105 WESSON TERRACE, NORTHBOROUGH, MA. 01532
TEL: 212 809 3800
www.tellefsen.com

October 31, 2013

Ms. Melissa D. Jurgens,
Secretary of the Commission,
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street NW.
Washington, DC 20581.

Re: CFTC Concept Release – Risk Controls and System Safeguards for Automated Trading Environments RIN 3038-AD52

Dear Ms. Jurgens:

We are pleased to provide you with our comments and views about the CFTC's recent concept release for Risk Controls and System Safeguards for Automated Trading Environments

Tellefsen and Company, L.L.C. ("TCL") supports the concept of Risk Controls and System Safeguards for Automated Trading Environments as a mechanism to improve risk management in our nation's derivatives and futures markets, and instill investor confidence and faith in our industry's ability to appropriately mitigate technological and operational risks.

We urge the Commission to consider the simplicity of the approach, the level of complexity in the implementation and the impact on liquidity when implementing any or all of the risk controls or system safeguards under consideration.

The enclosed perspectives are our own and do not necessarily reflect the views of major exchanges, investment banks, broker dealers, automated trading systems, trading platform providers or industry organizations.

Background:

TCL is a boutique management consulting firm founded by Gerald Tellefsen in 1984. Since then, the firm has been exclusively focused in the global capital markets, derivatives and financial services industries.

Over the years, we have worked for numerous market constituents - major U.S. equity, options and futures exchanges, clearing organizations, futures commission merchants, securities broker-dealers, investment banks, proprietary trading and asset management firms.

Four of our major, relevant practice areas include market structure/micro structure consulting, regulatory compliance, operational risk management and business continuity management, which we believe qualifies us to provide domain expertise, industry insight and direct working knowledge guidance to the Commission:

1. In our market structure practice area, we have consulted to exchanges, ECNs, ATSs, interdealer brokers, start-up markets and other market participants on the workings of the equity, options and futures markets.

2. In the market micro structure arena, we have assisted these entities with the development of comprehensive system testing strategies and plans. These have included user acceptance testing, quality assurance testing, stress and failover testing, etc. Most of these assignments have been relative to CFTC Core Principles or SEC ARP compliance.

3. In the regulatory compliance arena, we have consulted to futures commission merchants, exchanges and clearing houses on the evolution and interpretation of regulatory changes, including the convergence of the exchange traded and OTC markets, Dodd-Frank and EMIR regimes, etc.

4. In the operational risk management and business continuity management practice areas, we have consulted to exchanges, clearing houses, investment banks, broker dealers, futures commission merchants, investment management firms and proprietary trading firms.

We have advised and provided our counsel to these market participants on their business continuity strategies and plans, technology and network architectures and set ups for key, mission critical systems (i.e., electronic trading, order management, market data dissemination, price reporting, clearance and settlement, surveillance and risk management).

Our firm has been actively involved with the Futures Industry Association ("FIA") for over 15 years and our principals have been members of the FIA Information Technology Division. In this capacity, John Rapa chairs the FIA's Business Continuity Management committee and has coordinated the annual industry DR testing since 2003.

Proposed CFTC Rulemaking:

The main thrust of the concept release encompasses enhanced approaches and sound practices to the development, management, operation and maintenance of mission-critical systems used to operate and support fair and orderly markets.

The Commission seeks feedback on how risk controls and system safeguards can be best implemented and be most beneficial to the markets and market participants. In addition, the Commission is seeking feedback on the potential for uniform order/trade cancellation and adjustment policies and the circumstances for trade cancellation.

When and if enacted, the concept release will potentially have a significant impact on the technology, strategic direction and cost structures of numerous market constituents, including but not limited to: exchanges, operators of automated trading systems, futures commission merchants, broker-dealers, trading and back office system services providers and clearing firms.

The Commission seeks input and counsel as to what should be within the scope of the concept release for risk controls and system safeguards, what can be applied as consistently as possible and what the potential impact and costs thereto would be.

Under the concept release, Designated Contract Markets ("DCMs" or "exchanges") and firms that operate Automated Trading Systems ("ATS") would be required to conduct adequate, regular testing and review of their automated trading and clearing systems to ensure properly functioning systems, and have adequate capacity and security.

The rush to develop and implement faster trading technology and infrastructures is analogous to an arms race. This increase in speed has magnified the damage from and the visibility to technical problems and system disruptions.

The unintended consequence of this is that it can greatly impact exchanges and ATSs priorities. If developing, testing and implementing bullet proof software slows the system down by a few microseconds, an exchange or ATS provider trying to be the fastest might think re-think it.

From our direct experience and working knowledge of the major exchanges, futures commission merchants ("FCMs") and global clearing houses, they have built out and evolved their technology infrastructures and networks in the last 3-5 years and have designed resiliency, redundancy and fail over capabilities into their mission critical system architectures.

They have learned valuable lessons from the September 11, 2001 disasters, the Northeast blackout of 2003, Hurricanes Rita and Katrina and most recently Hurricane Sandy. They have become sensitive to system disruptions and the potentials for physical threats, terrorist attacks, acts of God/nature, cyber terrorism, software worms, spoofing, and pandemics.

The main thrust of the concept release encompasses enhanced approaches and sound practices to the development, management, operation and maintenance of mission-critical systems that support fair and orderly markets.

The Commission acknowledges that the industry is comprised of numerous market participants of varying sizes and that have diverse business lines (e.g., agency only, principal trading only, market making, hybrid, etc.).

As a result, we strongly believe that there are multiple ways to achieve the same risk management objectives, and any "hard coded" approaches are likely to become obsolete very quickly.

Over the last decade, the exchanges, ATSs, FCMs and clearing houses have refined their strategies, plans and tactics via regular testing and enhancements to processes and procedures. The backdrop of this has been commensurate with:

- The growth of electronic trading / compression in open outcry trading
- Introduction of new products, new systems, new business lines
- Globalization of trading and clearing constituents
- Growth and introduction of proximity hosting, algorithmic trading, high frequency trading, direct market access
- The availability of new system and network technologies and tools that are more advanced and cost-effective than previous generations
- New technologies and tools that can identify/isolate network and/or system faults, facilitate system failover/roll back capabilities
- Modern tools and technologies that allow them to remotely manage data centers, systems, servers and networks, failover/roll back systems, load balance systems and networks – with limited technical staffs
- Regulatory evolution
- Technologies that have redundant hardware components and/or software tools to facilitate backup and recovery capabilities.

Comments and Areas of Concern:

We are concerned that the concept release, as structured, is overly broad and has numerous potential and unintended consequences. Many of the questions, definitions and potential safeguard areas contain numerous absolute determinations that would trigger compliance requirements.

As such, we have reviewed the proposed rulemaking and have comments, observations and concerns in the following areas:

1. Scope and Applicability
2. Pre and Post-Trade Risk Controls
3. Standardizing and Simplifying Order Types
4. System Safeguards - Order and Trade Cancellation Policies and Procedures
5. ATS Design, Testing, Information Security and Change Management
6. Incident Management Procedures

7. Data Reasonability Checks
8. Requirements for Firms that Operate ATSs
9. Market Evolution and Preparing for the Unknown

1. Scope and Applicability:

The scope and applicability of the proposed rulemaking should address the unintended consequences of the growth and introduction of high velocity, high frequency trading.

Taking into consideration the demographics of order flow providers, the proliferation of algorithmic trading, high frequency trading and flow trading, even the smallest, least capitalized, tech savvy traders can rapidly flood the market with thousands of orders, cancellations and messages that have the potential to slow down, clog or disrupt even the best tested and most resilient exchange or ATS trading infrastructure.

The proposed rulemaking goes into great detail to suggest various quantitative trigger points that would require an entity to become compliant.

As the remaining aspects of Dodd-Frank crystalize and given their importance in the convergence of the OTC and exchange traded derivatives markets, securities based swap execution facilities ("SEFs") and swap data repositories ("SDRs") should also be required to be compliant with the rule making.

In this regard, those exchanges, clearing houses and ATSs which are deemed "systemically important" to the fair and orderly operations of the US markets should be subject to its compliance.

2. Pre and Post-Trade Risk Controls:

The Commission seeks feedback on various aspects of pre-trade and post-trade risk controls, as well as understanding what are the existing sound practices in this area.

Our firm has direct working knowledge of various pre-trade, at-trade and post-trade compliance requirements at numerous global derivatives market. We have recently conducted an exhaustive review of global derivatives markets for a major global futures commission merchant with operations in North America, Europe, the Middle East and Asia Pacific.

The client operates multiple front end execution management systems, numerous sales/trading desks and connectivity to over 57 global equity, options and derivatives markets. They have recently replaced several execution management systems ("EMS") with a centralized order management system ("OMS").

To ensure that the new system has the requisite regulatory compliance features and functions, our firm researched and developed the requirements for each of the 57 markets, relative to:

Pre-trade risk controls, DMA controls, limit order protection, limit order display, maximum order sizes, maximum position sizes, permissible native order types, complex orders, best execution, trade reporting, market data permissioning, user authorization and permissioning, drop copies, audit trail, market abuse controls, and other local market nuances.

The key requirement for our client's implementation of the new OMS was that the system was flexible enough and functionally rich enough to accommodate these nuances, across the markets that the system operates on.

As a result, we can attest that there are many inconsistencies across global derivatives markets as to what pre-trade and post-trade functions they either require or accommodate.

Many of the proposed controls listed in the concept release are required or offered by major derivatives exchanges, however, there are inconsistencies and there is no "one size fits all" across the board.

Current controls at exchanges and FCMs can include price tolerance and order size controls, credit risk limits, order/trade drop copy capabilities, message throttling capabilities and switches to cancel working orders upon a disconnect from the network.

The FCM in this case uses the OMS to set the pre-trade and post-trade controls to screen client orders/reports. In many cases, the "house" rule for these market controls is set at a more stringent level than the exchange prescribed controls.

One of the commonly accepted mechanisms to capture pre-trade information is via drop copies. FCMs and GCMs commonly utilize drop copies of trade execution data, obtained in "near real time", to perform risk management on their downstream customers, DMA clients, etc.

This data is captured by their FIX gateways and fed to their risk management systems. Some firms also capture drop copies of orders for the same purposes.

In high frequency trading, firms may have a challenge keeping up the volume and velocity of drop copies and the sequencing of transactions.

If FCMs do not have front end systems such as OMS, EMS of FIX gateways that are flexible enough to accommodate these capabilities, they will have difficulty in complying and will either be forced to change systems or incur heavy costs to enhance their systems to be compliant.

3. Standardizing and Simplifying Order Types:

Global derivatives exchanges' trading systems support numerous order types, trading qualifiers and trading strategies. Much of this stems from the evolution and asset class focus of these markets.

As new products and trading strategies have been introduced, trading firms and ATS operators have created new order types (or variations of existing order types), in an attempt to provide market participants with new ways of gaining an edge in the market (e.g. a new limit order type that would prioritize orders that remain resting in the order book for some minimum amount of time).

Order types have been introduced that contain complex logic embedded within them. These have challenged front end trading system providers and firms that operate them to retro-fit these capabilities into OMS and upstream risk management systems.

TCL believes that attempts to simplify or standardize order types across exchange and ATS will not improve the effectiveness of such controls, and have the consequence of stifling creativity and reducing innovation in our industry.

As a result, we do not believe that attempts to simplify or standardize order types will provide any additional protection to the markets.

4. System Safeguards - Order and Trade Cancellation Policies and Procedures:

There has been much publicity and opinions lately about the need for exchanges, ATS and other trading platform providers to have "kill switches" that can be triggered if there are disruptions similar to the Flash Crash, Knight Capital, BATS, CBOE, Direct Edge, London Stock Exchange, NASDAQ, Hash Crash, SIP disruptions etc.

Given the rapid acceptance and growth of high frequency trading and the potential adverse impact on exchanges' and firms' trading infrastructures, it would be prudent for exchanges to impose a minimum time period for which orders must remain on the book before they can be withdrawn (i.e., resting orders).

In TCL's opinion, this resting time should be applied to all orders, irrespective of size. Implementing this across the board on either a product or product family basis will provide an improved level of fairness to the markets.

However, from our direct experience, there are no consistent policies or procedures across global markets, when it comes to order/trade cancellation practices.

a. Kill Switches:

The Commission also seeks feedback on "automatic shut-offs or kill switches" that would turn off trading programs when they run afoul of preset limits on risk or other parameters, and at what point people are able to step in to switch off a system.

Global market regulators are trying to gain a better grasp on heavily-automated markets, alongside a separate review of big high-frequency trading firms and an investigation into whether some high-speed firms enjoy special advantages when dealing with exchanges.

However, market practitioners are concerned that if an automated kill switch kicks in at the wrong time, it may have the effect of de-stabilizing the system. Firms are generally reluctant to pull the trigger and shut off their order flow from the market.

They are concerned that the timing of the decision to turn off the system may lie with understanding the nature of the underlying problem.

Many brokers want to be alerted before their orders are cut off, to be able to explain to their customers if the trading is unusual or normal.

Market participants and regulators have debated the need for multi-level kill switches, whereby an exchange or ATS would notify firms by phone calls or email before cutting off their order flow.

But, this may have the effect of setting kill switch trigger points with a wider margin of error to their threshold calculations.

Others are concerned that we do not add more layers of complexity onto an already complex, fast moving market structure.

With today's high speed, smart routing of orders to the best market, how effective would a kill switch be on orders that are "routed away" or in flight?

There are pros and cons to the concept of having a kill switch. Consider the following:

- How would the kill switch account for inter-product or inter-market spread orders? What is the exposure if only one leg of the order strategy was killed?
- Who is liable to the customers for any resultant market action error trades?
- A kill switch with one threshold based on one variable will not work!
- The last thing people want is a well-intentioned kill switch that disrupts proper (i.e., not run away) market activity

The concept of a kill switch is a great idea, but it is inconceivable that an exchange, ATS or trading platform provider will implement a system that abdicates the total control of the market or system's operations to an automated kill switch function.

If more trained eyeballs were looking at control screens during the above problems, humans would have intervened and common sense would have/should have prevailed.

Real-time monitoring systems should identify any indications of run-away or irregular market movements and should provide real time alerts to market oversight staff. They, in turn, should have access to kill switches that they can activate once they have determined that the condition is irregular.

Fast moving, complex, inter-linked markets need smart technologies as well as smart humans overseeing them.

5. ATS Design, Testing, Information Security and Change Management:

a. System Design and Testing:

Recent high-profile market disruptions illustrate the urgency for conducting design reviews and quality assurance reviews of mission-critical systems.

In today's competitive markets, it seems that the urgency to "get it out" has superseded the rationale to "get it right".

Lack of proper attention to detail/oversight, making production changes on the fly, etc. can lead to operational risk or reputational risk. Both can be costly as we have seen in the last few months and can lead to significant realized losses.

As markets have become more fragmented, inter-linked and reliant on high velocity data, the complexities of systems design and interrelationship of these "moving parts" may not be fully understood by technologists or business staff.

This becomes exacerbated when something goes wrong, and the law of unintended consequences comes into play. These incidences hit the media as "software run amok", "rogue software" or "tech glitches".

In the last 5-7 years, algorithmic trading has permeated global markets – equities, options, futures - and, as electronic market making has taken off, so has the phenomenon of proximity hosting / co-location.

Competition, market structure changes, smart order routing and shrinking margins have driven the need for speed and smart technologists have discovered cleaver ways to gain an edge via low-latency hardware, software and network technologies.

This arms race has escalated the speed at which trades are executed at, and the overall market velocity.

Business analysts and trading systems software designers need to have sanity checks – both in systems design review by humans - and in the logic of the system code.

An order or trade that moves the market and creates a new high or new low outside the primary market - may not be the intent of the trading strategy or the system's design.

Trading systems should have logic in the code or circuit breakers that stop run-away algorithms or slow down order flow, so that humans can intervene and determine what the underlying problem might be.

Once an abnormal or unrealistic market condition is detected, the system should have separate logic on how/when to handle it.

This could be as simple as stopping or slowing the order flow and presenting it to an experience trader for review/release.

The Knight Capital problem in August 2012 may have been as simple as a trader that missed a setting for a TWAP algo (e.g., set the order to execute in 5 minutes versus 5 days), or as egregious as an inadequately tested software release.

The other previously described high profile technology disruptions that roiled the markets, may have been able to be avoided if those entities invested the time and effort to do a proper code review and extensive testing of the system.

In our professional experience, these types of problems are difficult to totally prevent and cannot be solved via regulation.

We believe they can be mitigated by:

- Conducting software walk-throughs with both software engineers and subject matter experts

- Back-testing for highly irregular trading (e.g., high water mark days) (e.g., May 6, 2010 Flash Crash, August 1, 2012 Knight Capital sell off, etc.)

- Conducting QA reviews for defects in application design logic; stress and regression testing.

b. Industry Testing Initiatives:

TCL supports the notion of robust testing and evolving business continuance planning and disaster recovery capabilities.

From our direct knowledge of the major equity and options exchanges and numerous ATS, they already perform a number of testing initiatives as part of their resiliency and obligations to operate fair and orderly markets:

- As exchanges, ATSs, trading platform providers and clearing houses have introduced new systems, applications, products and system functions, their internal IT staffs have conducted regular system testing, regression testing, stress testing, failover testing etc., to ensure their availability, capacity, resilience and readiness

- They have invested in the technology and people skills required to maintain the systems infrastructure and environments that facilitate fair and orderly markets

- These organizations regularly augment IT testing with other BCM exercises (e.g., they conduct annual BC/DR plan updates, building evacuation drills, and business disruption scenario planning workshops)

- In addition, all the U.S. exchanges and clearing houses have participated in the planning and execution of the annual DR test initiative conducted and coordinated by the FIA.

- These industry tests were started after the events of September 11th 2001 and are have now passed their 10th year.

- The FIA industry-wide tests have involved a tremendous amount of planning, foresight and coordination.

As the Chair of the FIA's Business Continuity Management ("BCM") committee, I can attest that thousands of man-hours of preparation are required by FCMs, exchanges, clearing houses and key service providers' staffs to prepare for and execute the annual industry test.

When the FIA BCM committee was started in 2002, one of the original goals was to establish a common date where most/all firms can test with the various exchanges they belong to once annually, as opposed to testing with multiple exchanges on multiple dates throughout the year.

The industry test has been intended to provide the opportunity for exchanges and their members and major service providers to test their backup systems and sites and leverage the economy of scale of doing it all on one day.

It has not yet been intended to be a scenario exercise (e.g., neighborhood or key service provider outage, Lower Manhattan outage, Chicago Loop outage).

Since most of these firms are constantly making changes to their infrastructures and environments, there are a lot of "moving parts" and the potential for many things to go wrong. Planning and conducting regular tests such as these are important tools to test the resiliency of systems infrastructures.

The firms and exchanges have found the annual industry testing valuable - to be able to test the resilience of their infrastructure, and fail over to their backup systems and facilities, to ensure they work "as designed" and "as specified".

Unless they have an actual disruption, invoke DR and fail over during the course of the year, they do not have the opportunity to ensure that their networks, firewalls, systems and infrastructure that support business continuance really work as expected.

The FIA industry tests have not been mandatory, but over the years we have enhanced the scope of testing, encouraged and engaged more firms, exchanges and market entities to participate each year.

We have developed and enhanced the process to engage the exchanges, clearing houses and firms, educate them on the scope of the testing and manage the overall test process. In addition, we have actively expanded the test every year to include more firms and exchanges.

This year, for example, the annual FIA industry test* involved 23 exchanges and clearing houses, 64 futures commission merchants/clearing and non-clearing firms. The exchanges reported that the firms that tested represented ~80% of their clearing members and that these firms do ~83% - 95% of their YTD 2013 volumes.

The exchanges typically engage their mission critical production and backup systems and facilities for the test. As part of the scope, it is expected that firms typically fail over from production to their backup systems/sites.

Since no changes to application software code are anticipated, the backup should function identically to production. Typically, firms are required to enter a small but meaningful amount of orders in specified products, from which the exchanges will send execution reports.

This is intended to test the efficacy of round trip communications of orders, quotes, execution reports and related messages. The intent is that if firms can enter a few orders in DR mode effectively, they can trade.

---

* See the enclosed link to the 2013 industry test results on the Futures Industry Association website:
http://www.futuresindustry.org/downloads/2013_DR_Test_Results_Final_101613.pdf

However, given the scope of these tests, they are not designed to be "stress tests", given the complexities of orchestrating a stress test with so many players across multiple markets on a Saturday.

We suggest that the Commission consider that at any given time, there will never be a 100% participation of all market participants in testing, no matter how much advanced planning is done (e.g., we have had firms cancel on the day before the industry tests due to changes in internal operational schedules and senior management priorities).

The Commission should consider an "80-20" approach to mandatory testing, i.e., typically 20% of the firms might provide 80% of the order flow or liquidity.

If exchanges and ATS entities can engage their key order flow and liquidity providers that collectively provide at least 80% of their total transaction volumes, they should have a core nucleus of liquidity, and thus be capable of managing a fair and orderly market.

If exchanges and ATSs require their "systemically important" order flow and liquidity providers to test and encourage as many of the rest to do the same, one can conclude that they should be prepared and can manage a fair and orderly market with that subset.

With all this said, the best system testing strategies, written procedures and policies, robust capacity planning, testing and state of the art technologies are *not designed for multiple events all going wrong at the same time*.

Hurricane Sandy in 2012 was a perfect example of this.

Comprehensive BC/DR plans today should be able to achieve recovery time objectives ("RTOs") of the next business day for trading and two hours (2) for clearance and settlement operations.

However, the demand by regulators to "...trade, no matter what..." is not appropriate under wide area disruption scenarios such as Hurricane Sandy, and is potentially unrealistic.

In a situation like Hurricane Sandy, mandating rapid recovery of mission critical systems creates potential risks wherein exchanges and ATS entities must choose between putting the safety of their employees and market participants at risk, against risking a potential rule or core principal violation.

With New York City, State and Federal authorities closing all major roads, public transit, busses, bridges and tunnels, the ability to commute or move staff out of harm's way or into place to support the business was adversely impacted.

Considering that there was no immediate loss of life of industry staff, the decision by NYSE, NASDAQ and the SEC to close the primary cash equity markets on Monday and Tuesday was the right thing to do, and, as expected, impacted liquidity on U.S. derivatives exchanges and other global markets.

At minimum, the Commission should consider that even where BC/DR capabilities exist and are ready for use, other factors may exist that would justify the delay of operations from DR facilities.

c. Information Security:

Information security breaches, website hacking and denial of service attacks are constant and growing threats in today's wired world, and global financial services firms have been the target of many of these disruptions or attempts.

The proposed regulation calls for increased vigilance and hardening of information security ("InfoSec") controls for their mission critical systems and information.

We believe that as part of the proposed regulations, exchanges and ATSs should be required to demonstrate to the Commission the scope and extent of their InfoSec controls, technology infrastructure, processes and written procedures.

This should include, but not be limited to activities such as regular, independent reviews of network security, controls, network penetration tests and policies and procedures to identify, isolate and mitigate the effects of InfoSec breaches.

The target systems for this should be those mission critical systems that are utilized to "run the business" and that have client-facing impact. Those systems that are utilized internally for testing or that do not have a point of entry from the public Internet should not be subject.

Independent, network intrusion detection tests should be conducted, *both from outside an entity's firewalls and from within.* Testing should conducted by qualified, independent network security firms in concert with the entity.

Testing should encompass, but not be limited to: network intrusion, penetration testing, phishing attempts, worms, virus, denial of service attacks, etc.

InfoSec systems, processes and procedures should encompass mission critical systems (e.g., order management, risk management, trade matching, clearance and settlement), as well as any web portals, internal shared drives and systems that support the management and administration of the business (e.g., finance, operations, administration, regulation and surveillance)

d. Change Management:

Some of the high profile system blow ups previously described above could have been prevented if a more rigorous change management process were in place.

Exchanges and ATSs should have formal processes and procedures for change management. These should encompass the process for testing, migrating and installing new software features/functions from development, quality assurance environments into the production environments.

The exchanges and ATSs should have a formal production installation authorization ("PIA") process, whereby any software changes are subject to a review and signoff process.

This process typically involves key representatives from application software development, middleware development, quality assurance and systems operations staff, and is overseen by a senior operations manager or the chief technology officer.

In our professional opinion, in a PIA environment, NO ONE should be allowed to touch or change the production systems. This includes the installation of software fixes or patches intra-day or "on the fly".

The testing procedures suggested in the Concept Release are overly broad and potentially incompatible with the notions of disciplined change management and the ATS systems to which it is targeted.

By requiring the testing of any changes to the ATS prior to implementation, and periodic testing of all such systems and any changes to such systems after their implementation, the safe harbor provisions of the Concept Release would force ATS entities to take a narrow view of what constitutes a change.

6. Incident Management Procedures:

With the growth of electronic trading over the last 7-8 years and the volume and velocity of information, we have seen more high profile system and market disruptions making the financial news headlines.

We reiterate our earlier statement that there is no "one size fits all" approach to the market. Attempting to standardize a crisis or incident management procedure will be challenging and difficult to implement.

Attempting to hold senior management accountable for certifying and signing off on the effectiveness of their procedures and testing, when there are variables outside of their control will not be well received.

If thresholds for risk event notification and reporting are to be considered, the Commission needs to better understand from market participants as to how and where the triggers could be practically implemented, given the market structure and global composition of the industry participants.

Objective feedback is needed from senior technologists who have built and implemented large complex trading systems, as well as senior management from exchanges and trading platform providers that are responsible for trading operations.

These individuals should have experience with the vagaries and nuances of trading, as well as how to best handle disruptions dynamically, on the fly, while maintaining fair and orderly markets.

7. Data Reasonability Checks:

Exchange trading and market data systems typically have logic that perform reasonableness checks on structured market data. These include price reasonableness checking and range checking on market data to preclude posting incorrect prices, setting new highs/lows or mis-posting bid/offers.

Exchange market data systems or sub-systems have this type of logic as part of the exchanges' obligation to maintain fair and orderly markets.

In the last few years, a number of firms have captured and "mined" news data and social media communications in an attempt to gain an edge in the market. Many of these flow traders analyze social media venues looking for directional plays.

Industry participants and regulators have come to realize that the velocity of market moving events has been exacerbated as a result of the proliferation of smart phones, tablet computing and social media tools such as Twitter and Face Book.

The challenge to technologists and risk managers is how to capture, edit and process these large quantities of unstructured data.

The April 2013 "Hash Crash" - when the Associated Press's Twitter account was hacked and caused the Dow to sell off 144 points in two minutes - is illustrative of how imbedded the monitoring of social media is in the global financial services industry.

The pervasive use of social media has generated unprecedented amounts of social data. Mining social media has the potential to extract actionable patterns that can be beneficial for business, users, and consumers.

Social media data is vast, noisy, unstructured, and dynamic in nature, and thus subject to numerous and novel challenges.

Our markets must keep up with the evolution of financial technologies, and to ignore the power that social media has on market-moving events is a gross mistake.

Data mining of social media will continue to evolve, and new, commercially available technologies and routines will be created.

In TCL's opinion, the equivalent systems operated by ATSs should also be required to demonstrate the same levels of controls.

8. Requirements for Firms that Operate ATSs:

TCL believes that the Commission should create a category of ATS and that firms that operate ATS within CFTC-regulated markets should be subject to registration and CFTC oversight.

Furthermore, there should be an appropriate level of coordinated oversight of the ATS between the relative regulatory organizations (NFA, FINRA etc.), given the size, scale and asset class focus of the ATS.

However, TCL firmly believes that there should not be different standards for ATS that deploy HFT strategies and those that do not.

TCL believes that for ATS that are subject, they should be required to certify their pre-trade risk controls, post-trade risk controls and other system safeguards at least annually, or whenever a major functional change to their business environment is implemented.

Furthermore, the concept of self-certification and notifications by ATS involves considerable challenges to the ATS and the market, should the ATS be required to notify other market centers when "risk events" occur.

Barring the creation of a real time, centralize switching system, the interconnectivity challenges to comply with this would be daunting.

9. Market Evolution and Preparing For The Unknown:

We hope that the Commission receives thoughtful and insightful feedback and suggestions from market participants as to how the proposed rulemaking should be implemented.

Given the current state of market structure in U.S. markets today, we urge the Commission to consider market evolution and unknowns as it solidifies its approach to the proposed regulations.

Market impacting events such as the previously described system disruptions, cannot be easily foreseen nor adequately tested for.

The next major headline event will not necessarily the same as these. The biggest unknown is the impact from the law of unintended consequences.

Many of the issues that the Commission seeks to resolve have been caused by the volume and velocity of trading created by market evolution and fragmentation (e.g., algo trading, smart order routing, inter-market sweep orders, co-location).

As our markets evolve, our regulation and compliance oversight needs to evolve in lock step. In order to do this, we need smart regulation to be able to evolve hand in hand with smart technologies.

Conclusions, Going Forward:

In our professional opinion, most/all of the entities under discussion have the technology and network infrastructure and procedures in place to address the spirit of what the Commission is seeking.

However, the general rule of thumb is that *one size does not fit all*.

The Commission should implement a workable approach, commensurate with the size and scale of the respective DCMs, DCOs and ATSs, and consider how each of them are set up and organized to achieve them.

We believe that the Commission should consider modifying its guidance on what constitutes "materiality" and rely on a risk-weighted determination made by the exchange or ATS.

We urge the Commission to consider implementing a framework for risk mitigation, as opposed to risk elimination.

If rushed to implement, a broad based approach to these new standards may only be as good as the weakest link that exists – the slowest, least capitalized organization that is the last one to have this capability in place.

Regular and varied testing will be key to corroborating industry readiness going forward.

We suggest the Commission look to the exchanges, ATS and key trading platform providers for their feedback.

In today's inter-connected, sub-millisecond high-speed markets, we need smart regulation, not more regulatory crush… having a zero tolerance for risk controls and system safeguards will not cut it… a degree of common sense must prevail!

Our best counsel to the Commission is to analyze the feedback from the comment period, and assess the time frames that the major exchanges, ATS and key trading platform providers indicate that they can adopt the new standards.

We would be pleased to continue the dialogue with you and other industry constituents. We will be available for any follow up questions or to discuss the state of industry sound practices in this area.

Very truly yours,

John J. Rapa

John J. Rapa, CBCP
President/Chief Executive Officer

TELLEFSEN AND COMPANY, L.L.C.