Market Access Rule 15c3-5: The Knight censure brings further clarity to the definition of 'reasonableness': mentions open order limits, technology controls and automated Broker-controlled 'kill switches'.

Alarms, Codes and Lock-Down Modes for the Market Access Rule: SEC vs. Knight

By Anthony Masso, CEO Succession Systems

In 45 minutes, Knight Capital unintentionally acquired a $3.5 billion net long position in 80 stocks and $3.15 billion net short position in 74 stocks. An algo, not able to 'read' the accumulated fills, kept sending orders to market. Knight's proprietary trading systems were not tied into the firm's overall credit thresholds.

4 million orders across 154 stocks

The event moved prices, but the firm's trades could not be broken under the Clearly Erroneous Rule. The result was catastrophic for Knight.

First enforcement of a far reaching rule

Last month, the SEC settled charges with Knight. It is the first enforcement action for the Market Access Rule, 15c3-5. Adopted in November 2010, the Rule is designed to prevent disruption in the financial markets. As such, it is a 'catch all' across many broker regulations. It requires the Broker to measure trading risks and to implement control procedures before the submission of orders to an Exchange or ATS. To comply with 15c3-5, Brokers must consider: Reg SHO, Reg NMS, all Exchange Rules and a host of real-time trading surveillance requirements.

Defining Reasonableness

Written with broad directives, the Rule gives Broker Dealers the ability to establish '***reasonable'*** controls for both client and broker market access. The broad language may give Broker's flexibility, but it also makes the interpretation and implementation challenging. What exactly constitutes 'reasonable'?

Open order limits and lock down procedures

In light of the Rule's broad language and sparse guidance, the SEC Order is particularly interesting. The Order makes clear the need for a comprehensive approach to catch mistakes which can impact the public markets. Of particular note, are 'open order' checks, detailed technology procedures and the call for automated 'lock down 'modes. Here are the top takeaways:

- ***Open order limits for the aggregate firm***
- ***Automatic lock down for trading beyond thresholds***
- ***Use of drop copy reconciliation as system operational check***
- ***Checks to ensure market data is not stale***
- ***Circumvent a single point of failure in the risk control design***
- ***Run 'compliance drills / fire drills' to shut down trades***

The SEC statements set the stage for a holistic, technologically advanced approach to trading risk management. At a minimum, establishing automated 'lock down' controls when open order limits are met is most certainly a discussion topic for the Board.

Selected Observations from the SEC vs. Knight Capital Settlement

Knight SEC Order: www.sec.gov/litigation/admin/2013/34-70694.pdf
Market Access Final Rule: www.sec.gov/rules/final/2010/34-63241-secg.htm

SEC: "Knight did not account for the firm's exposure from outstanding orders"

Outstanding, Unexecuted Order Exposure

The open exposure check used to monitor marketing making and proprietary trading strategies received a clear mention. Other checks that would have helped:

ADV Checks: *Trades were more than 50% of the volume*
Position Limits: *$3.5 billion long*

SEC: "Knight did not broadly consider whether it had sufficient controls to prevent the entry of erroneous orders"

Market Access Kill Switches

The expectations of a 'lock down' mode are becoming clear. The SEC's focus on prevention indicates firms should institute automatic 'shut down' triggers. No longer are humans, monitoring a screen good enough.

Market Access 'kill switches': *Defaulted to trigger upon limit breach*
Pre-set Capital Thresholds, for the aggregate firm: *Knight omitted their proprietary trading group*
Automated Controls: *Knight relied on a person with knowledge of the limits to monitor the screen*
Other checks that could have helped:
Real-time Market Surveillance Alerts: *Reports to detect deviations from "normal" parameters*
Warning Zone Triggers: *Allows for alternative action before a full shutdown*

SEC: "Ask [what] would happen if the component malfunctions"
"The Commission believes controls should be reasonably designed to detect malfunctions" and "ensure the orderly deployment of new code"

Technology Controls

The Commission seemingly wanted to clarify the area of technology controls, technology design resiliency, and considerations of computer malfunction checks. Several mentions are of note:

Use of Drop Copies: *Compare router [algo] before and after drop copies*
Market Data Check: *Knight did not test for stale data*
Technology Compliance for ALL systems: *Including prop trading*
Change Management Procedures for Deployments: *Second technician review, Knight Technicians left old code on one server*
Testing Log(s): *Consider the use of UAT testing certification of patches and updates*

SEC: "Supervisory procedures to guide employees' responses to <u>significant technological</u> and compliance incidents"

Compliance Codes and Drills

When everyone is in agreement, it's fine. But how will the employee react to conflicting instructions or information? Every second counts against you while the client screams for one course of action, co-workers suggests another. The stress of real-time trading situations can cause paralysis.

How to Shut Off and Lock Out: Ask your team about a particular algo, client or router
Keep an Incident Log: Add them to your risk scenarios
Work with Clients: Communicate "your" procedures
Run Compliance Drills: Like fire drills, go through the code of conduct and chain of command