sifma
Invested in America

April 26, 2019

Jennifer Piorko Mitchell
Office of the Corporate Secretary
FINRA
1735 K Street, NW
Washington, DC 20006-1506
pubcom@finra.org

Re: Regulatory Notice 19-06 - Retrospective Review of Rule 4370 Regarding Business Continuity Plans and Emergency Contact Information

Dear Ms. Mitchell:

On behalf of the Securities Industry and Financial Markets Association ("SIFMA"),[1] we appreciate the opportunity to comment on FINRA's retrospective review of Rule 4370 (Business Continuity Plans and Emergency Contact Information), FINRA's emergency preparedness rule, to assess its effectiveness and efficiency.[2]

Generally, SIFMA believes the Rule was well written and has had its intended effect, as it is efficient and effective at ensuring member firm preparedness for a wide range of potential business disruptions. SIFMA is strongly supportive of the flexibility the Rule offers members, summarized in section (a) "*Each member must create and maintain a written business continuity plan …. must be reasonably designed to enable the member to meet its existing obligations to customers*…." The Rule's flexibility allows members to maintain and evolve a resiliency program to restore operations so that the member may fulfill obligations to their investors and counterparties. This requires financial institutions to consider recovery of facilities and impacts on personnel, processes, technologies and third-parties – taking into consideration the member's risk profile and tolerance, size and operating model.

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate on legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

[2] http://www.finra.org/industry/notices/19-06

Notwithstanding SIFMA's general support for the Rule as written, and discussed fully below in response to question two, SIFMA believes that FINRA should consider amending the section of the Rule related to customer disclosures in account opening documents to permit firms to follow more flexible – yet effective – disclosure practices. Specifically, FINRA should consider amending the Rule 4370(e) to permit firms in account opening documents to provide: (a) a short description of a firms BCP resources; and (b) information that (i) directs the customer to the firm's BCP resources on the firm's website, and (ii) informs the customer of his or her ability to request the firm mail a copy of its Business Continuity Plan disclosures. In the alternative, SIFMA requests that FINRA clarify that required "written" BCP disclosures at account opening outlined in Rule 4370(e) may include disclosures provided in digital formats.

Please find below SIFMA's comments in response to the questions FINRA posed as part of its Retrospective Rule Review. We would be happy to provide further clarification or answer any questions regarding our comments.

* * *

1. **Has the rule effectively addressed the problem(s) it was intended to mitigate? To what extent has the original purposes of and need for the rule been affected by subsequent changes to the risk environment, the markets, the delivery of financial services, the applicable regulatory framework or other considerations? Are there alternative ways to achieve the goals of the rule that FINRA should consider?**

   SIFMA believes the Rule's flexible approach to business continuity planning is effective at ensuring member firm preparation for a wide range of potential scenarios. Because member firms vary significantly in size and business models, they require flexibility and adaptability in developing business continuity plans and resilience strategies, while still incorporating the basic elements outlined in the Rule.

   We acknowledge that the threat environment has changed significantly since the Rule was issued and continues to evolve. Today, members must plan for a variety of risks including increased cyber-security threats, potential power grid disruptions, extreme weather events and geographic and third-party risks. The resiliency programs developed by the industry when the Rule was first introduced were designed to recover from a less complex threat environment and our members continue to evolve their plans and adapt to these new risks.

   The financial services industry also continues to increase in complexity. Members continue to evaluate the resilience of their critical functions, which – if disrupted – could be impactful. Members also continue to include these considerations in their risk assessments and business resiliency strategies and plans.

The increasingly global nature of the evolving threat environment further reinforces the need for firms to continually analyze and address issues around the resiliency of people, processes, technologies, third-parties and critical facilities.

Given the rapid pace of change around technology innovation, threats and regulation that shape the industry's approach to resiliency planning, we suggest that rules and guidance continue to be flexible, non-prescriptive and risk-based to allow firms to implement controls and mitigation strategies that fit well with their unique operating environments, risk tolerance and profile.

2. What has been your experience with implementation of the rule, including any ambiguities in the rule or challenges to comply with it?

SIFMA believes the Rule was well designed and that implementation challenges associated with the Rule were not significant. Looking ahead, business continuity planning in the financial services sector is a mature discipline and continues to evolve with the threat environment, therefore, additional prescriptive guidance to Rule 4370 may not result in significant benefits to the sector.

However, related to the Rule's required customer disclosures, SIFMA believes that the Rule's requirement that a firm provide its business continuity procedures to customers at account opening unnecessarily adds significant volume to the account opening packet. As a general matter, disclosure only aids a customer to the extent a customer is capable of, and willing to review the information that has been disclosed. If the customer is not both, disclosure may cease to be informative, protective or curative. In this context, the provision of detailed business continuity planning information in the account opening documents is more granular than necessary to disclose to customers that the firm is prepared for business continuity events and has resources available for customers should an event occur. Further, information maintained on the firm's website can dynamically react to a business continuity event in progress, and direct customers to relevant resources.

As such, SIFMA believes that the Rule should permit firms to provide a summary of their business continuity planning resources in account opening documents. The summary should provide information that directs the customer to the firm's business continuity planning resources on its website. In addition, the summary should inform the customer of his or her ability to request the firm mail a copy of its full Business Continuity Plan (BCP) disclosures. Proposed text changes to Rule 4370(e) are outlined below.

The current text of Rule 4370(e) reads as follows:

(e) Each member must disclose to its customers how its business continuity plan addresses the possibility of a future significant business disruption and how the member plans to respond to events of varying scope. At a minimum, such disclosure must be made in writing to customers at account opening, posted on the member's Web site (if the member maintains a Web site), and mailed to customers upon request.

To provide flexibility for members to comply with the disclosure requirements, SIFMA proposes that FINRA make the following changes to Rule 4370(e):

(e) Each member must disclose to its customers how its business continuity plan addresses the possibility of a future significant business disruption and how the member plans to respond to events of varying scope. At a minimum, such disclosure must ~~be~~ **include a summary of the firm's business continuity plan** ~~made in writing~~ **provided** to customers at account opening~~,~~ **that directs the customer to business continuity plan information** posted on the member's Web site ~~(if the member maintains a Web site)~~, and **inform** ~~mailed to~~ customers **of the firm's willingness to furnish full business continuity plan disclosure information to the customer via mail** upon request.

SIFMA believes that the proposed language accomplishes the goal of customer disclosure regarding a firm's business continuity plans while providing the firm the ability to organize and present disclosures applicable to the customer in a manner best designed to ensure customer understanding of such disclosures. Further, directing customers to the firm's business continuity planning resources on its website is a more effective means of providing current, comprehensive and dynamic information to the customer regarding business continuity planning.

Should FINRA not pursue the above requested changes to the Rule related to disclosures, SIFMA asks that FINRA clarify that required "written" business continuity plan disclosures at account opening may include disclosures provided in digital formats. The physical delivery of printed business continuity plan disclosures is not optimum for many customers, including those who largely interact with member firms though the internet. Separately, the inefficiency and environmental impact associated with providing customers printed business continuity plan information at account opening is substantial without a meaningful benefit over providing such disclosures in a digital format, where appropriate. Of course, consistent with the Rule, members will mail the firm's business continuity plan disclosures to the customer upon request.

3. **What have been the economic impacts, including costs and benefits, of creating, maintaining or updating a business continuity plan? To what extent do the costs and benefits have a disproportionate impact on firms based on size and business model? Has the rule led to any negative unintended consequences?**

The financial services sector continues to improve its business continuity posture. Independent of the Rule, the costs to meet a changing risk environment have grown significantly due to the addition of new sites, communication lines, testing, equipment, etc. In addition, some members are required to maintain robust business continuity programs to meet other global regulatory requirements that also satisfy FINRA requirements.

Coupled with recent large-scale business continuity events discussed below, the Rule is part of an overall landscape that requires firms to have robust business continuity plans and continual testing programs.

In summary, the Rule's principles-based approach has been a benefit to the financial sector, providing firms with the flexibility to meet an ever-changing threat and risk environment. New rigid or amended rules, regulations and guidance could be cost prohibitive for small firms and impact their competitive position without further improving their risk profile. A one-size-fits-all prescriptive approach would be a challenge for the industry, and often has unintended consequences, especially in contrast with the success to date of risk-based approaches. As such, SIFMA supports the flexible approach of the Rule, which permits members to tailor business continuity plans to their unique business, technical, and operational models.

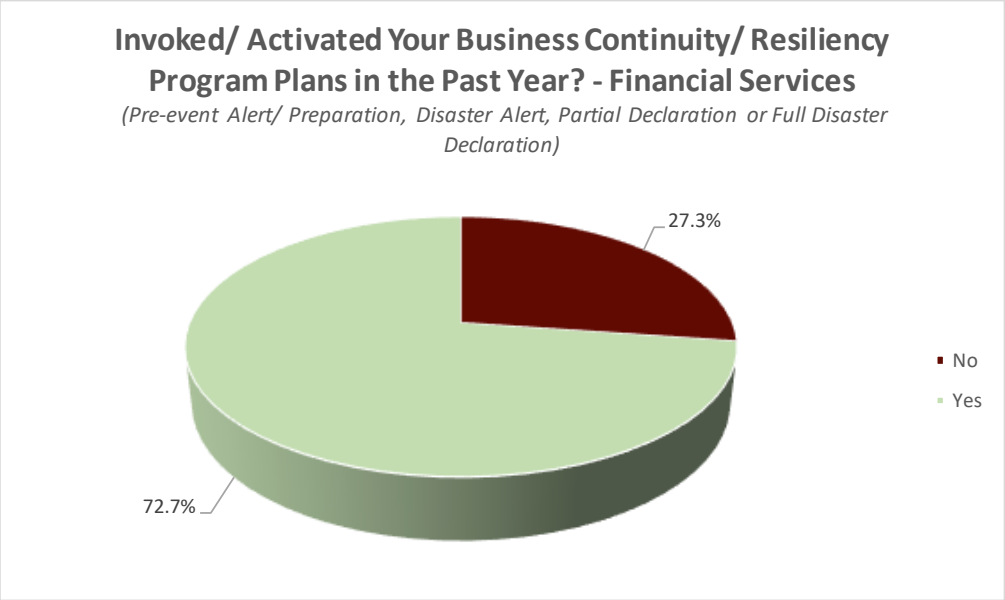
4. Can FINRA make the rule, guidance or attendant administrative processes more efficient and effective?

SIFMA believes the Rule is well written and that related guidance and administrative processes are efficient and effective. Importantly, SIFMA supports the Rule's flexibility which allows members to build and implement appropriate business continuity plans and solutions.

5. Have you ever needed to activate your BCP and if so, was it effective? Please describe the circumstances that led to the activation of your BCP

A recent study by Firestorm Inc. covering over 70 financial firms (e.g., banks, brokerages, asset managers, credit cards et al) from 14 countries showed that over 70% of those firms experienced significant events requiring activation of their business continuity plans during 2018 (see Exhibit A below). The study also shows 30% of firms either did not experience a significant event and/or had sufficient resiliency built into their recovery programs. One global firm did report that over the course of a year they successfully recovered from more than 70 significant events with minimal or no impact.

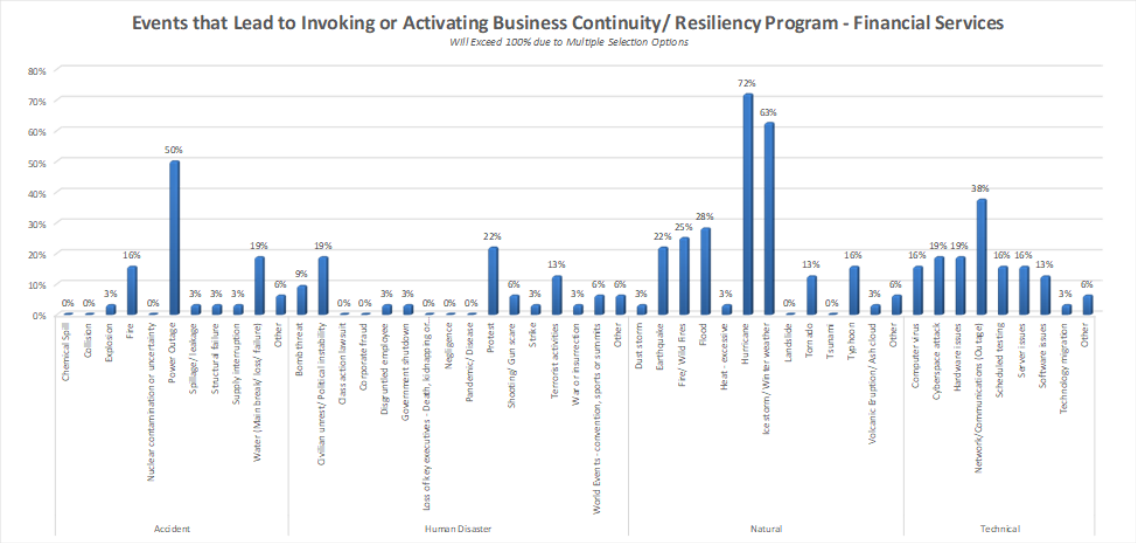
Exhibit A: Percent of firms activating business continuity plans in 2018



Source: Firestorm Inc.

Exhibit B below illustrates the broad range of incidents which led to the activation of business continuity plans – with the most common drivers of activation covering a broad spectrum of risks, ranging from infrastructure issues such as power outages to extreme weather such as hurricanes and ice storms, to civil and public safety issues such as protests and terrorism to technology failures.

Exhibit B: Types of events financial firms experienced in 2018



Source: Firestorm Inc.

6. **How do you determine what may constitute a significant business disruption? To what extent do you address specific types of significant business disruptions in your BCP (e.g., cyber events, terrorist attacks, pandemics or natural disasters)?**

   A significant business disruption is any disruption which prevents a firm or their customers from performing critical business services and/or the inability to recover essential functions within their stated Recovery Time Objectives (RTO).

   Financial services members, in the course of conducting regular business continuity and disaster recovery tests, and dealing with actual incidents, will exercise a number of scenarios (e.g., cyber, natural disasters, IT outages, terrorist attacks, extreme weather), based on their firm's risk profile, to ensure the firm can respond and recover timely from various business disruptions. As a normal course of operations, business continuity teams focus on continuous improvement, enhancing playbooks and building strategic relationships with partners in the public and private sector that can assist firms in recovering from potential disruptions.

7. **What other rules, if any, conflict with or get in the way of business continuity planning?**

   Various regulatory bodies have issued potentially conflicting or unaligned business continuity rules/guidance resulting in a major source of inefficiency as firms must take time to analyze and harmonize different rule sets and map them to their internal controls. In addition, global firms may be subject to multiple examinations related to business continuity and closely related topics from different regulatory bodies, sometime covering the same issues or controls. As a result, business continuity teams spend a significant amount of time on duplicative, overlapping or sometimes conflicting examinations and meetings.

   The industry encourages regulators to harmonize their rule sets and also engage in mutual recognition of other regulatory examination results. This would create greater efficiencies within financial firms as well as the regulatory bodies that provide oversight.

8. **To what degree does your business or BCP rely on vendors or other external providers? Would the rule be more effective if it addressed expectations around additional diligence into vendor resiliency?**

   While businesses do rely on third-parties, the Rule would not be more effective if it addressed vendor resiliency as there are existing guidelines that adequately address third-party risk management. In addition, financial firms today have robust third-party risk management processes, procedures and organizational constructs that cover the entire vendor life-cycle (e.g., due diligence, SLAs and contracts, on boarding, monitoring, off boarding et al). On-going participation in industry-wide and individual disaster recovery tests with

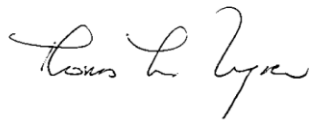
service providers presents an opportunity to validate firms can meet established recovery times and strengthen client and third-party relationships.

* * *

We welcome further engagement and discussion with FINRA concerning the comments provided in this letter. We also look forward to working with FINRA in the creation of business continuity programs and plans that complement existing requirements to ensure effective management of existing and emerging risks.

If you have any questions or require further information, please do not hesitate to contact Tom Wagner at 212-313-1161 or twagner@sifma.org.

Sincerely,



Thomas M. Wagner
Managing Director
SIFMA