Tellefsen and Company L.L.C.

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

August 29, 2016

Mr. Brent J. Fields
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549-1090

Re: SEC Proposed Rule – Adviser Business Continuity and Transition Plans, Rule IA-4439, File No. S7-13-16

Dear Mr. Fields:

We are pleased to provide you with our comments and views about the SEC's proposed rulemaking on Adviser Business Continuity and Transition Plans ("BCTP").

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:

Tellefsen and Company, L.L.C. ("TCL") is a financial services 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 investment management firms, U.S. equity, options and futures exchanges, clearing organizations, futures commission merchants, securities broker-dealers, investment banks and proprietary trading firms.

Three of our major, relevant practice areas include market structure consulting, operational risk management and business continuity management ("BCM"), which we believe qualifies us to provide domain expertise, industry insight, direct working knowledge and guidance to the Commission.

We have conducted numerous operational risk assessment reviews of large investment management firms, and have conducted comprehensive assessments of their operations and businesses (trading, portfolio management, research, operations, portfolio accounting, fund accounting, finance, tax accounting, information technology, legal/compliance).

We have developed BCM strategies for these entities, as well as comprehensive business continuance and disaster resilience plans. We also have conducted independent test oversight and attestation reporting for various market participants, as part of their regulatory compliance.

We have provided our counsel to these entities 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 services, clearance and settlement, portfolio management, accounting and risk management), and staff remote worksite recovery, connectivity and resiliency.

In addition, our firm has been actively involved with the Futures Industry Association ("FIA") for over 15 years and our principals have been officers and members of the FIA Market Technology Division.

In this capacity, John Rapa has chaired the FIA's Business Continuity Management Committee and coordinated the annual industry DR testing since 2003.

The Proposed Rulemaking:

The Commission has developed a proposed rulemaking (a new Rule 206(4)-4 and an amended Rule 204-2 of the Advisers Act), that, if enacted, would require all SEC registered investment advisers to adopt and maintain written business continuity and transition plans, that are reasonably designed to address operational and other risks related to significant business disruptions in the adviser's operations.

The Commission seeks input and counsel as to what should be within the scope of the rulemaking.

Business Continuity Management is analogous to Operational Risk Management. We view business continuity plans ("BCPs") as operational risk management documents that have been designed and developed for use in response to significant business disruptions ("SBDs"). A BCP is an insurance policy that most firms hope they will never need to use.

From our perspectives, most organizations do an excellent job in this area and have been diligent in their BCM planning and implementations.

In our experience and working knowledge of numerous large investment managers (AUM of between $1 billion and $40 billion), they have built out and evolved their technology infrastructures and networks over the last 3-5 years and have designed resiliency, redundancy and failover capabilities into their mission critical system architectures and infrastructures.

They have learned valuable lessons from the September 11, 2001 attacks, the Northeast blackout of 2003, Hurricanes Rita and Katrina in 2005, and Hurricane Sandy in 2012. They have become sensitive to the potential for physical threats, terrorist attacks, acts of God/nature, cyber terrorism, software worms, spoofing, pandemics etc.

These firms have refined their strategies, plans and tactics accordingly via regular testing and enhancements to processes and procedures. The backdrop of this has been commensurate with:

- The complexity and introduction of new investment strategies, new products and new systems
- The growth and availability of internet-based applications service providers ("ASPs") of applications and systems that span the lifecycle of trading
- Growth of proximity hosting, algorithmic trading and direct market access
- Migration of selected services and applications to cloud-based service providers
- The availability of new system and network technologies and tools that are faster, cheaper and better than previous generations
- New technologies and tools that can identify/isolate network and/or system faults, and facilitate system failover/roll back capabilities
- The evolution of cybersecurity tools and services
- 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.

Most of the investment management firms we work with have mature BCPs that conform to industry sound practices for business continuity management. Their plans address:

- The identification of mission critical systems, data and key service providers
- Recovery time objectives ("RTOs") for mission critical applications, systems, services and infrastructure
- Replication and backup of critical data and systems
- An Incident Management Team structure ("IMT") to respond to and manage significant business disruptions ("SBDs")
- Use of two or more key service providers in selected mission critical areas (e.g., trading venues, prime brokerage, market data services)
- Alternate communications with their staff

- Alternate communications with their clients
- Rally points for building evacuation/staff dislocation from offices
- Use of hardened data centers for their primary and DR data centers
- Use of alternate work sites/remote offices for work recovery
- Communications with regulators

These firms also regularly test the efficacy of their plan strategies. They conduct various BCM exercises, including, but not limited to:

- Failover tests from production to back up sites to corroborate RTOs
- User remote connectivity tests with users
- Periodically working from remote work site locations
- Building evacuation drills to designated rally points

Comments and Areas of Concern:

We have reviewed the proposed rulemaking and have comments, observations and concerns in the following areas:

1. Definition of Significant Business Disruption
2. Scope and Applicability
3. Business Continuity Resilience
4. Transition Plans
5. BCP Disclosures
6. Information Security
7. Vendor Due Diligence
8. BCP Maintenance/Records Retention

1. Definition of Significant Business Disruption:

In our BCM practice, we define a significant business disruption ("SBD") as *anything that prevents you from opening for business on the next business day*. This could be an internal malfunction, blocked access to the office building for more than a day, loss of a key service or part of the infrastructure, loss of the telephone switch or internet connectivity etc.

In situations like these, the Incident Management Team would be convened to identify and oversee the disruption scenario, and counsel the management and staff about the extent of the problem and expected next steps.

If a firm cannot - or does not believe it can - recover its business operations by the next day, it's considered a significant business disruption. Under these conditions, the Plan will be invoked.

However, there are disruption incidents when a firm will invoke its BCP, *but not need to failover its production systems to a backup data center* (e.g., the building/ or immediate area is in inaccessible for the remainder of the day, but production systems are intact, a transit strike or snow storm).

These may not be considered "significant", however, they should be written up and the recap stored in a BCP folder for future reference. The recap should include the cause, effect, response, elapsed time to full restoration of services, action items, lessons learned etc.

This definition is agnostic as to the cause, not the effect…

2. Scope and Applicability:

From our extensive experience and in our professional opinion, we believe that *"one size does not fit all"* in the business continuity space.

We have seen different levels of detail and structure in firms' BCPs, processes and procedures, depending on the maturity of the entity:

- Some investment management firms have their own dedicated data centers that house their technology and infrastructure
- Others utilize co-location hosting sites and manage them remotely
- Some newer entities are almost entirely cloud based and do not want to own any technology

In the request for comments, the Commission references several large investment management firms, numerous times (Blackrock, Fidelity, BNY Mellon, Wellington). These entities are in the top 10 investment managers by assets under management. These firms have large IT and dedicated business continuity management staffs and mature business continuity plans and tools.

Within the top 100 investment management firms, the next 90 investment managers have between $1 trillion and $100 billion AUM. Most of these entities also have mature BCPs and dedicated staffs for BCM.

Since these entities are most likely categorized as "*systemically important*", they would have BCPs and *should have* transition plans.

We believe that those entities are untypical of the 11,000+ investment management firms that fall under the Adviser Act and the Commission's regulatory umbrella. As such, they should be subject to more prescriptive rules in this area.

Additionally, the Commission makes numerous references to Regulation SCI, which is not targeted at investment management firms. This is not immediately relevant to the proposed rulemaking.

We believe that all investment management firms with over $100 million in AUM should be required to have a written BCP in place that adheres to industry sound practices.

3. Business Continuity Resilience:

Most of our investment management clients typically have two or more key service providers in selected functions for resiliency purposes (e.g., order management, trading, prime brokerage, market data services).

Given the availability of robust, internet services, these application service providers are easily accessible for numerous mission critical functions (i.e., from the office, from remote worksite locations, home offices etc.).

Investment management firms typically have contracted with these entities to add resiliency to their critical operations and services, in case a service provider experiences a disruption or changes their business or revenue model (i.e., pricing structure, change of ownership, bankruptcy).

Investment management firms have made their infrastructures as bullet proof as possible, and test it regularly to detect any potential single points of failure.

However, if a certain service provider were to experience a significant business disruption or bankruptcy situation, they would present a stressful situation to numerous (i.e., common) market participants.

Significant disruptions to service providers utilized by a large percentage of the industry - major fund administrators, data center hosting site providers or a service provider like Bloomberg, LP - would have a wide-scale, debilitating impact on firms' abilities to trade, move funds, price portfolios, process subscriptions, redemptions etc.

A fund administrator is one of the few service providers for which most investment management firms do not have an alternate arrangement. They are therefore a potential single point of failure. There is a many to one to many relationship between investment management firms and fund administrators. Additionally, there is a large concentration of AUM with the top 5 fund administrators.

In this regard, many firms have deployed portfolio management and portfolio accounting systems that perform shadow processing of key data (and other functions), should there be a problem with the fund administrator or its systems.

While many of the large firms can afford or have implemented this approach, the majority of the smaller firms (<$100 million AUM), most likely have not implemented these, chiefly because of the complexity and costs involved.

We would counsel the Commission to seek more objective feedback from senior technologists who have built and implemented large complex systems and infrastructure. These individuals should have experience with the vagaries and nuances of their operations and businesses, as well as how to best handle disruptions "on the fly".

With all this said, the best BCP strategies, written procedures and policies, robust capacity planning and state of the art technologies are *not designed for multiple events all going wrong at the same time (e.g., Hurricane Sandy scenario)*.

4. Transition Plans:

Most investment management firms we know have succession plans built into their general partnership agreements.

As the Commission has positioned it, a Transition Plan ("TP") should address how a firm would potentially:

- Transition its client segregated assets to another fund administrator
- Transition its client accounts to another firm
- Wind down its operations due to the death or incapacitation of a general partner, or the loss of a key man within the firm

We firmly believe that investment management firms should develop and maintain TPs *separate* from their BCPs, but cross reference them in the BCP.

Transition plans should identify the steps that the firm will take to minimize or mitigate risks, should the need for a transition or wind down be required. Personnel considerations should be identified, but should be flexible to respond to unknowns.

BCPs are operational documents, to be utilized by key managers (senior management and the IMT and staff in the minutes, hours and days following a significant business disruption.

The BCP is intended to be an operational risk management tool that the firm would use in response to a significant business disruption, to address the response, recovery and restoration of operations and services.

The intended audience for the TP should be the senior management team of the firm (general partner(s), chief operating officer, general counsel, outside counsel etc.).

The TP has a limited audience - those on a "need to know" basis, not the overall staff. Additionally, there are contractual. legal and regulatory compliance implications of enacting the TP.

The senior management team are the individuals who will be alerted to the situation that creates the need for an eventual transition, and are the logical individuals that will discuss the situation, the ramifications on the firm and a plan of attack for the eventual transition/wind down.

By comparison, a BCP has multiple audiences (staff, department managers, incident managers, outside service providers etc.), and will be invoked at the outset of an SBD that threatens the day-to-day operations of the firm.

The goal of the BCP should be the restoration of service and continuance of business operations following the disruption, and the resumption of as close to normal a business operation as possible.

The TP, by its nature, is intended to transition or wind down the operations of the firm. There is more "finality" to the business with a TP than a BCP.

A well-crafted BCP should reference the existence of transition plan and vice versa. The TP should illustrate who owns it and who is responsible for regularly reviewing and updating it.

The TP should be revisited when the BCP is updated, as an integral part of the regular Plan update process.

5. BCP Disclosures:

Since all BCPs contain sensitive, need-to-know information, confidential and proprietary information (staff contacts, key counterparty contacts, technology diagrams, network diagrams, IP addresses, etc.), parts or all the plan components must be treated as "*company confidential*".

As such, the Plan should be considered intellectual property of the firm and guarded as such.

However, most investment management firms have developed a summary of their BCP which is made available to potential and existing investors.

The BCP Summary should describe the firm's business continuity and disaster resilience strategy, at a high level, and what the investor should expect if the firm experiences a significant business disruption. It should not contain any sensitive or proprietary information about the firm or its operations.

The BCP summary should be revisited when the overall BCP is updated (i.e., no less than annually or when there is a significant change to the firm's business or operations).

Similarly, for the reasons stated above, we believe that investment management firms should not be required to submit complete copies of their BCPs to the Commission.

The Plan should be made available onsite at the firm's offices upon request by the Commission staff, when an audit or onsite inspection of the firm's books and records is scheduled.

6. Information Security:

Information security (InfoSec") 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.

We believe that as part of the proposed regulations, investment management firms should be required to demonstrate 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, staff BCP and cybersecurity education, and policies and procedures to identify, isolate and mitigate the effects of InfoSec breaches.

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 the entities' mission critical systems (e.g., order management, risk management, portfolio management, clearance/settlement), as well as any web portals, internal shared drives and systems that support the management and administration of their business (e.g., finance, operations, administration, legal/compliance, etc.)

We believe that imposing rigid cybersecurity frameworks such as NIST will be too onerous and grossly inefficient for smaller investment management firms (<$100 million AUM). There is no one size fits all approach here.

7. Vendor Due Diligence:

Investment management firms typically contract with multiple key service providers for key mission critical systems and service. These include fund administrators, market data providers, data center hosting sites, ASPs for order management, portfolio management, risk management, fund accounting, etc.

In the last 2 years, we have seen these entities conduct enhanced due diligence reviews of these key players. Some of this has been at the request of their investors/prospective investors, and some has been for regulatory compliance purposes.

Investment management firms have developed due diligence questionnaires ("DDQs") and have sent them to their service providers for response. Some of these DDQs have very invasive questions, some are more practical in structure.

Many firms have between 4 and 20 key service providers, so developing a comprehensive DDQ can be challenging. Determining which subset of them is considered "key" is another process.

From our observations, the content in the response to DDQs is only as good as the quality and granularity that the service providers respond with.

Key to this process is the turnaround time from when the DDQ is sent to a service provider and when they respond, and the quality and comprehensiveness of the response.

Since many of these service providers are large entities, finding the right person or group to send it to can be challenging, let alone chasing them for a satisfactory response within a reasonable time frame. Quite probably, that person or group has received multiple DDQs from multiple entities.

Depending how the questions are structured (i.e., objectively or subjectively), and the quality and degree of details in the vendors response, the answers to the DDQ may be inconsistent or vague.

In spite of numerous follows up or prodding from the firm, the vendor may just say "that's the extent of our answer..."

It is conceivable that some DDQ questions could be answered as "Yes", "No", "Not applicable" or "Do Not Know". In these cases, the investment management firm will need to push back and attempt to obtain more granular details. However, there is no guaranty that the vendor will reply with a satisfactory answer all the time.

Vendor due diligence should conducted on a “best efforts” basis by the investment management firm or by contractors on its behalf. The reviews should expect to be conducted within practical limitations.

A major issue is the maintenance and updating of vendor DDQ response content. The next time that the firm sends it to the service provider for an update, they may have to repeat the entire process described above, especially if the person or group who responded the first time has moved on.

It is unreasonable to expect that smaller investment management firms (<$100 million AUM) will have the resources, skills and time to create an effective DDQ, launch it and chase their key service providers for a satisfactory response. The Commissions estimates of time and costs to conduct these is grossly inaccurate.

8. BCP Maintenance, Records Retention:

From our experience and knowledge of industry sound practices for BCM, most investment management firms review and update their BCPs no less than annually.

At that time a business impact analysis is conducted with all business units and the entire BCP documentation suite is reviewed and updated.

The process starts with a review of the then current version. When the review and update process is complete, the new plan version is implemented and the new version is stored electronically and distributed/accessed by the relevant staff members and managers.

The previous versions of the plan should be archived and stored in a BCP folder for any future reference.

In addition, the firm should also maintain other business continuity related documents in its BCP folder, including but not limited to:

- Soft copies of the plan and all older versions
- Attendance sign in sheets illustrating staff members participation in any business continuity training or briefing sessions
- Documentation of test plans and test results
- Independent test oversight attestation
- Details on any disruptions, including cause/effect, lessons learned, action plan, post-mortem results

Conclusions, Going Forward:

In our professional opinion, most large investment management firms (by AUM) have the technology and network infrastructure and procedures in place to address the spirit of what the Commission is seeking. We feel strongly that:

1. The Commission should consider that anything that prevents an investment management firm from opening for business by the next business day is an acceptable definition of significant business disruption
2. There is no one size fits all when it comes to business continuity management, information security and transition planning
3. The top 10 investment management firms by assets under management should be subject to a transition plan, as should the top 5 fund administrators
4. Transition plans should exist outside of a BCP, but should cross reference the existence of each other
5. Investment management firms should be required to have written, comprehensive BCPs in place, commensurate with their business and operations size, maturity and structure
6. BCP summary disclosures should be provided to clients at account opening or as part of the client due diligence process, and updated as part of the regular BCP update process
7. Investment management firms' BCPs typically contain confidential and proprietary information and should be considered so and guarded as company confidential
8. Firms should be able to provide access to their full BCP to the Commission, when requested and on site at the firm's offices
9. BCPs and TPs should be reviewed and updated no less than annually, or when there is a significant change to the firm's business or operations, whichever occurs first
10. Firms should maintain the existing and prior versions of their BCPs electronically, and make them available to the Commission upon request, on site
11. Vendor due diligence reviews and vendor questionnaire surveys should be conducted on a best efforts basis and should be revisited on an annual basis by the firm.

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

As 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.

If rushed to implement, a broad based approach to these new rules 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.

In today's markets, we need smart regulation, not more regulatory crush…

Our best counsel to the Commission is to analyze the feedback from the comment period, and assess the time frames that investment management firms indicate that they can adopt the new standards within.

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.