FIA

Order Handling Risk Management Recommendations for Executing Brokers

Building on recent FIA publications, including *Market Access Risk Management Recommendations* (April 2010) and *Recommendations for Risk Controls for Trading Firms* (November 2010), this document offers a number of recommendations for executing firms to consider both in designing policies for their own brokers that handle orders electronically and in dealing with customers that access the markets through a broker's trading platform.

Electronic orders are by nature low touch. This document is intended to outline best practices for orders that are routed through a trading platform that the broker fully administers including 1) a FIX connection from a client's proprietary trading system, 2) a FIX connection from a third-party Order Management System ("OMS") or Execution Management System ("EMS") or 3) a single dealer platform that is either internally developed by the broker or provided to the broker by a third-party software vendor.

This document is not intended to cover broker-provided direct access to an exchange; for best practices for this type of order flow please refer to *FIA Market Access Risk Management Recommendations*.

The situation of inadvertent wash trades generated through electronic trading has been omitted from this document since FIA feels that this issue needs to be discussed separately.

Several items within this document—particularly recommendations regarding executing broker automated execution tools—are not currently common practice within the futures industry but are becoming increasing typical for equities trading, and may be considered equally applicable for all electronically traded asset classes.

The Role of the Executing Broker

We use the term "executing broker" to describe both brokers providing execution-only services to a client and giving up their trades to a separate clearing broker as well as full-service brokers providing both execution and clearing services to the client. This distinction is important because the roles and responsibilities of the two will differ, particularly with respect to credit risk management. While the execution-only broker will generally not be in a position to evaluate the creditworthiness of a client, the full-service broker is required to evaluate and manage its credit risk against the client. As a result, the execution-only broker will focus primarily on pragmatic "fat finger" and intraday position limits designed to prevent unintended trading, while the full-service broker also will set and manage credit limits.

It is also important to note that in some cases, a full-service broker will provide execution services to related clients through an omnibus relationship whereby the broker will set controls for the relationship as a whole rather than the individual underlying clients. These distinctions may affect how executing brokers- adopt these recommendations.

Executing Broker Pre-Trade Controls

FIA recommends that executing brokers use pre-trade controls to reduce the risk of 1) inadvertent entry of orders at the wrong price or quantity, 2) unintentional triggering of a client algorithm or 3) an improperly configured client algorithm.

It should be noted that executing brokers see only a portion of the client's activity and cannot fully measure the risk that a client may be exposed to, particularly where they do not have a clearing relationship with the client. Where possible, the executing broker should try to ascertain the appropriate risk levels for the activity that is directed through their trading platform, but it should be emphasized that pre-trade limits are set on a "best efforts" basis since comprehensive real-time credit checks across all of the client's trading activity (where they use multiple counterparties) are currently difficult to achieve.

Effective pre-trade controls may include the following:

- **Trader and Automated Trading System Identifiers.** Account and trader identifiers are required to be attached to the order when sent to the exchange. In addition, each automated trading strategy that sends orders to the exchange must have a unique identifier. These identifiers are required by exchanges and regulators to correctly trace the source of trades they wish to review.

- **Order Size or "Fat Finger" Limits.** As a prudent risk management measure, executing brokers should set maximum quantities per order for each client, and where possible each trader within the client firm if such granularity is available within the trading platform. The limits should be based on the broker's experience in the market including factors such as its liquidity and contract size, as well as an assessment of what is appropriate for the particular client based on their risk profile. Orders exceeding "fat finger" limits should be blocked entirely, unless allowed pursuant to a manual override used at the discretion of the executing broker. The executing broker should have a procedure in place for reviewing limits with the client and documenting requested changes.

- **Position or Margin Limits.** As an element of an effective broker risk management system, executing brokers should set maximum long or short position limits by product for each client, and/or where possible the individual trader, based on factors such as their risk profile, level of sophistication, and type of trading activity. Limits can be higher for an executing broker handling orders from multiple accounts for a client than from an individual trader at the client. Further, limits should be cumulative intraday and may or may not include start-of-day positions. It should be recognized that providing pre-trade position or margin checks can only be implemented on a "best efforts" basis for clients that may use multiple systems to trade through an executing broker and, as such, these limits are designed as "speed bumps" and not full credit controls. It is expected that these limits would be set when the client is onboarded and adjusted infrequently. The executing broker should have a procedure in place for reviewing limits with the client and documenting requested changes.

- **Cancel-on-Disconnect.** When an executing broker trading platform disconnects from the exchange for any reason, the client may lose control of their working orders and may be unable to obtain accurate information on the status of their orders. To the extent that an exchange offers a cancel-on-disconnect capability, we recommend that a broker who chooses to use this functionality should also have procedures in place to notify clients that orders have been cancelled and should be resubmitted.

- **Independent Order Cancellation Capability.** As a prudent risk management measure, exchanges should provide executing brokers with a tool--independent from the broker trading platform--that enables the firm to view and cancel working orders submitted through their membership on the exchange. Such a tool would permit the broker to view current order status, fill information (including partial fills), cancel/replace history, and order timestamps. This tool would also give the executing broker the ability to cancel individual or groups of working orders in the event of losing direct control of the orders placed through its trading platform.

- **Kill Switch.** Executing brokers should have access to a "Kill Switch" which enables the broker to disable the trading platform's ability to trade and cancels all resting orders. This kill switch capability can be enabled at the exchange level.

Executing Broker Automated Execution Tools

Executing brokers often provide clients with electronic execution tools, which offer the ability to work an order automatically. Such tools, often known as "execution algorithms," typically divide a defined "parent" order into a series of smaller "child" orders so as to achieve more efficient execution compared to entering the order directly into a market. Often the tools attempt to reduce the displayed size of a large order by targeting a benchmark (such as Volume Weighted Average Price ”VWAP" or Time Weighted Average Price "TWAP"), participating evenly in the market regardless of trend, or blending-in with other trades in the market so as to minimize impact. Parameters for such tools can include, but are not limited to, tactic, trigger, limit price, start time, end time, duration, patience, percentage of volume and display size.

Ultimately, automated execution tools are useful as they can help market participants transact more efficiently, regardless of whether the trade is initiated for hedging, taking profit or providing a contingency against adverse market moves.

Automated execution tools for futures are increasingly being offered by executing brokers using technology that has been developed within the firm. Such tools are the intellectual property of the broker.

With the wider adoption of automated execution tools within the futures industry, third-party software vendors are offering similar tools for market participants to use. The best practices recommended in this document are particularly aimed at broker-developed tools but are equally applicable to all providers of automated execution tools.

Where a third-party software vendor offers a tool or framework for developing a client's own execution algorithms or models, the broker should treat the tool in the same way that it would treat a client's own proprietary system and certify that the third-party software vendor follows all rules regarding conformance of messages. It is not practical for the broker to certify the algorithm or trading model since it is not their intellectual property. Risk management of such third-party tools should be handled based on the orders generated and prudent limits implemented by the executing broker.

The use of a broker-provided automated execution tool requires both client and broker to be cognizant of the performance of the tool and how it is expected to behave under different market conditions. Consistent with prudent risk management, we recommend that executing brokers establish general controls similar to those detailed in the previous section but with additional checks for the tool while it is working, as well as checks against the orders that the tool submits to the market. These may include:

1. *Controls before the Execution Tool*

   - **Order Size Limits.** Brokers should set limits on the number of contracts that can be entered into an automated execution tool at any time, based in part on the relative sophistication of the trader as well as the liquidity and/or volatility of the market to be traded. In some cases it may be appropriate that a broker provides larger order size limits for orders being worked by an execution tool compared to orders that are sent directly to market.

2. *Controls embedded within the Execution Tool*

- **Market Impact Checks.** The parameters provided on an order submitted via an execution tool dictate how the order will be worked in the market. Where practical, execution tools should be configured to provide an ongoing comparison between the size of an order, its level of patience in completing the execution of the order, and the average daily volume of the product being traded. In a prudent risk management environment, such a tool would reject orders that may be considered too big relative to the size of the market over the duration which the order will be worked. In such cases, the broker would contact the client to determine a more appropriate tool for their objective.

- **Dynamic Price Checks.** Automated execution tools should always be cognizant of current market prices. Since an order submitted via an execution tool may work over a longer duration than an order sent directly to market, it is appropriate to check slices generated by the algorithm against a pre-defined range around the last price on the market. The range should be defined by market volatility and current market conditions. This also helps to ensure that orders without a limit price constraint will not cause accidental disruption of the market. A limit price supplied on an order worked through an execution tool provides protection by preventing child orders from trading beyond the limit.

- **Dynamic Market Move Checks.** Where practical, we recommend that execution tools also compare current market prices against the bid/ask at the time of arrival, so that it is possible to flag any sizeable deviation in the market while the execution tool is working. Such a flag could prompt the broker to contact the client, either directly or via an automated alert to the client, so that the client and broker can evaluate whether the tool should continue executing under current market conditions or whether it should be paused, cancelled or resubmitted.

- **Market Halt Parameters.** Executing brokers should implement procedures to clarify how the execution algorithm will respond under certain market conditions, e.g., limit-up, limit-down or a similar circuit breaker. Note that such halts will affect the ability of an execution algorithm to meet its execution objective, often causing a recalculation of how the tool should perform in terms of "catching up" to any schedule it may be using. In the event of a market halt, to the extent possible, the broker and client should discuss what they expect to happen upon resumption of trading and whether the order should be paused, cancelled or resubmitted.

3. *Controls after the Execution Tool*

- **Last-Look Reasonability Checks.** We recommend that a broker have the ability to perform a final automated reasonability check on the individual slices of the execution tool--such as size and price relative to current market conditions--before the slice is released to the marketplace. This generic check would evaluate the slice on its own and not as part of the overall ticket being worked through the execution tool, and could prevent accidental market disruption due to any failure of checks within the tool itself. Such a check could be implemented as part of a risk management tool within the broker's exchange connectivity or through an exchange provided tool.

- Wherever possible exchange provided risk management tools should be used to minimize the possibility of inadvertent disruption to the market. Such controls include limit checks and kill switches. It should be emphasized that such a tool should provide an appropriate degree of granularity to allow for brokers that have multiple clients or trading platforms sharing a single exchange session.

Client Post-Trade Reconciliation

FIA supports the widespread industry practice of allowing clients to compare their internal trade records against the executing broker's own records. This practice identifies any trade(s) that may not have been correctly reported back to the client from the broker's trading platform.

Similarly, FIA recommends processes that allow clients to reconcile both orders and fills through their executing broker's trading platforms. For the purposes of this document we are limiting discussion to the reconciliation of trades done through an executing broker and not the reconciliation of trades cleared through a clearing broker, which is typically handled through a separate workflow.

Executing brokers may elect to provide clients with trade data via an alternate channel to ensure that client trades match those that are reported in the broker's trading platform. Information should be provided using media of the client's choice, for example email recaps, FTP files or FIX drop copies. FIA advises that the post-trade data feed contain all fills at a minimum but may also contain additional data (messaging, cancels, etc.) at the discretion of the executing broker or at the request of the client.

In addition, FIA urges brokers, exchanges and other trading platforms to work toward an industry standard for delivering cleared information within a standard deadline (e.g., two-to-three minutes after a trade is executed). We recommend that this data be delivered wherever possible via a standard protocol, preferably via FIX API. Such an approach could address some of the gaps highlighted earlier in this document regarding pre-trade risk management, and could allow clearing brokers to manage and report all activity that they clear on the client's behalf in a more efficient manner.

Validation of Client Access and Oversight of Client Activity

Electronic trading is designed to be low-touch, involving little human interaction at the executing broker. Particularly in situations where clients entering orders are not members of the exchange and not otherwise regulated, executing brokers should provide information to clients that access the brokers' trading platforms in the following areas:

- Guidance on relevant rules and regulations for trading on an exchange, including where possible a link to the exchange website.
- Alternative methods to contact the executing broker during any outage of their trading platform.

In addition, the executing broker should develop internal procedures for reviewing the workflow generated by a client's trading system before it is approved to connect to the broker's trading platforms (see "Client Conformance Testing"). Such procedures are intended to validate the messages used for electronic trading and not algorithms or trading models used by the client before messages are generated.

Executing brokers should develop procedures for reviewing electronic execution of orders, including:

- **Trading restrictions.** Executing brokers should establish a process to help clients determine what products and exchanges they are eligible to trade.
- **Review of internal administrative terminal access.** Executing brokers should take steps to determine that clients are unable to gain administrative access to the broker's trading platforms or override administrative controls set by the broker.
- **Ratios of orders to fills.** Executing brokers should provide guidance to clients on the appropriate ratio of unfilled orders and cancellation messages to actual filled orders. The purpose of this recommendation is to avoid occurrences of excessive (and unnecessary) messaging, which can disrupt the trading of other users of the platform or the exchange. Brokers should tie these guidelines to either published exchange policies or ratios derived by the brokers themselves based on their own experience with excessive messaging.

Executing brokers should also implement procedures to address inadvertent trading and errors that may result from such. In this context "inadvertent trading" is used to cover situations such as unauthorized access to a client's trading account or an accidental misconfiguration that may lead to trades incorrectly being executed into the client's account. As highlighted in the "Client Post-Trade Reconciliation" section, executing brokers should take steps to provide clients with information on filled orders in as close to real time as practical so that clients can detect inadvertent or unauthorized trading. Executing brokers should also make efforts to ensure that their clients understand the procedures for canceling and/or trading out of erroneous trades (see "Electronic Error Trade Process" on page 14).

Client Conformance Testing

In the event that a client seeks to have its systems write directly to the order entry or market data interfaces of a broker's trading platforms, the executing broker should require the client to satisfy a set of conformance tests to ensure that the client's systems interact correctly with the relevant platforms. Such conformance tests are also applicable for third-party OMS' and EMS' that interface with the broker's trading platform.

The most effective means of accomplishing this goal would be through a conformance or test environment that replicates the actual behavior of the trading platform that the client will access to trade in production. This could be accomplished by providing the client with access to an exchange test environment where available and/or a simulation environment for the broker's automated execution tools. Consistent with FIA's *Market Access Risk Management Recommendations*, FIA strongly recommends that exchanges provide a test environment that brokers, vendors and clients can use for certification of their message flow. This should be as close as possible to the current production environment and should be available throughout the business week.

It is important to note that conformance testing performed by the executing broker is solely to certify that the interaction between the client's system and the executing broker's trading platforms behaves as predicted. Executing brokers should not be expected to certify a client's algorithm or trading model to ensure that it could not be disruptive to the market place since: 1) the broker does not have access to the intellectual property behind the algorithm in order to assess how it may behave in different scenarios; and 2) it is not feasible for the broker to create the multiple simulation scenarios required for back-testing.

For these reasons, ensuring that a client written algorithm or trading model will not cause or contribute to market disruption should remain the exclusive responsibility of the client to test before it puts its algorithm into production.

FIA recommends that executing brokers test the ability of the client's trading system to:

- Send a request for and process the conformance environment's response to the following: Log On, Log Off, New Order, Cancel, Order Modify, Sequence Reset, Instrument Definition Requests, and Market Snapshot requests (where available or relevant to the type of connection).

- Process the following conformance environment's messages: Business Reject, Session Reject, Complete Fills, Partial Fills, Exchange Open/Close, Market Data Updates, and Trade Updates (where available or relevant to the type of connection).

- Properly handle messages sent to or from the client's trading platform during recovery following periods when the trading platform is not actively connected.

Additional conformance testing should be performed in certain situations, including:

- Whenever core functionality has changed on the executing broker trading platform. It should be up to the executing broker to decide what functionality needs to be recertified, as well as notifying each client with a proprietary system or third-party software vendor of the need to recertify.
- Whenever a client's proprietary system core functionality has changed. It is up to the client to notify the executing broker when this happens and to schedule the conformance test.
- Whenever a third-party OMS or EMS core functionality has changed. It is up to the vendor to notify the executing broker when this happens and to schedule the conformance test.

Additional Recommended Best Practices for Executing Brokers

1. *Electronic Trading Interruptions*

- In cases where clients access a broker's trading platform, we recommend that executing brokers establish monitoring tools to alert support staff when a trading connection is broken and/or orders are being rejected. Additionally, we encourage the use of procedures and tools to enable cancellation of working orders and reconciliation of executed orders. Under such a scenario, where possible, executing brokers should make available a back-up method to execute trades when trading is disrupted on a particular platform.

2. *Physical Security*

- In addition to any specific exchange or trading platform rules related to physical security, executing brokers should take steps reasonably designed to limit access to trading platforms under the broker's control to only those authorized to trade on a particular platform or for a particular account or user.

3. *Electronic Security*

- As with all electronic systems, FIA recommends that firms consider the security of their trading and business networks and be aware of the risk of access to their network infrastructure by unauthorized personnel. In particular, we recommend that firms with direct access to exchange matching engines be aware of the potential for intruders to use their network infrastructure to launch attacks against exchange networks or potentially engage in unauthorized trading, and firms should take steps to mitigate such risk.

- FIA strongly encourages the use of network firewalls, virtual private network ("VPN") connections or other security devices to prevent unauthorized remote access to business networks. Conversely, FIA strongly advises against any deliberate failure to employ firewalls or other security measures for the purpose of reducing latency or increasing throughput.

- As required by exchange and trading platform rules, users of VPN connections, computer systems and software should be authenticated through use of login IDs and passwords or other measures such as token-based authentication systems. Although an executing broker may have no control over the physical security of systems accessing markets and the use of passwords and logins by its clients, FIA recommends that all brokers' staff be trained on proper security and accountability for passwords and logins. Use of a login other than one's own should be forbidden for both the broker and the user, particularly with respect to electronic trading systems. Further, FIA recommends that firms develop policies requiring minimum levels of password complexity (e.g., use of upper and lowercase letters, numbers and special characters) and rules specifying periodic password expiration. We encourage the use of detailed logging systems to record user and system activity. We advise executing brokers to perform regular security audits of their systems (conducted by third parties where appropriate) to ensure continuing levels of security.

- Executing brokers should have policies and procedures to address staff departures, particularly relating to removal of physical and electronic access privileges and recovery of business assets. Such policies and procedures should include:
  - Withdrawal of electronic or voice trading privileges from electronic trading platforms.
  - Revocation of status as an authorized contact, responsible individual or other privileges with exchanges.
  - Recovery of other firm-owned computing equipment (e.g., laptops, desktops, wireless broadband cards).
  - Revocation of login privileges on firm computing systems, VPNs, and other points of access (especially important for IT and support staff with access to many trading platform components).
  - Forwarding user's e-mail to appropriate staff and removal of e-mail account from distribution lists.

4. *Business Continuity*

- FIA encourages firms to consider the necessity of a comprehensive disaster response plan in the context of their business. Such plans should designate disaster response personnel with all necessary contact details.
- To minimize the impact of certain types of disruptions, firms should consider the utility of standby failover for production infrastructure such as servers and network hardware in addition to key services such as the trading platform as well as supporting services such as back office and even business e-mail continuity. In addition, business continuity policies may include alternative paths for order execution in the event that trading platforms become unavailable.
- Similarly, FIA encourages regular testing of business continuity plans and participation in both exchange-sponsored and industry-sponsored failover testing, such as the annual FIA Business Continuity/Disaster Recovery test.

5. *Electronic Error Trade Process*

- Executing brokers should have in place flexible but robust processes to address electronic error trades for their trading platform. The process would address situations that are reasonably within the overall control of the broker and be designed to resolve them in accordance with error policies put in place by exchanges to ensure market integrity. The electronic error trade process should include the escalation of issues within the organization but should also give the broker and client appropriate discretion to resolve errors on a case-by-case basis.

Summary

Order Handling Risk Management Recommendations for Executing Brokers is the third a series of risk management recommendations produced by the FIA on behalf of the industry. These recommendations should be considered in conjunction with the *FIA Market Access Risk Management Recommendations* and *FIA Recommendations for Risk Controls for Trading Firms*.

The executing broker has an important role to play in monitoring and controlling market access. These order handling guidelines address the responsibilities of the broker handling client orders that are sent directly to an exchange or worked through an automated execution tool that is under their supervision. It highlights that clients also have responsibilities regarding the conformance of their systems before they submit orders to a market electronically through a broker.

FIA strongly recommends that automated execution tools should always be tested thoroughly before being deployed into production. Where the broker has full control of the execution tool they should ensure that it behaves in a manner that will not cause market disruption and should have controls built in that will logically handle as many different scenarios as possible. However, a broker cannot be expected to certify automated execution tools that are outside of its control, including algorithms or trading models that are the intellectual property of a client or third-party vendor. Instead, through the use of prudent risk management controls inserted by the broker between the client and the market, the chance of inadvertent market impact can be minimized.

By following the practices outlined within this document, FIA believes that executing brokers can provide an electronic trading platform that is robust for their clients to use as well as designed to protect market integrity.

Futures Industry Association
2001 Pennsylvania Avenue, NW
Suite 600
Washinton, DC 20006
202.466.5460 / 202.296.3184 fax
www.futuresindustry.org