The Futures and Options Association
Guidance on Managing the Risks of Direct Market Access

FOA

Contents

Clause	Name	Page
1	Introduction	1
2	What is DMA?	1
3	The Risks associated with DMA	1
4	Credit risk	2
5	Regulatory Risk	4
6	Operational risk	9
7	Future Guidance	10

FOA

GUIDANCE ON DIRECT MARKET ACCESS

1 INTRODUCTION

The provision by firms of direct market access ("**DMA**") to their clients is increasingly common. This fact, together with the fact that providing DMA creates a number of specific risks, has led to increased regulatory scrutiny of DMA. As a consequence, it is very important that firms which provide DMA properly assess and manage the risks that DMA gives rise to. This guidance is designed to help FOA member firms develop and implement appropriate risk management systems.

Clearly, the degree and type of risk that firms face as a consequence of providing DMA will differ from firm to firm depending on the precise nature of the DMA service provided, the nature of the clients to whom such service is provided and the volume of business undertaken by way of DMA. Firms should carry out an assessment of the risks they face as a result of providing DMA and tailor their controls according to the degree of risk faced.

As different firms will face different levels of risk, this guidance is not intended to be prescriptive. Firms should feel free to select from the risk management strategies referred to in this guidance and adapt them as appropriate to the needs of their business.

Although this guidance is primarily aimed at FOA member firms providing DMA access to third party clients, it is also relevant to any "internal" DMA users (e.g. proprietary traders or other group companies) which a firm may have.

2 WHAT IS DMA?

DMA generally refers to two categories of access via intermediaries namely:

(a) **Direct access via an intermediary firm** whereby clients submit orders electronically to an intermediary firm, a market member, which are then routed through the internal systems of the intermediary and automatically transmitted for execution to a market under the intermediary's market member ID. In this case, the intermediary retains the ability to monitor internally and, if necessary, stop an order prior to it being executed.

(b) **Sponsored access** whereby an intermediary, who is a market member, may permit its clients to use its market member ID to send orders directly to the market without passing through the systems of the intermediary firm. In this case the intermediary is not able to view the order in real time and cannot intervene to stop it.

In the case of either direct access via an intermediary firm or sponsored access, the order is sent to the market as the intermediary's order and the intermediary retains full responsibility for the order.

3 THE RISKS ASSOCIATED WITH DMA

The risks to intermediaries offering DMA to clients fall into three broad categories:

(a) Credit risk;

(b) Regulatory risk;

(c) Operational risk.

The following sections analyse each of those risks in detail and suggest measures which firms can take to manage those risks. As noted above, different firms will face different risks and the risk management suggestions are not therefore intended to be prescriptive. Rather, firms should feel free to select from the suggested measures and adapt them as appropriate to the needs of their business.

When assessing the risks to which they are subject, firms with overseas offices or branches should ensure that they take into account whether their overseas offices or branches grant DMA access to their clients and, if so, ensure that they have procedures in place to track and control the granting of such access, as well as meeting any additional local requirements in the overseas jurisdiction.

4 CREDIT RISK

Credit risk in the context of DMA trading activity refers to the risk of a firm incurring a loss as a result of the trades of a DMA client.

DMA provides some specific challenges relating to the management of credit risk. Where there is direct access via an intermediary firm, the firm has the opportunity to implement its risk management requirements such as pre-trade controls relating to position limits and "fat finger" error trades.

In sponsored access situations, the ability of the firm to conduct any risk assessment on submitted orders on a pre-trade basis, is limited in the absence of software risk management functionalities engineered into the execution path to the relevant market. This increases the probability of a mistake occurring or of a DMA client exceeding position or credit limits.

Regardless of whether direct access or sponsored access is provided, given the speed with which electronic execution takes place, firms will need to ensure that their post-trade risk management controls are adequate to deal with the limited time frame for the detection of, and response to, position limit breaches or error trades.

In order to ensure that credit risk is being properly managed, firms should consider three areas each of which is examined below, namely:

- analysis of potential DMA clients;
- pre-trade controls; and
- post-trade controls.

4.1 Analysis of potential DMA clients

Given the challenges of implementing comprehensive pre- and post-trade controls in the context of DMA trading activity, it is very important for firms to have a thorough understanding of a DMA client's overall risk profile. For example, a firm may impose different pre- and post-trade controls on a client which is a large global firm trading across different markets as compared to a smaller firm trading on just one market.

As part of the assessment of a client's credit risk profile, firms should consider analysing the following areas:

(a) The extent to which a potential DMA client has appropriate risk management tools in place to analyse its positions and risk profile;

(b) The potential DMA client's proposed trading strategy and anticipated trading volumes;

(c) The potential DMA client's credit rating (if available) and net worth.

(d) The DMA client's capitalisation and levels of collateral deposited with the clearing firm.

4.2 Pre-trade controls

In assessing the risks they face as a consequence of DMA and therefore the requirement for and nature of any pre-trade controls, firms should, among other things, consider levels of collateral received from clients, the client's own risk management capabilities and the extent to which the client is permitted to control any pre-trade controls that have been put in place.

Pre-trade controls may be implemented at the trader, client, intermediary firm or trading venue level.

Where a firm wishes to impose pre-trade controls, it may use some or all of the following:

(a) Protection against error trades (i.e. so called "fat finger" protection) configurable by product;

(b) Filters providing for a maximum order size and value[1];

(c) Filters on a client's credit and/or total margin exposure;

(d) Functionality that facilitates the timely withdrawal of erroneous orders;

(e) Restrictions on further order flow when position limits or credit and margin limits are breached or close to being breached;

(f) Early warning triggers in the client's own risk systems aimed at preventing breaches of limits;

(g) Controls which allow a firm to see a client's unexecuted, pending order flow.

(h) Configurable product access controls which allow the firm to configure its system so as to restrict a client's DMA trading activity to specific products.

(i) "Message throttling controls" aimed at allowing a firm to impose limits on a client's message processing rates so that the firm is able to comply with any message throttling controls to which it is subject under the rules of a relevant market/trading venue.

---

[1] Given that there may be occasions when a larger order is justified, firms may also offer clients the opportunity to request an adjustment to such limits. In addition, limits may need to be adjusted dynamically according to the amount of liquidity in the market.

4.3 Post-trade controls

Firms should ensure that their post-trade controls adequately address the credit risk arising from trades executed by DMA clients, by active monitoring of executed DMA client trades on an aggregated basis and the imposition of various limits such as credit, stress risk, concentration risk and position limits.

Some markets/trading venues may provide its members with so-called "drop copy" functionality which provides them with duplicate copies of clients' unexecuted orders and/or executed trades via separate near real time data feeds. This facilitates the tracking of all executed and unexecuted orders as well as any order amendments or cancellations. Such feeds, if available, will assist firms in monitoring client positions on a real time basis and/or in being able to identify rejected trades.

5 REGULATORY RISK

Regulatory risk in the context of DMA refers to the risk of an intermediary failing to comply with market rules and other relevant law and regulation applicable to orders sent to the market in the intermediary's name and executed on behalf of its DMA clients.

5.1 Clients' compliance with market rules and other applicable law and regulation

Markets do not generally have the authority to take enforcement action against non-members. It follows that a market member firm which grants DMA to a non-member client could be held liable for a breach of market rules as a result of the actions of its DMA client. However in determining such liability, the trading venue may take into account the extent to which the member firm has provided its client with educational materials on the applicable rules. In addition, firms providing DMA could be accountable to the FSA (and other relevant regulators) in circumstances where a client who executes trades through DMA commits breaches of applicable law and regulation. For example, in circumstances where a DMA client commits market abuse, such as insider dealing or market manipulation, the firm could be held liable for assisting the market abuse or for failing to have appropriate systems and controls to prevent that abuse occurring.

In light of the risk of firms facing regulatory action as a consequence of breaches of market rules or other applicable law and regulation, firms should consider adopting the following measures:

(a) **Assessing each DMA client's knowledge and experience.**

Prior to granting DMA to a client, firms should assess the client with respect to the following factors:

- familiarity with market rules and other applicable law and regulation including those relating to market abuse;
- prior sanctions for breaches of applicable law and regulation; and
- proposed trading strategy and associated volumes.

(b) **Providing regulatory education**

Firms should consider taking steps aimed at ensuring that clients are familiar with relevant market rules and other applicable law and regulation (eg market abuse laws). Such steps could include providing relevant regulatory education to clients prior to granting DMA. This could take the form of a written summary which could include links to the relevant Exchange Rules.

(c) **Pre-trade controls**

Firms should consider putting in place pre-trade controls, such as filters to prevent activity that would breach market rules or applicable law or regulation (see paragraph 4.2 above).

(d) **Monitoring**

Trading venues have primary responsibility to monitor trading activity on that venue for compliance with its market rules and applicable law and regulation. Additionally, firms should monitor, on a post-trade basis, the trading activity of DMA clients for compliance with market rules and other applicable law and regulation. Firms should adopt a risk based approach to monitoring so that the degree of monitoring undertaken is proportionate to the firm's assessment of the risk of a particular DMA client breaching market rules or other applicable law and regulation. In assessing such risk, a firm should have regard to the factors referred to in paragraph 5.1(a) above.

(e) **Contractual protections**

Given that a client will trade in the name of a firm in its capacity as an exchange member, firms should consider entering into written contracts with DMA clients which seek to document the client's requirement to comply with market rules and other applicable law and regulation and which permit the firm to impose appropriate controls on the client's DMA trading activity. Firms should consider including the following terms and conditions in their contractual agreements with DMA clients:

- Terms which address the parties' respective rights and liabilities relating to DMA use and, in particular, which make it clear that the client accepts all liability arising from its DMA trading activity and will indemnify the firm against losses arising from the client's DMA use.

- A requirement to have knowledge of and comply with applicable market rules and other applicable law and regulation.

- A requirement that employees of the client who execute trades on a DMA basis are appropriately qualified, competent and authorised to trade by the client.

- Terms relating to the security of both the client's and the firm's systems used for the purposes of DMA (for example, terms requiring the use of user IDs, passwords and authentication codes) which aim, among other things, to prevent unauthorised system access.

- Terms which give the firm the right to impose limits on the size and volume of the position which a client can execute through DMA.

- Terms which impose conditions on the way in which orders can be entered and limit the client's right to cancel transactions after execution.

- Terms which give the firm the right to cancel orders, reject orders and suspend DMA access at its own and sole discretion.

- Terms confirming that the client is only allowed to access markets from jurisdictions specifically agreed with the firm so as to avoid the firm breaching laws and regulations in certain jurisdictions.

- Terms confirming that the client has all appropriate licences, approvals and regulatory consents that it may require in order to undertake DMA business.

- Terms which require the client to provide information to the firm in relation to any investigations that a market/trading venue may undertake in relation to trading undertaken by the firm's clients on a DMA basis.

- Terms which require the client to comply with any IT systems or testing requirements and other IT related requirements prescribed by the DMA system provider.

- Where relevant, terms which restrict the onward distribution of exchange data.

- Terms limiting liability for losses rising from DMA trading activity including any losses arising from the firm's use of functionality that facilitates the withdrawal of erroneous orders (see paragraph 4.2(d) above).

- Terms which impose a prohibition or restrictions on the use of DMA by Underlying Clients (see paragraph 5.1(f) below).

Whilst contractual protections are clearly important in helping to mitigate the risk to which firms are subject as a result of engaging in DMA activity, firms should be wary of relying solely on such protections. Among other things, the FSA may not regard such reliance as sufficient in terms of assessing the adequacy of a firm's system and controls.

(f) **Use of DMA by clients of a client**

In certain circumstances a client of a firm providing DMA may wish to make DMA available to its own clients ("**Underlying Clients**"). As the firm will not have any underlying contractual relationship with Underlying Clients relating to the use of DMA, it needs to manage the additional risk that this gives rise to. In broad terms this will involve taking either of the following steps:

- Prohibiting the use of DMA by Underlying Clients by including a contractual restriction to this effect; or

- Requiring a client who proposes to allow an Underlying Client to use DMA to notify the firm of this fact and to impose restrictions on an

Underlying Client equivalent to those to which the client is subject under the terms of its contract with the firm.

5.2 **Firms' compliance with market rules and other applicable law and regulation**

In addition to taking steps to ensure that DMA clients comply with applicable market rules and other applicable law and regulation, firms themselves are subject to regulatory requirements arising from the provision of DMA. The regulatory requirements likely to be of most relevance to FSA authorised intermediaries providing DMA are as follows:

(a) **Market rules**

Markets on which DMA transactions are executed may impose additional obligations on firms providing DMA, for example by requiring them to have appropriate systems and controls in place to monitor their clients' trading activity which takes place on a DMA basis and by requiring firms to retain trade data and related information.

(b) **FSA requirements relating to systems and controls**

Principle 3 of the FSA's Principles for Businesses provides that *a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.*

In addition SYSC 4.1.1R requires, among other things, a firm to have *effective processes to identify, manage, monitor and report the risks it is or might be exposed to and internal control mechanisms, including sound administrative and accounting procedures and effective control and safeguard arrangements for information processing systems*.

According to Market Watch 30, published by the FSA in November 2008, the Principle 3 and SYSC 4.1.1R requirements mean, among other things, that in the context of DMA activity, an intermediary should impose pre-trade controls on orders and implement post-trade measures to monitor trading activity regardless of whether the DMA takes place by means of direct access via an intermediary firm or sponsored access.

Given that firms offering sponsored access will not be able to exercise pre-trade controls directly, unlike in the case of direct access via an intermediary firm, the requirement to impose pre-trade controls and post-trade monitoring is more challenging and may, as the FSA itself recognises, involve parties other than the sponsoring intermediary in the operation of those controls and measures (for example, the market operator itself) and may include outsourcing. In Market Watch 30, the FSA reminds firms that, if a sponsoring intermediary firm outsources critical or important operational functions, it remains fully responsible for fulfilling its obligations under the regulatory system.

Firms must also ensure that their systems and controls relating to DMA are sufficient to allow them to comply with:

(i) SYSC 6.1.1R which requires firms *to establish, implement and maintain adequate policies and procedures sufficient to ensure*

compliance with the regulatory system and for countering the risk that the firm might be used to further financial crime; and

(ii) SYSC 7.2.1R which requires a common platform firm *to establish, implement and maintain adequate risk management policies and procedures, including effective procedures for risk assessment, which identify the risks relating to the firms' activities, processes and systems, and where appropriate, set the level of risk tolerated by the firm*.

(c) **Suspicious transaction reporting**

SUP 15.10.2R requires *a firm which arranges or executes a transaction with or for a client in a qualifying investment admitted to trading on a prescribed market and which has reasonable grounds to suspect that the transaction might constitute market abuse must notify the FSA without delay*.

In light of this, firms providing DMA must ensure that their system and controls are sufficient to allow them to detect indications of market abuse arising from trading activity undertaken by clients to whom they provide DMA and to evaluate the data with a view to deciding whether a suspicious activity report needs to be made to the FSA or, as appropriate, law enforcement agencies.

(d) **Transaction reporting**

SUP 17.1.4R requires *a firm to report to the FSA details of a transaction which it executes:*

(i) *in any financial instrument admitted to trading on a regulated market or a prescribed market (whether or not the transaction was carried out on such a market); or*

(ii) *in any OTC derivative the value of which is derived from, or which is otherwise dependent on, an equity or debt-related financial instrument which is admitted to trading on a regulated market or on a prescribed market.*

Firms providing DMA must ensure that their systems and controls allow them to comply with their transaction reporting obligations in respect of transactions executed in their name by means of DMA. In particular, firms offering sponsored access should be aware that it is not sufficient to submit a report detailing the market-side transaction and that they must also submit a client-side report identifying the client, which includes all the details required under SUP 17.

(e) **Overseas regulatory obligations**

Firms should be aware that granting DMA access to clients outside the UK may trigger legal and regulatory obligations in the jurisdiction in which a client is based. Accordingly, firms proposing to grant such access should ensure that they are permitted to do so under the laws of the relevant jurisdiction and, if so, whether this will subject the firm to regulatory obligations in that jurisdiction. If granting DMA access to overseas clients does give rise to regulatory obligations outside the UK, the firm will need

to fully understand the nature of those obligations and put in place procedures to comply with them.

6 OPERATIONAL RISK

Operational risk refers to the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. In the context of DMA, the major aspects of operational risk relate to the electronic trading infrastructure provided by the firm and the client's own infrastructure which forms the interface with the firm's trading infrastructure or, in the case of sponsored access, the market.

As noted in Section 5 above, firms providing DMA are subject to various FSA requirements relating to systems and controls and a failure to manage operational risk properly means that a firm could be in breach of these regulatory requirements in addition to incurring other potential losses such as having to compensate clients for losses arising from a system failure. Firms should therefore view the management of operational risk relating to DMA as a key priority.

Given the importance of IT in the context of DMA, firms should consider implementing controls relating to the use of IT. These controls should apply not just to the firm itself but to the client. In particular, firms should consider the following issues:

(a) **Compatibility**: Firms should ensure that the IT systems used by its clients are compatible with its own systems and that it meets any applicable IT hardware specifications and network configuration required by the market on which the orders will be executed.

(b) **Capacity Management:** Firms should ensure they understand their overall DMA system's capacity. They should monitor consumption of that capacity proactively to mitigate the operational risk (to the firm as well as the overall market) of a client, firm or trading venue system failure after reaching a capacity limit.

(c) **Restrictions on use of clients' IT:** Given that efficient performance can be inhibited by a DMA client's own activities (e.g. by a client running additional software alongside dedicated order routing software), firms should consider imposing restrictions and controls on the use by clients of their own IT to the extent that it interfaces with the firm's own systems or the systems of a market.

(d) **Security:** Firms may be liable to markets for any systems failure that results from the introduction of viruses or similar items, even where the virus or similar item results from an action of a DMA client. Accordingly, the firm should require their clients to ensure that they have adequate procedures in place to prevent the introduction of viruses. Firms should seek to reinforce this requirement through their contractual arrangements with DMA clients by making it clear that clients will be held liable for, and indemnify the firm in respect of, losses arising as a result of the introduction of a virus or similar item from the client's systems.

(e) **Authority:** In addition to the security features referred to above, firms should consider imposing requirements on DMA clients which restrict access to authorised personnel.

(f) **Errors:** Firms should make it clear that DMA clients will be liable for any losses arising as a result of an incorrectly or erroneously entered order.

(g) **Connectivity:** Firms should ensure that clients have the functionality to monitor loss of connectivity with a trading venue and, when connectivity is lost, the functionality to disable their trading system and cancel resting orders.

(h) **Compliance with IT related requirements:** Firms will need to ensure that they have the right to require their clients to comply with any IT requirements imposed by a market/trading venue e.g. message throttling limits or requirements relating to approved price injection models or algorithmic/black box trading systems. Where relevant, firms should also make clear in their contract with a DMA client whether a client has an obligation to determine when it must re-conform a model when the logic within that model has changed.

(i) **Key contacts:** Firms should ensure that they agree with their clients a key contact to whom queries relating to DMA trading activity can be directed, such as the employee responsible for overseeing the client's DMA trading activity.

7 FUTURE GUIDANCE

DMA is a growing and rapidly evolving way of doing business. Consequently, firms should monitor developments in this area and ensure that their risk management practices adequately address risks arising from those developments. This guidance will be kept under review to ensure that it takes adequate account of commercial, operational and regulatory developments that impact on the provision of DMA.