NATIONAL EXAM PROGRAM
RISK ALERT

By the Office of Compliance Inspections and Examinations[1]

Volume II, Issue 3 August 27, 2013

In this Alert:

Topic: *Staff observations after a review of certain advisers' business continuity plans following Hurricane Sandy.*

Key Takeaways: *Advisers should review their continuity plans in light of the staff's observations and consider revising their plans if they see ways to make them better.*

SEC Examinations of Business Continuity Plans of Certain Advisers Following Operational Disruptions Caused by Weather-Related Events Last Year

Hurricane Sandy caused significant and wide-ranging damage across the northeast coast of the United States on October 28 and October 29, 2012, which led to the closure of the equities and options markets on October 29 and October 30, 2012. The storm prompted the SEC's National Examination Program ("NEP") to review the business continuity and disaster recovery plans ("BCPs") of approximately 40 advisers in the impacted areas to assess their compliance with applicable laws, rules, and regulations relating to BCP plans.

The NEP contacted advisers in the geographic region affected by Hurricane Sandy to gain an understanding of how the advisers were impacted by the events surrounding the storm; specific emphasis was given to firms' implementation of their BCPs. The NEP discussed with these advisers the range and impact of anticipated disasters and contingencies given the firm's location and circumstances, and the impact of Hurricane Sandy on processing of securities transactions (order taking, entry, execution, allocation, clearance and settlement) and delivery of funds and securities, client relations, financial and regulatory obligations, and technology, among other topics.

This Alert contains the NEP staff's observations and lessons learned from the BCP review. The NEP encourages firms to review their BCPs and consider implementing these lessons as appropriate to help improve responses to, and to reduce recovery time after, significant large scale events.[2]

---

[1] The views expressed herein are those of the staff of the Office of Compliance Inspections and Examinations, in coordination with other SEC staff, including in the Division of Enforcement's Asset Management Unit and the Division of Investment Management. The Commission has expressed no view on its contents. This document was prepared by the SEC staff and is not legal advice.

[2] In addition to the effective practices noted herein, advisers should also consider the best practices and lessons learned as described in the Joint Review of Business Continuity and Disaster Recovery of Firms by the Commission's National Examination Program, the Commodity Futures Trading Commission's Division of Swap Dealers and Intermediary Oversight and the Financial Industry Regulatory Authority on August 16, 2013, available at http://www.sec.gov/about/offices/ocie/jointobservations-bcps08072013.pdf ("Joint Review on BCP").

I. RELEVANT SECURITIES LAWS, RULES, and REGULATIONS

Rule 206(4)-7 under the Advisers Act requires each investment adviser to adopt and implement written policies and procedures reasonably designed to prevent the adviser from violating the Advisers Act.[3] These policies and procedures should include BCPs because an adviser's fiduciary obligation to its clients includes taking steps to protect the clients' interests from risks resulting from the adviser's inability to provide advisory services after, for example, a natural disaster.[4] Under Advisers Act Rule 204-2, advisers have responsibilities to maintain books and records including a requirement to maintain electronic storage media "so as to reasonably safeguard them from loss, alteration, or destruction."[5]

II. STAFF OBSERVATIONS

The NEP staff describes below its observations from the BCP review, including the general BCP policies and practices of the advisers it examined. Observations also include notable practices of advisers that were able to perform critical business operations and maintain more consistent communications with clients and employees while operating under their BCPs, as well as BCP weaknesses of advisers that experienced more interruptions in their key business operations and inconsistently maintained communications with clients and employees. The staff also identifies areas that advisers may consider when reviewing their BCPs.

A. Widespread Disruption Considerations

1. General Observations and Notable Practices

- Advisers generally adopted and maintained written BCPs. The degree of specificity of the advisers' written BCPs varied; some had also developed specific BCPs for Hurricane Sandy just prior to the storm's arrival.

- Advisers also generally distributed their BCPs widely within their businesses and operations. In some cases, employees were required to sign that they have received the plan annually, along with the compliance manual and code of ethics.

---

[3] 17 CFR 275.206(4)-7, available at http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=f213a4d9b959087f82822dac376045ee&rgn=div5&view=text&node=17:3.0.1.1.19&idno=17#17:3.0.1.1.19.0.142.40.

[4] See *Final Rule: Compliance Programs of Investment Companies and Investment Advisers*, Advisers Act Release No. 2204 (December 17, 2003) ("Final Rule Release"), available on the SEC's website at http://www.sec.gov/rules/final/ia-2204.htm. In this release, the Commission discussed the need for advisers to establish a reasonable process for responding to emergencies, contingencies, and disasters, and that an adviser's contingency planning process should be appropriately scaled, and reasonable in light of the facts and circumstances surrounding the adviser's business operations and the commitments it has made to its clients.

[5] See Advisers Act Rule 204-2(g), available at http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=56d142fae2fd474bf00f574de20aa3c6&n=17y3.0.1.1.19&r=PART&ty=HTML#17:3.0.1.1.19.0.144.22 .

- Some advisers' BCPs addressed critical systems of the adviser and were tailored to fit the adviser's business operations.

- Some advisers' BCPs considered continued facility and systems operations with wide-spread remote access by employees.

- Some advisers' compliance personnel worked collaboratively with the advisers' various business lines to develop the BCPs and sought to achieve redundancy in key services and operations.

- Some advisers required all business units to identify contingency scenarios that would affect operations and derive multiple solutions to help ensure the advisers could meet their fiduciary duty to clients.

- Some advisers formed special committees to plan, develop, test and, if necessary, execute the advisers' BCP. The staff observed that these committees were typically comprised of business unit staff and senior management.

2. Weakness Noted

- Some advisers adopted BCPs that did not adequately address and anticipate widespread events. These advisers generally experienced more interruptions in their key business operations and inconsistent communications with clients and employees. For example, some advisers did not have adequate plans addressing situations where key personnel, such as portfolio managers, were unable to work from home or other remote locations.

3. Possible Future Considerations

- Advisers should enhance the design and implementation of their BCPs by developing policies and procedures to address and anticipate widespread events, including possible interruptions in key business operations and loss of key personnel for extended periods.

B. Alternative Locations Considerations

1. General Observations and Notable Practices

- Advisers generally switched to back-up sites or systems, if needed, in advance of trouble rather than waiting for shutdown or imminent threat. Some advisers reported that the buildings where they usually conduct their business were closed for days. One reported its building was closed for several weeks. Some reported extended outages of power, phone systems, and internet service.

- Some advisers had back-up facilities on a power grid separate from the adviser's primary facility.

- Some advisers maintained critical business functions in more than one location in order to reduce potential disruption of operations by regional events. For example, an adviser established a remote, back-up location with an unaffiliated adviser. More often, however, the advisers used employees' homes, branch offices, data centers or hotels as alternate locations. Additionally, advisers had back-up generators at homes to ensure connectivity.

2. Weakness Noted

- Some advisers did not have geographically diverse office locations, even when they recognized that diversification would be appropriate. Many smaller advisers had fewer geographically dispersed staff.

3. Possible Future Considerations

- Advisers should evaluate how to operate when faced with the possibility of electrical failure and the loss of other utility services (e.g., cable, phone). Establishing a back-up site inland may reduce risk if the adviser's business is located on a coast. In addition, advisers may want to consider other sites farther away from the adviser's main office – sites that are not affected by the same power and utility outages as the main office. Loss of internet connectivity was an issue for many of the advisers reviewed.

C. Vendor Relationship Considerations

1. Notable Practices

- Some advisers required third party service providers to test their BCP annually and report results to the adviser.

2. Weakness Noted

- Some advisers did not evaluate the BCPs of their service providers. For example, some advisers did not acquire or critically review service providers' Statement on Standards for Attestation Engagements No. 16 reports ("SSAE 16 reports")[6] and BCPs. In doing so, the advisers did not ensure that the service providers' plans incorporated key business

[6] Information regarding SSAE 16 reports is available on the American Institute of CPA ("AICPA") website at http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx. This website describes Service Organization Control ("SOC") reports for service providers as reports prepared by independent Certified Public Accountants using the SSAE 16 professional standards. These reports are "intended to meet the needs of the entities that use service organizations (user entities)… in evaluating the effect of the controls at the service organization on the user entities' financial statements."

continuity controls that related to the advisers' ability to execute their own BCPs. In some cases, advisers reported that they did not keep an updated list of vendors and respective contacts at each entity.

3. Possible Future Considerations

- Advisers should consider reviewing the IT infrastructure of service providers – as their infrastructure may be in the same geographic area in which the adviser is located. Advisers may wish to consider whether, based on risk, it is necessary to have multiple back-up servers.

- Advisers should evaluate how to operate when the adviser or a service provider's facilities are faced with the risk of weather-related events, including flooding. Disrupted operations at service providers can create unforeseen operational challenges.

D. Telecommunications Services and Technology Considerations

1. General Observations and Notable Practices

- Advisers had generally implemented technology to allow employees to work from remote sites, which typically included from home. Some utilized offsite technology, such as Citrix and VPN, to accomplish this and others utilized internet-based access portals. Some advisers established and tested direct point-to-point network lines between their main offices and multiple back-up office sites.

- Some advisers maintained current portfolio data at multiple service providers and had tested the connectivity to the providers to ensure that the data was accessible from remote locations.

- Some advisers arranged to have key power systems tied to advisers' generators so electricity and air conditioning would be available for the entire building (especially important in a multi-tenant building with no electricity back-up).

- Some advisers adequately maintained system capacity (physical and electronic) to accommodate staff who may be displaced and may need to work from home or an alternative location.

- Some advisers established and tested server internet connection via wireless cards for use if the primary connection was lost.

- Some advisers' electronic equipment kept in ground level facilities was elevated to mitigate risk of damage in the event of flooding.

- Some advisers maintained uninterrupted battery power supply that kept power for essential operations running until the back-up generator turned on during power outages.

2. Weakness Noted

- Some advisers did not engage service providers to ensure that back-up servers functioned properly. Rather, the advisers relied solely on self-maintenance, which led to more interruptions in their key business operations.

3. Possible Future Considerations

- Advisers should consider having alternate internet providers available or obtain guaranteed redundancy from internet providers. If key suppliers are not diversifying their data/telecommunication connectivity, such lack of diversification is a risk in its own right.

- Advisers are encouraged to explore the appropriateness of keeping back-up files and systems in the adviser's primary office location. Many advisers stated that they are now exploring the use of cloud computing.

E. Communications Plans Considerations

1. General Observations and Notable Practices

- Advisers generally communicated with employees before, during, and after the storm regarding such things as the status of the adviser's business, operations, and back-up locations. One firm reserved local hotel rooms for essential employees in anticipation of the storm.

- Some advisers regularly communicated the status of their operations with their clients. For example:

    - Main telephone line provided a recorded message stating that offices were closed and provided clients with instructions for contacting the firm and employees who were working remotely.
    - Websites provided information regarding the firm's status.
    - Third party vendors were used to send emails in connection with the storms to clients.
    - Answering services provided updates to clients.

2. Weakness Noted

- Some advisers did not adequately plan how to contact and deploy employees during a crisis, and inconsistently maintained communications with clients and employees. Some advisers had an overall plan, but it did not identify which personnel should execute and implement the various parts of the plan.

3. Possible Future Considerations

- Advisers should consider contacting clients (directly and/or via an e-mail blast) before a major storm to see if they have any transactions (cash raised, funds transferred, wire instructions executed, etc.) they will need executed if an extended outage occurs.

F. Regulatory and Compliance Considerations

- As noted in the Joint Review on BCPs for broker-dealers, advisers should regularly update their BCPs to include new regulatory requirements. In addition, advisers should consider time-sensitive regulatory requirements, since a crisis event can occur at any time.

G. Review and Testing Considerations

1. General Observation and Notable Practices

- Advisers generally conducted tests of their BCPs prior to the storms. These tests were conducted at least annually, and some advisers specifically tested their BCPs in preparation for the storm.

- Some advisers developed comprehensive plans that had been tested periodically, typically annually.

- Some advisers tested generators frequently, such as weekly, to validate that they were working properly.

2. Weaknesses Noted

- Some advisers inadequately tested their BCPs relative to their advisory businesses, such as applying limited scenario-testing assumptions or not testing all critical business operations and systems.

- Some advisers opted not to conduct certain critical tests because vendors provided disincentives or charged for testing. For example, some advisers opted not to test their cloud-based disaster recovery solution because of the extra charge for this service. Consequently, these advisers did not secure contracts to provide back-up generators and did not know that there was insufficient capacity to handle all of their customers.

3. Possible Future Considerations

- Advisers should consider testing the operability of all critical systems under the BCP using various scenarios. Such testing may minimize disruptions to operations because critical weaknesses may be identified and resolved and personnel may become more fluent with using key systems while in the BCP mode.

III. CONCLUSION

The NEP staff's review of certain advisers' BCPs following Hurricane Sandy provided insight into the ways that advisers affected by weather-related events had implemented their plans and how effective they were in a live scenario. The Commission has previously discussed the need for advisers to have BCPs in place,[7] and the NEP encourages advisers to review their plans and consider their effectiveness in light of the observations and information in this Alert.

The staff also welcomes comments and suggestions about how the Commission's examination program can better fulfill its mission to promote compliance, prevent fraud, monitor risk, and inform SEC policy. If you suspect or observe activity that may violate the federal securities laws or otherwise operates to harm investors, please notify us at http://www.sec.gov/complaint/info_tipscomplaint.shtml.

This Risk Alert is intended to highlight for firms risks and issues that the staff has identified in the course of examinations regarding the business continuity plans of certain investment advisers following operational disruptions caused by weather-related events in 2012. In addition, this Risk Alert describes factors that firms may consider to (i) assess their supervisory, compliance and/or other risk management systems related to these risks and issues, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. These factors are not exhaustive, nor will they constitute a safe harbor. Other factors besides those described in this Risk Alert may be appropriate to consider, and some of the factors may not be applicable to a particular firm's business. While some of the factors discussed in this Risk Alert may reflect existing regulatory requirements, they are not intended to alter such requirements. Moreover, future changes in laws or regulations may supersede some of the factors or issues raised here. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

[7] *See* note 4, *supra*.