passwords.

C. Direct Access by Non-intermediary Market Members

Markets generally impose two broad types of requirements with regard to non-intermediary market-members[8]. These include (i) qualifications of key individuals such as requisite training or competency and "fit and proper" standards; and (ii) structure, management and resources of the applicant. This latter category generally includes: adequacy of internal controls financial resources, technical systems and operational controls; certification of system requirements; and integrity of order routing systems.

[8] Market members that are registered intermediaries also need to meet the same kind of requirements.

Since such a non-intermediary market-member is generally not eligible to become a clearing member, markets will generally require a contractual arrangement between the non-intermediary member and a clearing member. Some markets are party to the same contractual agreement ("tripartite agreement"). Those contractual agreements set out the respective responsibilities of the parties with regard to, among other things, risk management expectations, position limits and, for some markets, filters.

V. Risks/Concerns associated with DEA Arrangements

A. Introduction

Trading and credit risks are the key concerns raised by DEA arrangements. Trading risk can generally be described as the risk to an intermediary regarding compliance with market rules applicable to orders sent to the market and executed on behalf of its DEA Customers, whether this is done through AOR or SA. This type of risk will generally not exist for the intermediary who simply clears for a Customer who is a member of the market.

On the other hand, credit risk, generally described as the risk that an intermediary is normally financially responsible for the trades of a Customer, exists for both clearing and non-clearing members, although the clearing firm may bear the most pronounced risk as it bears ultimate financial responsibility for a trade (although the intermediary is financially responsible to the clearing member).

B. Market Integrity / Compliance with market rules

(1) Market Perspective

All markets that allow their members to offer Customers DEA by way of AOR/SA indicated that the market-members remain fully responsible for the orders entered by their Customer. For all markets that allow DEA, the market-member is thus subject to the market disciplinary procedures whether orders are entered by the member or "through" the member.

All markets can impose disciplinary actions upon a market-member for a failure to comply with applicable rules, including those relating to DEA. A number of different penalties, ranging from warnings - for less severe violations - to the revocation of the permission to trade, were mentioned in this context. The market can require the market-member to deny DEA access to a particular Customer or to exclude a particular Customer from using the system for a certain time.

Markets do not generally have the authority to take disciplinary actions directly against non-members, *e.g.*, the DEA Customers of members, whether or not they are registered intermediaries. In addition, clearing firms (also regulated intermediaries) are generally not held responsible for violations of market rules by the Customers for whom they clear (whether such Customers are registered intermediaries or not), but assume credit risk for all DEA Customers,

whether market-members or not (a point made by a number of intermediaries, as noted in the following section). Markets, therefore, focus their compliance efforts on their market-member's responsibility and capacity to monitor the member's Customers who access the market.

Some markets expressed concern about their inability to take disciplinary action against a non-member, *i.e.*, the DEA Customer of an exchange member. The lack of jurisdiction by markets over persons accessing the markets, especially under sponsored access arrangements, may be problematic when such a sponsored access client engages in manipulative trading practices but the responsible intermediary is found to have in place fully adequate policies and supervisory procedures. The concern expressed was that even though market rules may provide that market-members are responsible for their Customers' trading through DEA, it may be difficult to prosecute an intermediary for the underlying violation of the market rules caused by the Customer and instead, actions may be taken to sanction the market-member for a lack of supervision of trading. In fact, it may be difficult for a market authority to prove that the intermediary had inadequate policies and procedures in place. It should be noted, however, that in all TCSC2 and TCSC3 member countries, the relevant statutory regulator has jurisdiction over any person engaged in fraudulent trading practices on a market, whether a market-member or not.

Another factor that complicates enforcement of market rules in the DEA context is that most market electronic systems do not identify the particular Customers of market-members who may have SA or AOR (*i.e.*, the systems do not support sub-user identifiers or passwords). Indeed, some markets even permit the sub-delegation of a Customer's DEA access to another party.[9] This may delay the process of an investigation if the market authority seeks information to identify the ultimate Customer or user. Additional complicating factors include increased volume and complexity of information caused by algorithmic trading, a key tool of DEA. As a result of all this, investigations may take much longer.

(2) Intermediary Perspective

A number of intermediaries stressed the importance of trading risk. Specifically, the market authority will hold the intermediary responsible for the violation of any trading rules imposed by the market. One North American intermediary expressed particular concern about possible violations of SEC or other rules pertaining to trading conduct – for example, improper trading designed to manipulate the closing price. As the intermediary for such a trade, it will be held to account for any problematic trading activity performed by its Customer.

Most intermediaries enter into written contractual agreements with their DEA Customers, the purpose of which is to restrict, condition or otherwise control how their Customer utilizing their infrastructure may transmit orders, as well as to seek to ensure compliance by their DEA Customers with market rules. Some of the key terms and conditions contained in such contracts include the following:

---

[9] This is used primarily to accommodate structures of the market-member whose affiliates have DEA Customers outside of the jurisdiction. However, there are rarely any specific rules that govern such sub-delegation.

- Provisions that address the respective rights and liabilities of the parties such as statements that the Customer accepts all liabilities resulting from DEA use (including use of identification codes, settlement and delivery).

- Provisions relating to the security (physical and IT security) of the infrastructure (user identity, passwords, authentication codes, etc.), to avoid unauthorized system access;

- Limits that are expressed as a notional amount for each Customer above which the orders are rejected by the system, as well as by reference to the maximum amount per order/per user;

- Warranties, indemnities, charges and Customer/product specific conventions;

- Conditions (such as for entering orders, error trade policies, etc.) and restrictions such as the right to suspend the service, to reject or cancel orders, etc.;

- Use of specific standard format for order routing such as SWIFT or FIX;

- A requirement to have knowledge of trading rules and applicable laws and regulations or a requirement to comply with these;

- A requirement that the Customer's users are authorized, qualified and competent.

These terms and conditions are usually standard in terms of restrictions, conditions and controls although most intermediaries clarify that they are adapted to the business relationship with the Customer and the type of service provided (dealing services, clearing services, prime brokerage).

In addition, most intermediaries are required to have in place proper procedures and policies to monitor DEA Customers and their trading activities. For example, as discussed in section (3) below, most intermediaries have in place pre-execution controls, such as filters, plausibility and security checks for intermediated trades. Trade monitoring is usually applied in a consistent manner, also through the compliance function, regardless of the trading pathway.

C. Risk Management

(1) Introduction

Credit risk is a key risk management concern. It is generally described as the risk that an intermediary may be financially responsible for the trades of a Customer. Some industry representatives at meetings held by TCSC2 and TCSC3 emphasized that non-clearing market members presented essentially the same degree of *credit risk* to a clearing firm as a DEA Customer of an intermediary. A number of intermediaries who responded to the TCSC3 questionnaire made the same point.

As an example, one North American based firm indicated that compliance or regulatory risks are more pronounced when a Customer that is not a market-member places orders directly on a

market in the name of the intermediary, and that credit risks are more pronounced where the Customer, who has DEA, is a non-clearing member of the market.

Concerning the question of credit risk in a situation where the intermediary only provides clearing services for the Customer, the firm noted that the clearing intermediary bears ultimate financial responsibility for a trade. That is, if the Customer cannot deliver sufficient cash and/or securities to settle and clear the trade, the intermediary will be expected to do so.

It should be noted that financial risks also exist for the non-self-clearing intermediary with the non-member DEA Customer since the trade is technically that of the intermediary; and therefore the intermediary is ultimately financially responsible to the clearing member for the trade.

In most jurisdictions, primary responsibility for overall credit control and risk management, including with regard to DEA, is the responsibility of the market-member and the market member's clearing firm (collectively referred to as the "Responsible Firms"), and the clearance and settlement (C&S) entity,[10] but *not* the market. Although C&S entities do not assume *per se* the risk management obligations of intermediaries specifically with regard to DEA, they do play an important supporting role. Indeed, in response to the TCSC2 survey, a large number of jurisdictions stressed the important role played by C&S entities vis-à-vis an intermediary that is a member of the C&S entity and either is self-clearing or clears on behalf of other intermediaries. The C&S entity will have systems in place to manage risk, including the imposition of trading and position limits, the setting of margin requirements, as well as collateral control and monitoring the financial health of its clearing members.[11]

Where there is automated order routing, *i.e.*, where orders are sent through the intermediary's infrastructure, the intermediary has the opportunity and time to implement its risk management protocols, including pre-trade controls. However, even then, the speed of electronic execution narrows to milliseconds the available time for traditional risk management and error trade detection and response. In SA situations, *i.e.*, where orders are transmitted to the exchange trade matching system outside the intermediaries' infrastructure, the ability of the responsible firm to conduct robust risk assessment, particularly on a pre-trade basis, is even more limited in the absence of software risk management functionalities engineered into the execution path to the markets. This magnifies, *e.g.*, the potential negative effects of a mistake (*e.g.* errant algorithm) or of a Customer exceeding credit limits.

---

[10] The term "clearance and settlement entity" refers in general to both a central counterparty, *e.g.*, the National Securities Clearing Corporation located in the United States, and a central securities depository, *e.g.*, the Depository Trust Company, also headquartered in the United States.

[11] As previously noted in the report, *Recommendations for Central Counterparties,* Final Report of the IOSCO Technical Committee and the Committee on Payment and Settlement Systems, November 2004, available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD176.pdf, a central counterparty has the potential to reduce significantly risks to market participants by imposing more robust risk controls on all participants and, in many cases, by achieving multilateral netting of trades. It also tends to enhance the liquidity of the markets it serves, because it tends to reduce risks to participants and, in many cases, because it facilitates anonymous trading.

Although competition appears to be driving major markets to implement the risk management tools desired by intermediaries,[12] differences remain in the risk management functions made available by markets and C&S as part of their electronic trading systems. The regulatory issue is whether market authorities should specifically identify the type of controls (*e.g.*, filters) that trading systems should make available for risk management purposes.

12 Eurex trading platform release 11.0 combines trading (order entry), risk management (risk exposure, including the ability to stop specific traders from continuing to trade) and post-trade clearing (margin, settlement netting) functionalities. *See* http://www.eurexchange.com/r11/functional_features_en.html. Among other things, Eurex permits members to trigger a "stop" action on individual trader IDs, which encompasses both individuals and algorithms that run under specific trader IDs. Triggering a "stop" action will make it impossible for the Trader ID to engage in any further trading activities and will delete all open orders preventing any increase in risk of that trader ID. See http://www.eurexchange.com/r11/functionalfeatures/risk/stop_button_en.html.

(2) Current Practices: Market Perspective

Survey results indicate that markets recognize the critical need for Responsible Firms to have in place risk management controls and procedures. Indeed, markets appear to have implemented a spectrum of policies to facilitate the establishment of the necessary systems.

Some markets articulate high level principles setting out broad risk management expectations. Accordingly, these markets require market-members offering DEA to their Customers to implement procedures that are intended to achieve certain risk management objectives, but do not impose any detailed or specific parameters to achieve such objectives. Typically the absence of detailed risk management/internal control requirements reflects an approach that Responsible Firms should be permitted the flexibility to make credit judgments and establish controls that are consistent with the overall structure and business philosophy of the market-member or clearing firm.

Others markets set forth more detailed expectations. For example, they may enumerate a list of expected controls, such as monitoring capabilities and the ability to set credit control parameters (e.g., trade quantity limits, position limits, exposure limits, loss limits, and eligible products and instruments) and the ability to adjust control values and parameters in real time during a trading session.

Although many markets' execution systems include numerous functionalities, including a variety of pre-trade controls[13] (e.g., filters,[14] real-time drop copy notification of trades and "stop trade" functions) that facilitate the Responsible Firm's risk management functions, the availability for such enhancements varies between markets. For example, the TCSC2 survey found much disparity in the availability of markets system functions that provide intermediaries the ability to monitor trades on a real-time basis (although in some jurisdictions it is the C&S that monitors trades).

With regard to the adequacy of both pre- and post-trade information, most markets believed that the scope of such information as well as the timeliness of such data was sufficient for risk management purposes.[15] In contrast, a number of intermediaries offering sponsored access stated that they do not receive from markets sufficient system tools or data of a sufficient scope and timeliness to enable them to implement effective real-time, pre-trade risk management controls. These matters will be discussed in more detail below in section (5).

---

13 *See, e.g., supra* note 12.

14 Some markets have concluded that automatic filters should be made part of a DEA system. Again, there is a range of requirements that vary with regard to which party provides the filter (*i.e.*, the market or the market member) and what elements should be made part of such a filter.

15 Survey responses did not specifically enumerate in all cases the types of information provided.

(3) Current Practices: Intermediary Perspectives

Intermediaries appear to manage the risks posed by DEA using a three-pronged approach: (1) an analysis of the potential DEA Customer (*e.g.*, history, creditworthiness, etc), (2) pre-execution risk controls, and (3) post-execution controls. Each of these three mechanisms must work together to provide a comprehensive risk management program.

Of the three risk management tools available to the intermediary, the first - analysis of the Customer- is sometimes described by intermediaries as the most critical, since it is not possible to impose meaningful pre- and post-execution risk control measures unless the intermediary has a comprehensive understanding of the Customer's risk profile. For example, an intermediary might place different pre- and post-execution controls on a Customer who is a large global firm trading on different markets (and which may be using trades in one market to hedge against a position in another jurisdiction), as compared to those that might be imposed on a smaller firm that trades on only one market. Moreover, because the intermediary is ultimately responsible for the orders placed by its Customers on the market, such intermediaries review closely the extent to which Customers seeking DEA have appropriate risk management tools in place to handle DEA.

All intermediaries who responded to the TCSC2 and TCSC3 surveys reported monitoring trades on both a pre- and post-trade basis, but monitoring on a pre-trade basis took various forms. Moreover, some intermediaries that require their Customers to use the intermediaries' infrastructure indicated that one of the reasons for not permitting "sponsored access" was due to the inability of the intermediary under such circumstances to impose sufficient pre-execution risk controls. Most intermediaries reported that pre-trade controls, at a minimum, included protection against orders placed in error, sometimes referred to as "fat finger" protections. Other common pre-execution controls included "abnormal activity" alerts, and filters that provide for a maximum order size.

Intermediaries also reported that their risk management systems are designed in a way to respond immediately to increasing risk presented by a Customer's trading pattern. Several intermediaries across TCSC2 and TCSC3 member jurisdictions reported setting trading limits or filters, *e.g.*, on the size of the orders placed on the markets, their credit and total margin exposure, maximum order and total value of an order. These limits restrict further order flow when breached. One intermediary reported that it expects Customers to adhere to the trading limits set for them and to have early warning triggers in the Customer's own risk systems to prevent possible breaches of these limits.

A number of intermediaries stated that if a Customer reaches a trading position that is close to the total limit set for the Customer, they have the ability to reduce the frequency and/or size of subsequent orders, in order to prevent subsequent Customer orders from going over the pre-set limit. Such tools may be particularly relevant with respect to Customers using automated algorithms to place orders on a market. In addition, intermediaries generally have the ability to press a "stop" or "panic" button, in order to prevent a Customer from placing any further orders on the market.

Additional pre-trade execution controls appear to be coming into use. For example, some intermediaries reported that they now have the ability to see pending order flow placed by their Customers, but not yet executed on the market. Still other intermediaries are trying to develop the ability to delay orders in order to run a pre-execution filter, so that after a Customer places the order, the intermediary's automated systems will have a period up to one second in which to reject the trade. However, one UK respondent noted that it would not be possible to impose "systematic limits" on Customers on pre-executed orders if those transactions did not flow through the intermediary's infrastructure. The intermediary further stated that it would have to ensure that controls existed on the Customer's front end (rather than the intermediary's), and that such controls would be difficult to manage and would necessitate additional legal obligations.

Pre-execution trading filters are more common in AOR. In such cases, the intermediary has the ability to see the order flow and interact, *i.e.*, it can stop an order before execution. However, in SA, the use of such filters appears to be less prevalent and, in some cases it was argued that it may not be possible to implement, depending on the policies of a particular market or clearinghouse.

A common theme through the responses was that Customers would not accept any filter that imposed a delay in order execution.[16] One North American intermediary stated that a filter that relied on a calculation algorithm would take too long in a trading environment, and as a result, was rejected by its Customers.

Some European intermediaries highlighted policies of dealing only with regulated firms subject to prudential ratios and risk management controls whilst also employing a monitoring tool to calculate the Customer's order position on the market and utilizing filters to monitor size limits imposed by the intermediary on Customer orders. In this regard, one European intermediary highlighted the reliance on automatic filters enforced through the firm's systems. However, their more sophisticated Customers are expected to implement credit and risk management controls for their trading activities.

All surveyed intermediaries confirmed that they monitor trades on a post-trade basis. One European firm reported applying an in-house developed risk management model over the aggregated position in addition to applying various limits such as credit, stress risk, concentration risk and long option premium limits. There was however, a varied approach in terms of applying post execution controls. A US intermediary stated that post-execution controls were not enforced through filters as the intermediary managed regulatory exposure through a series of surveillance reviews and exception reports.

(4) Competitive pressures and a potential "race to the bottom"

Of the issues highlighted above, one of the most paramount is the availability of system filters, particularly whether intermediaries should be expected to use such controls and the scope of

[16] Some intermediaries indicated that the filters had not slowed order execution. Another intermediary acknowledged that filters could slow the order process, and indicated that it was working on enhancements to its filtering tools so that it would not add to the "latency" period in order execution. Another intermediary indicated that where filters are implemented "appropriately," there is only a minimal latency period.

monitoring by such filters. This would include pre-trade filters that guard against mistaken order entries (fat finger) and those designed to prevent or curtail Customer orders that exceed pre-set limits on a Customer's positions or a Customer's credit. The importance of this issue is illustrated by reported requests from so-called "high speed algorithmic traders," who seek to reduce latency by resisting the activation of DEA pre-trade system controls.

Information received during the course of TCSC2's and TCSC3's inquiries revealed that pressure for quick order fills by high velocity, algorithmic traders who perceive that a meaningful advantage exists with respect to millisecond latency reductions in trade execution have increased demands for trading without pre-execution filters. As a result, some intermediaries have reported that they are under competitive pressure to accept DEA orders that have not been subject to pre-trade filters.

Some US exchanges also have reported similar pressure from high speed non-intermediary members to disconnect pre-trade filtering functions from the market's trade execution system in order to reduce latency, thereby depriving the responsible clearing firm of pre-trade controls.
In this regard, it is important to note that some markets make available to intermediaries or clearing members' pre-trade filters.[17] Such filters can either be set to trigger a warning to the responsible intermediary or clearing firm that a trade has exceeded agreed upon limits or could be set as a "hard limit" to reject an order.

Potential disconnection of a DEA system filter at the request of a Customer could have significant risk management and other compliance and regulatory implications. Specifically, acceding to demands by Customers to turn off system filters to reduce latency could result in a "race to the bottom" in risk management practices, as high speed Customers cluster to intermediaries that accept orders without pre-trade filters. Indeed, acceptance of this practice would provide an incentive for intermediaries to eliminate what can be a valuable risk management and market integrity protection tool in order to accede to the demands of Customers or non-clearing members seeking a latency advantage, albeit in milliseconds.

On the other hand, some C&S and intermediary representatives argue that risk management should not be viewed in terms of a "one-size-fits-all" series of mechanical actions and that responsible risk management approaches can appropriately rely more heavily on robust "know your Customer" inquiries and "post-trade" controls rather\ than on pre-trade filters. Some intermediaries and market representatives have noted that a mechanistic rejection of an order that exceeds a "hard" trading limit without knowledge of the Customer's entire trading strategy and positions in other instruments could inadvertently convert a winning trade into a losing position. In addition, these intermediaries note that their institutional Customers frequently place orders in order to *reduce* their overall risk profile. For example, a Customer may place a trade in order to offset its existing exposures. Accordingly, some intermediaries believe they should provide a

---

[17] In November 2007, Eurex introduced Release 10.0 pre trade limits, which allows clearing members to control and track their DEA non-clearing members. Clearing members can monitor order frequency, order sizes and position limits for their non-clearing-members. Under this release, clearing members were also given a "stop button," which disconnects the Non-Clearing Member in question from the Eurex derivatives marketplace so that the Member in question's current open position is frozen and no additional orders can be entered. See http://www.eurexclearing.com/risk/pre_trade_en.html. See also *supra* note 12.

sufficient amount of latitude to Customers in order to avoid a situation where they inadvertently restrict their Customer's ability to enter into risk mitigating trades.

In effect, those arguing for a flexible risk management approach believe that responsible risk management decisions cannot be reduced to a formula, but must be the result of an active, case-by-case decision-making process that takes into consideration the distinct characteristics and sophistication of the Customer. Under this approach, it is argued that an intermediary might rely more heavily on credit determinations and the sophistication and background of the Customer, along with past experience with the Customer, rather than on pre-trade controls that set hard limits on order quantities, and that therefore pre-trade controls might vary. For example, a pre-trade filter may be used to trigger a warning rather than impose a cap on orders.

Nonetheless, it should be recognized that technological advances have minimized the latency effects of pre-trade filters, a key risk management tool. Accordingly, this raises the issue of whether markets that offer DEA should make certain pre-trade filters and post-trade functions available as a matter of best practice in order to facilitate better risk management at the firm level.

In any case, this issue is of paramount importance to regulators and need to be thoroughly considered to address concerns arising from current market developments.

(5) Concerns about Adequacy of Information from the Market and/or Clearinghouse

(i) Pre-trade order data

Pre-trade data regarding trades placed by a Customer vary according to the type of access granted by the intermediary to this Customer. Interestingly, there was some divergence of views on the necessity of such pre-trade information, with a majority of intermediaries asserting that pre-trade order data is critical for risk management purposes, and that the inability to obtain pre-trade information was a factor in their determination not to offer SA. Some intermediaries, by contrast, including some in both Asia and North America, believe that monitoring of Customers on an immediate post-trade basis is sufficient. Other intermediaries highlighted their ability to monitor information on a real-time basis.

For most of the respondents who permit access only through AOR, the type of data obtained by the intermediary is no different than the information they obtain where the intermediary executes the order directly – this includes general information on buy/sell type, order status, product, price, quantity, Customer ID.

However, the responses highlight that intermediaries that permit Customers to use SA in order to execute transactions do not always receive information concerning pending orders on a pre-execution basis. As an example, one North American intermediary stated that "to the extent that Customer transactions [are] on a sponsored access basis, the Customer's orders are not visible to it before execution, other than through supervisory terminals made available by connectivity providers/service bureaus." An Asian intermediary stated that "no pre-trade order data is

received [with] respect [to]…orders placed directly by direct access Customers who use their own infrastructure."

Some intermediaries emphasized their ability to obtain information on a real-time basis, sometimes referred to as "drop-copy." In general, this refers to the intermediary receiving a "copy" of its SA Customer's order as it is placed for execution. In theory, the order is not yet executed, but in practice there is generally no way to stop the order once the "drop copy" has been received. Based on presentations made to TCSC2 and TCSC3, however, there remains some ambiguity as to whether new technology would enable an intermediary who receives a drop copy to actually stop the order prior to execution.

At least one regulator has taken the position that pre-trade controls that are imposed by intermediaries on AOR should also be imposed on SA, as the regulatory obligations of an intermediary (as well as applicable market requirements), applies without regard to whether the business they handle on behalf of Customers is executed by AOR or on an SA basis. [18] It bases its position on the view that intermediaries have obligations to meet regulatory requirements in relation to the management of the credit risk they assume as a result of allowing Customers to send orders to a market, and that the management of such credit risk is an important aspect of the management of an intermediary's business.

(ii) Post-trade data

Issues relating to post-trade data appear to be less acute than with respect to pre-trade information. Intermediaries generally reported that they are able to obtain information on a post-trade basis for their DEA Customers that is identical to, or substantially the same, as for Customers trading on a non-DEA basis, i.e. full trading details (type, instrument, price, quantity, time, etc.).[19] With very few exceptions, data is received immediately following the trade (once every 5 minutes at the latest, depending on the exchange). Speed of data appears to depend on the mode of access and electronic line/connectivity used by Customers.

Intermediaries were asked to suggest possible enhancements to pre- and post-trade controls by markets permitting direct access. Some of the suggestions include the following:

- *Standardization* – Several firms in various jurisdictions requested that a standardized format be utilized by the various exchanges when reporting Customer transactions;
- *Transparency for clearing firms* – One European firm highlighted the need for exchange clearing members to have full and transparent access to information on their clearing Customers;
- *Enhanced order flow information* -A North American intermediary stated that maximum order quantity, position limits and span margining at the exchange level would be most beneficial; and

[18] *See, for example, http://www.fsa.gov.uk/pubs/newsletters/mw_newsletter30.pdf.*

- *Timeliness* - For a North American intermediary, requiring near real time transmission of all trades to the clearing firms would assist risk management.

D. Capacity/Algorithmic Trading

The overwhelming majority of markets responding to the TCSC2 survey question on capacity issues indicated that they had no concerns about capacity; however, a smaller number expressed capacity and system response concerns related to algorithmic trading. While algorithmic trading has the potential to enhance the quality of the market through increased trading interest and resulting price discovery, it also can potentially overwhelm system capacity and force delays in order display and execution through the queuing of messages.

One market articulated the issue in terms of degradation of the trading system (including both the trading engine and the networks used to transmit information between members and the trading engine) and the potential to create disorderly markets. In order to avoid that result (and avoid the potential for rationing of system bandwidth), the market responded on two fronts: technological system enhancements and the adoption of policies that attempt to moderate excessive messaging by algorithmic traders. Specifically, the market requires the registration of algorithmic traders, who must observe daily message allocation limits on a product by product basis. Messaging in excess of the allocation is subject to specific charges. The market also specifically monitors message traffic to determine whether such messaging may be having an adverse impact on the quality of the market and takes corrective action if necessary.

E. Latency and "Fairness"

Markets offer a variety of means for its member to connect to the trade matching system. Different connectivity pathways carry with them differences in response time due to differences in the type of connection technology (*i.e.,* the elapsed time between the transmission of a transaction from the intermediary's system and the receipt of that transmission by the market server for execution, also referred to as "latency").

For example, many market's order entry systems have an open architecture that facilitates a variety of connection methods and trading applications that may be designed and offered by the market itself, by intermediaries or by a service bureau. The technical *design* of the connection (*e.g.*, bandwidth, means of communicating with the exchange server) may result in varying degrees of latency. For example, direct communication lines, often facilitated globally by telecommunication hubs, may offer faster and more secure communication than trades sent via the internet.

Some differences in latency may be the inevitable result of geographic location of the DEA user. In order to overcome geography-related latency, some markets offer high speed, algorithmic traders a "co-location" arrangement, which allows the high speed trader to place their DEA servers as close as possible to the server of the market. Although the advantage is measured in milliseconds, the existence of and demand for such co-location arrangements reveal that co-location is perceived to be a measurable advantage.

Other differences in latency may result when, as noted previously, market systems contain "filters" that allow intermediaries the ability to control or monitor trades. Although the delay in question may be measured in milliseconds, some intermediaries have reported that high speed trading Customers have been requesting that their trades not be subjected to automated filters in order to reduce latency.

It is helpful for markets to offer market-members a variety of connectivity options notwithstanding inherent differences in response time. Such diversity of connectivity options allows market-members to match their services to the needs of varying types of Customers. In this regard, the TC recognized in its Screen-Based Principles Report that:

> *"where system user terminals are dispersed over a large geographic area, it may not be possible or prove cost prohibitive to ensure equal response times. This difficulty may be exacerbated where parts of the same network are supplied and maintained by different communications carriers in various jurisdictions."*[20]

As to issues of "fairness" that may be perceived with regard to any differences in response time within a given connectivity option, the TC concluded in its Screen-Based Principles Report that *equality of treatment within a given connectivity option was most important* and that *differences in response time should be addressed by disclosure.* Specifically, the TC concluded that:

> *"the need to ensure that response times are equitable for all like classes of participants (e.g., market makers) is more important, from a regulatory perspective, than the actual time. Under usual circumstances, equal response time is a matter which can be monitored by the system sponsor. To the extent possible, the host computer, system user installation, the communication network, and the software should provide for equitable response times for all classes of system users. Market participants (including system users and, when relevant, their Customers) should be informed where equal treatment is not possible, and the extent of any lags . . . . In all cases however, the actual response times should be disclosed. Variations in response time should be identified and explained. The potential for random variations should be disclosed if they cannot be eliminated."*[21]

---

[20] *See* Principle 4 of the Screen Based Principles Report, supra note 4, *p. 22.*

[21] *See* Principle 4 of the Screen Based Principles Report, supra note 4, *p. 22.*

VI. PROPOSED GUIDANCE AND CONSULTATIVE QUESTIONS

A. Introduction

Markets and intermediaries that are market members should have appropriate policies and procedures in place that seek to ensure that Customers granted DEA will not pose undue risks to the market and the relevant intermediary. The increasing use of DEA has created, however, substantial challenges. For example, there is the potential, particularly if proper controls are not implemented, that a Customer may intentionally or unintentionally cause a market disruption or engage in improper trading strategies that may involve some elements of fraud (including manipulation), and/or that may expose the intermediary to excessive credit risk. Unauthorised access is also generally recognised as being a major concern in terms of market integrity and security.

TCSC2 and TCSC3 have identified three key elements to be considered in the promulgation of guidance by IOSCO in the DEA area:

(i) *Pre-conditions for DEA*
(ii) *Information Flow*
(iii) *Adequate systems and controls*

For each of these elements, TCSC2 and TCSC3 have identified possible principles that would provide guidance in the DEA area. The Technical Committee invites comments from industry and the general public on these possible principles or on any other aspect of this Report.

Please indicate in your comments whether they apply to AOR, SA, Direct Access by Non-Intermediary Market-Members, or to all three DEA pathways.

B. Pre-conditions for DEA:

(1) Minimum Customer Standards

POSSIBLE PRINCIPLE: DEA Customers should be required to meet minimum standards, including:

- **appropriate financial resources;**
- **familiarity with the rules of the market and ability to comply with the rules of the market;**
- **knowledge of the order entry system which the Customer is permitted to utilize; and**
- **proficiency in the use of that system.**

- Are these the appropriate qualifications for DEA Customers, or should others be added? Please elaborate.

(2) Legally Binding Agreement:

POSSIBLE PRINCIPLE: There should be a recorded, legally binding contract between the intermediary and the DEA Customer, the nature and detail of which should be appropriate to the nature of the service provided.

- Do you agree? If not, please explain or elaborate.
- What are the key points to be addressed in such a contract? *See* section V.B (2) for possible elements that could be included. Should SA DEA Customers be required to enter into a contractual relationship with the market as well?

(3) Sub-delegation:

POSSIBLE PRINCIPLE: Where a DEA Customer is permitted to sub-delegate its direct access privileges directly to another party (sub-delegatee), the responsible intermediary should seek to ensure that its contractual arrangements with its DEA Customer allow it to identify the sub-delegatee if required by a market authority.

- What requirements should be applicable if a DEA Customer is permitted to delegate its access privileges directly to another party (sub-delegation)? For example, should the sub-delegatee be required to enter into a contractual relationship with the intermediary, the DEA Customer and/or the market? If yes, what areas should be covered by such a contract?

C. Information Flow

(1) Customer Identification

POSSIBLE PRINCIPLE: Intermediaries should disclose to market authorities upon request and in a timely manner the identity of their DEA Customers in order to facilitate market surveillance.

- What problems, if any, do intermediaries have in obtaining or delivering the identity of their DEA Customers? If problems exist, how could information flow be improved? (*e.g.,* the use of sub-user identifiers for sponsored access or sub-delegated DEA orders? Are there other possible solutions?) Please explain.
- Should DEA Customers each be assigned their own Customer ID or mnemonic? Please explain.

(2) Pre and Post-Trade Information

POSSIBLE PRINCIPLE: Markets should provide member firms with access to all pre- and post-trade information (on a real-time basis) to enable these firms to implement appropriate monitoring and risk management controls.

- Do you agree with this proposed principle? If not, please explain.

- What information do intermediaries need to receive on a pre- and post-trade basis in order to perform effective risk management? What information should a market provide the intermediary regarding pending order flow and other data in order for such a firm to implement properly pre-trade controls?

D. Adequate Systems and Controls

(1) Markets

POSSIBLE PRINCIPLE: Markets wishing to permit AOR and SA should have rules in place that seek to ensure that intermediaries providing DEA access to their Customers have adequate pre-trade controls to manage adequately the risk to fair and orderly trading.

- Do you agree? If not, please explain.

(2) Intermediaries

POSSIBLE PRINCIPLE: Intermediaries (including clearing firms) should have in place both regulatory and financial controls, including automated pre-trade filters, which can limit or prevent a Customer from placing an order that exceeds existing position or credit limits on such a Customer.

POSSIBLE PRINCIPLE: Intermediaries (including clearing firms) should have adequate operational and technical systems to manage their DEA systems.

- Do you agree that such automated pre-trade filters are desirable and feasible? If not, please elaborate? Please clarify precisely which types of pre-trade filters you deem appropriate. For example, pre-trade filters might range from "fat finger" stop buttons, to more sophisticated filters applying Customer position and/or credit limits.

- Do you believe any distinction needs to be drawn between pre-trade filters for position limits and credit limits; that is, filters that stop or limit trades that exceed such position limits and/or credit exposure, taking into account latency and other factors, as well as the inherent relationship between a Customer's position limit and credit limits that might be imposed on such a Customer?

- As an alternative to pre-trade filters, some intermediaries and markets believe that post trade controls, performed on a real time basis, can be an effective tool to manage risk involved in DEA transactions. What are the relative merits and drawbacks to such post-trade controls in comparison to pre-trade controls, from both a risk management perspective and the point of view of market participants interested in the fastest possible execution?

- Should pre-trade controls be at the intermediary or market level or both? Please elaborate. What level of responsibility for risk management of DEA, if any, should be assumed by the market?

- Should DEA systems and control procedures (including pre-trade filters and post trade controls), be similar or equivalent to those applied at present to non-DEA business? Please elaborate.

- Do markets or the CCP currently provide intermediaries with the functions/systems needed to conduct effective risk management relating to SA?

- When a non-clearing market-member places a trade, does the mere fact that the Customer is a market-member reduce the credit risk to the clearing firm that accepts the trades?

- Can intermediaries who receive "drop copies" of their SA Customer's orders stop the orders prior to execution? If not, what is the utility of such a tool?

- Do differences in latency raise any concerns that should be addressed by means other than disclosure and equitable access? If so, please explain the problem

- Please describe the minimum operational and technical systems that intermediaries should have in order to manage effectively the DEA that they permit.

Appendix I

TCSC2 used the following definitions:

"Direct Electronic Access (DEA)" - DEA refers to the process by which a person transmits orders on their own (i.e., without any handling or re-entry by another person) directly into the market's trade matching system for execution.

"Participant" – a person that is granted access to the market to transmit orders using DEA, whether or not a licensed or registered intermediary.

"Person" - Use of the word "person" is used for convenience and includes individuals, as well as entities such as corporations, limited partnerships etc.

"Sponsored Access" – An electronic access arrangement under which an intermediary Participant permits a Customer to transmit orders through its own system and gateway directly to the trading system or, less commonly, to send orders electronically to the trading system through a service bureau pursuant to an arrangement between the vendor and the intermediary Participant(s).

"Sponsored Access Person" - A Person who contracts with one or more Participants for Sponsored Access to the market.

"Market" - refers to exchanges and alternative trading facilities.

TCSC3 used the following definitions:

"Access through intermediary or third party infrastructure" - An electronic access arrangement under which a Customer of an intermediary (such as a broker or broker-dealer) is able to transmit orders to one or more markets' order matching system for execution through the intermediary's own infrastructure and gateway directly, or to send orders to the market through a service bureau's IT infrastructure, pursuant to an arrangement between the vendor and the intermediary.

"Access without utilization of intermediary infrastructure" - This refers to the process by which a Customer (such as a fund manager) of an intermediary (such as a broker or broker-dealer), transmits orders on their own (*i.e.*, without any handling or re-entry by the intermediary), directly into one or more markets' order matching system for execution. While the Customer may be using the intermediary's "tag" number, or name, the order does not go through the intermediary's infrastructure (including the intermediary's order routing IT systems). Such direct access, without utilization of the intermediary's infrastructure, could be referred to as "back-door" access to the market.

"Customer" – a person that is granted access to the market to transmit orders using *either* access through an intermediary's infrastructure, or access without utilization of the

intermediary's infrastructure, whether or not that person is a licensed or registered intermediary.

"Person" - Use of the word "person" is used for convenience and includes individuals, as well as entities such as corporations, limited partnerships etc.

"Market" - refers to registered or licensed exchanges.