FIA

Principal Traders Group

Recommendations for Risk Controls for Trading Firms

The FIA Principal Traders Group has developed ***Recommendations for Risk Controls for Trading Firms*** to expand on the role of the direct access participant as it is described in the *FIA Market Access Risk Management Recommendations* published in April 2010. In recent months, financial regulators have been taking an in-depth look at access to exchange matching engines. Due to the varying scale and complexities of direct access participant businesses, defining specific policies and procedures is outside the scope of this document. Instead, this document offers a number of subjects for firms to consider in the context of their roles as direct access participants. A firm's specific policies and procedures will be based on multiple factors including business need, exchange rules related to membership and direct access, and contracts or agreements between the trading firm and its clearing brokers.

Although the primary audience for this document is firms that directly access exchange matching engines, many of the topics put forth for consideration are broadly applicable to the entire trading community.

Background

This document was created by a working group of the FIA Principal Traders Group. The FIA Principal Traders Group is a forum for firms trading their own capital to identify and discuss issues confronting the principal traders' community. Membership in the FIA PTG is limited to firms that trade for their own account rather than on behalf of customers. The group works to define common positions on public policy issues and advance the group's collective interests through the FIA; improve public understanding of the constructive role played by principal trading groups in the exchange-traded derivatives markets; and promote cost-effective, equal and transparent access to U.S. and non-U.S. markets.

Principal traders are active in a variety of asset classes such as equities, futures, foreign exchange, and fixed income, and on a variety of exchanges, both in the U.S. and abroad. The type of principal trader varies almost as much as the number of traders. Firms engage in automated, manual and hybrid methods of trade generation and execution encompassing various strategies. However, all principal traders have a vested interest in well functioning markets with effective risk controls, clear error trade policies that focus on trade certainty, and a strong regulatory framework. Principal trading firms take seriously their role in the markets—providing liquidity, tightening bid/ask spreads, and contributing to price discovery—and give due consideration to risk controls throughout their organizations to reduce the risk of market disruptions due to unauthorized access, system failures, and errors.

This document includes recommendations for risk controls applicable to trading operations and electronic trading systems ("ETSs").[1] The risk controls recommended here include, and expand upon, those outlined in the FIA Market Access Risk Management Recommendations.

[1] *ETSs encompass a variety of platforms including both manually driven by traders and computer driven automated trading systems ("ATSs"). A major tenet of this document is that all types of ETSs should be continuously monitored and supervised.*

Electronic Trading

Trading firms should have written procedures in place to cover ETS day-to-day operations. Tasks may include confirmation of market connectivity, verification of start-of-day and end-of-day positions and other critical system or business related tasks relevant to correct operation of electronic trading platforms.

Access & Oversight

Firms must ensure their ETSs are supervised at all times while operating in the markets. Staff must have training, experience and tools that enable them to monitor and control the trading systems and troubleshoot and respond to operational issues in a timely and appropriate manner. Firms should have processes to ensure trading operations staff is trained on the expected operating parameters of any ETS for which they are responsible. For example, staff may need to know the expected number of orders per second, maximum position, and maximum open order quantities of an algorithm.

Firms should have policies and procedures for ensuring that appropriate staff involved in supporting electronic trading operations have the necessary authorizations with relevant exchanges, brokers or clearing firms to inquire about order status, manage orders, execute trades by voice or screen, and invoke exchange error trade policies. Firms should have procedures for tracking and updating such authorizations with relevant business partners.

Each ETS should have a management console to display information about the actions and market exposure. This management console should also provide the trader with the capability to control the ETS.

Firms should have policies and processes for setting, modifying and tracking changes to pre- and post-trade risk checks. Policies should specify who is authorized to enter, view and modify pre- and post-trade checks, which checks are enforced, and in what manner.

Firms should consider how responsibilities are assigned for managing pre- and post-trade checks, inputting settings and operating other parts of the ETS and should strive to minimize potential opportunities for unauthorized trading.

Change Management & Testing—Firms should have processes in place to allow representatives from trading, risk, and software management to approve changes and verify internal testing before a new trading system can be enabled in production.

Conformance Testing—Trading firms are required to pass conformance testing with the party providing access when implementing a new direct access system or when the exchange deems it necessary because of a fundamental change in exchange functionality. The onus is on the trading firm to determine when it must recertify due to a change in logic within their system.

Error Control—Trading firms should have documented procedures that direct the actions of traders, ETS trading monitors and support staff in the event of a trading system error. The procedures should be aimed at evaluating, managing and mitigating market disruption and firm risk and should specify people to be notified in the event of an error resulting in violations of risk profile, or potential violations of exchange rules.

Pre-Trade Risk Management

In addition to pre-trade risk controls at the exchange and clearing firm levels, trading firms should set risk controls at the trading firm level.

Pre-Trade Risk Limits—Trading firms should establish and automatically enforce pre-trade risk limits that are appropriate for the firms' capital base, clearing arrangements, trading style, experience, and risk tolerance. These risk limits can include a variety of hard limits, such as position size and order size. Depending on the trading strategy, these limits may be set at several levels of aggregation. These risk limits should be implemented in multiple independent pre-trade components of a trading system.

Price Collars—Trading systems should have upper and lower limits on the price of the orders they can send, configurable by product. They should prevent any order for a price outside of the "price collar" from leaving the system.

Volatility Awareness—Trading systems should take a specified action (have an alert, pause, or automatically disable) if an unusual price move or volume spike occurs during a specified timeframe.

Fat-Finger Quantity Limits—Trading systems should have upper limits on the size of the orders they can send, configurable by product. They should prevent any order for a quantity larger than the fat-finger limit from leaving the system.

Repeated Automated Execution Throttle—Automated trading systems should have functionality in place that monitors the number of times a strategy is filled and then re-enters the market without human intervention. After a configurable number of repeated executions the system should be disabled until a human re-enables it.

Outbound Message Rate—Trading firms should limit the number of order messages their trading systems can send to the exchange in a short period of time. These limits should be in line with exchange rules and the trading firm risk tolerance.

Market Data Reasonability—Trading systems should have "reasonability checks" on incoming market data as well as on generated values.

Kill Button—Trading systems should have a manual "kill button" that, when activated, disables the system's ability to trade and cancels all resting orders.

Market Maker Protections—Firms acting as designated market makers should be aware of and, when appropriate, utilize exchange-provided market maker protections.

Trading Interruptions

Heartbeats Among System Components—Electronic trading systems should monitor "heartbeats" among their various components as well as with the exchange to identify when connectivity to any system component or the exchange has been lost. If connectivity is lost, the ETS should be disabled and working orders cancelled by the system or through exchange-provided "cancel-on-disconnect" functionality.

Emergency Notification Procedures—Trading operations staff should have contact details for incident response personnel responsible for network connectivity, software development, and third-party vendors as well as market operations staff at relevant exchanges.

Back-Up Execution Facilities—Trading firms should have alternate execution platforms available to their traders and trading monitors in the event that their primary systems or direct market access fail. Options include exchange, clearing firm or ISV-provided execution platforms. In addition, firms should have documented procedures for alternative trade execution methods (including trading desk phone numbers, account numbers, clearing information as applicable) in the event electronic trading is not feasible. When trades are executed through alternative methods, firms should have logs documenting the execution of such trades and recording the relevant trade details.

Post-Execution and Back Office

All firms should strive to maintain timely and accurate trade and account information by reconciling as soon as practicable their own electronic trading logs with records provided by their brokers, clearing firms, or other business partners. In satisfying this objective, firms should consider segregating trading and back office roles and responsibilities in such a way that an individual cannot conceal unauthorized trading activity.

Post-Trade Limits—Trading firms can also establish and automatically enforce post-trade risk limits that are appropriate for the firms' capital base, clearing arrangements, trading style, experience, and risk tolerance. For example, a trading firm can set daily loss-limits by instrument, asset class, and strategy and automatically close out or reduce positions if those limits are breached.

Order Fill Validity—Trading firms can monitor order fill messages they receive from the exchange in order to confirm they are valid. Validity can be determined by a number of trade-specific factors including fill price, fill quantity, order ownership, or aggregate measures such as net positions and fill frequencies. Should an order fail these checks, action should be taken to investigate the discrepancy.

Near real-time reconciliation—ETSs should have functionality to accept drop-copies from exchanges and clearing firms. Drop copies are duplicate copies of orders that allow a firm to compare the exchange or clearing firm view of trades and positions with the systems' internal view. This helps to assure that all systems are performing as expected and maintaining accurate and consistent views of trades and positions. The drop-copy data may also be used by risk managers to view their firm's risk exposure independently of the trading system.

Physical Security

Firms should consider physical security at their place(s) of business, co-location and/or proximity sites and be aware of the risk of access to their business infrastructure by unauthorized personnel.

Where feasible, firms should adopt measures such as electronic badges or other controls that limit physical access to their ETSs and/or management consoles at their place of business.

In co-location and proximity sites, firms should understand the security measures provided by the facility and should adopt policies and procedures which, in conjunction with such measures, enhance overall security. For example, a co-location or proximity provider may limit access to individuals named on a list of authorized persons. The firm may adopt policies specifying which personnel can be authorized to enter the facility and the manner in which the list of authorized personnel is kept current.

Electronic Security

Firms should 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, firms with direct access to exchange matching engines should be aware of the potential, once compromised, for intruders to use their network infrastructure to launch attacks against exchange networks or others or potentially engage in unauthorized trading, and firms must take steps to mitigate such risk.

The use of network firewalls, VPN connections or other security devices to prevent unauthorized remote access to business networks is strongly encouraged. Failure to use firewalls or other security measures in order to reduce latency or increase throughput is strongly discouraged.

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. Once authenticated, resources being accessed should ensure users are authorized to do so.

All staff should be trained on proper security hygiene and accountability for passwords and logins. Use of a login other than one's own should be a serious matter for both the owner and the user, particularly in respect to ETSs. Firms should develop policies requiring minimum levels of password complexity (use of upper and lowercase letters, numbers and special characters) and rules specifying whether passwords expire and, if so, how frequently.

Use of detailed logging systems to record user and system activity is strongly encouraged.

To ensure reliable levels of security, third-party electronic security audits, performed at regular intervals, are encouraged.

Firms 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:

- Addressing key and keycard recovery and/or disabling keycard in card reader system
- Withdrawal of trading floor privileges and badge recovery
- Withdrawal of electronic or voice trading privileges from electronic trading systems, brokers or clearing firms
- Revocation of status as an authorized contact, responsible individual or other privileges with exchanges
- Remote wipe and recovery of mobile devices (e.g., Blackberry, iPhone)
- 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 infrastructure components)
- Forwarding user's e-mail to appropriate staff and removal of e-mail account from distribution lists

Business Continuity

Firms should 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 application and supporting services such as back office and even business e-mail continuity.

Business continuity plans should be tested and participation in exchange-sponsored failover testing when available is strongly encouraged.

Futures Industry Association
2001 Pennsylvania Avenue N.W.
Suite 600
Washington, DC 20006-1823
202.466.5460
www.futuresindustry.org