Onboard Financial Management, LLC

Business Continuity Plan

Effective Date: August 27, 2020

CONFIDENTIAL – NOT TO BE DISTRIBUTED OUTSIDE THE FIRM

Using this BCP

Each Supervised Person of Onboard Financial Management, LLC must read and understand the Business Continuity Plan and comply with all of the policies and procedures herein.

Table of Contents

1. Overview

This Business Continuity Plan (herein the "BCP") for Onboard Financial Management, LLC ("Onboard" or the "Advisor") provides guidance to the Advisor, and its owners, employees, independent contractors and other insiders of the Advisor (herein collectively "Supervised Persons") in the event of a business interruption or loss of key personnel.

In connection with its fiduciary duty to its clients ("Clients"), securities regulators expect the Advisor to take reasonable steps to ensure continued operations in the event of a business interruption.

The goal of the BCP is to provide a framework to guide the continuation of business operations of the Advisor in the event of a Significant Business Disruption ("SBD") as defined herein.

The BCP shall take into consideration the length of the interruption and the priority of business activities to ensure that the Advisor's obligations to its Clients are met. It is understood by that minor modifications may be made to activities specified within the BCP as required by the specific emergency encountered at the time the event takes place.

There are numerous SBD scenarios in which the BCP would be implemented, including a loss of access to the Advisor's primary office, loss of Internet, phone outage, systems interruption, vendor outage, power outage, natural disaster, medical reasons, etc. As it is not practical to plan for every potential interruption, the Advisor will make every effort to ensure its ability to continue operations.

Chief Compliance Officer

The Chief Compliance Officer ("CCO") is responsible for the implementation of this BPC and accountable for oversight and supervision. The CCO also serves as the Disaster Recovery Coordinator ("DRC"). The CCO may also be referred to as the DRC throughout this BCP. The CCO shall fully understand the requirements of the BCP and to ensure that the BCP is remained current. The CCO may delegate a portion of the responsibilities to appropriate delegates (each a "Delegate") as long as the CCO remains primarily responsible for the BCP oversight and administration.

Amendments

The CCO will amend, modify, suspend, or terminate any policy or procedure contained in the BCP, as well as add any policy as necessary. The Advisor will endeavor to promptly inform Supervised Persons of any relevant changes and provide each Supervised Person with the respective updated BCP document as soon as practicable.

Receipt and Acknowledgement

The BCP is provided to each Supervised Person upon hire and annually thereafter. The BCP will also be distributed on an ad hoc basis if there are any material amendments. Electronic copies are posted and stored internally in a location that is accessible by all Supervised Persons. All Supervised Persons must review the BCP and sign an acknowledgment that they have read, understood, and will abide by the BCP.

2. Internal and External Communication

In the event of an SBD, communication is critical. Below are standard communication procedures for potentially affected parties. Please note that based on the incident's facts and circumstances, the DRC may alter the below procedures as necessary.

Advisor and Delegates

Depending on the nature of the SBD, the DRC will contact any Delegates, as appropriate, to notify them of the incident and provide next steps (i.e., work from the alternate worksite, come into the office, etc.). Throughout the life cycle of the incident, the DRC will keep Delegates updated. The mode of communication may vary between phone calls, texts, and/or email, depending on the timing and impact of the incident. The Advisor will maintain updated Delegate contact information within their Customer Relationship Management system ("CRM") or other

contact storage location. The Advisor will ensure that all Delegates have access to CRM or different storage location via an internet connection.

Additionally, it recommends that Supervised Persons maintain that a copy of the BCP and relevant appendices are accessible from their personal residences.

Clients

Depending on the nature and expected duration of the SBD, the DRC will determine when and how to communicate with Clients to alert them to the situation and keep them apprised as the situation evolves. The Advisor will maintain updated Client contact information within their Customer Relationship Management system ("CRM") or other contact storage locations. The Advisor will ensure that all Supervised Persons have access to CRM or other storage location via an internet connection.

Critical Vendors

The Advisor relies on critical vendors who operate enterprise-grade systems and maintain appropriate plans in place (i.e., business continuity and cybersecurity) to ensure the integrity and accessibility of the stored data.

Depending on the nature of the SBD, the DRC will contact critical vendors (businesses with which the Advisor has an ongoing commercial relationship in support of operating activities, such as vendors providing the Advisor with critical services), and determine the extent to which the Advisor can continue the business relationship during the SBD. The Advisor will quickly establish alternative arrangements if a critical vendor can no longer provide the needed services when needed because of an SBD to them or the Advisor. The Advisor will maintain updated Critical Vendor contact information within their Customer Relationship Management system ("CRM") or other contact storage location. The Advisor will ensure that all Supervised Persons have access to CRM or other storage location via an internet connection from any location.

Regulators

Depending on the type of business interruption, the DRC will work with the CCO or Delegate to contact regulators if there is the possibility of any regulatory reporting disruption or potential rule violations that could result from the business interruption. The Advisor will maintain updated regulator contact information within their CRM. The Advisor will ensure that all Supervised Persons have access to CRM from their alternate worksite.

3. Critical Business Functions

This section of the BCP discusses business functions segregated by how soon after the incident, they must be functional to provide seamless services to Clients.

Day One Critical Business Functions

Day One critical business functions are defined as activities that must be performed on a daily basis. Included are any processes that will result in financial, reputational, regulatory or operational risk.

1. Trading, Portfolio Management, and Operations
    a. Pre-trade research
    b. Position reconciliation
    c. Trade review and approval
    d. Trade execution
    e. Trade confirm reconciliation
2. Client Service
    a. Client account access
    b. Client contact information
    c. Client account restrictions
3. Systems
    a. Custodian and/or Sub-Adviser platform access
    b. Systems backup (online or portable backup drive[s] with critical information)

Day Ten Critical Business Functions

Day Ten critical business functions are defined as important and necessary functions that must be performed regularly, but if not performed for several days during a business interruption, they will NOT have a significant effect on the organization. Day Ten business functions include those that can be mitigated by applying additional financial and human resources to address the interruption and bring all systems and processes online.

1. Trading and Portfolio Management and Operations
    a. Management and ad hoc reporting
    b. Maintenance of Client files
    c. Accounts Payable (Billing, etc.)
    d. Delivery of disclosure statements to new Clients (48 Hours)
    e. Records retention and filing
    f. Performance calculation and reporting
2. Client Service
    a. Client portfolio review
    b. Management and ad hoc reporting
3. Systems
    a. Regular system maintenance
    b. Vendor inquiries
    c. Hardware/software testing
4. Executive and Compliance
    a. Regulatory filings
    b. E-mail monitoring
    c. Marketing material creation/review
    d. Certain compliance functions

Nonrecurring Critical Business Functions

Nonrecurring critical business functions are defined as critical activities that do not occur on a consistent basis but may be treated as a Day One critical business functions as necessary.

1. Trading and Portfolio Management and Operations
    a. Trade error correction
    b. Account terminations
2. Client Service
    a. Client change request - financial condition or suitability

4. Alternate Work Sites

In the event that the Advisor's office location[s] are not accessible, Supervised Persons (as applicable) will work from a public location using secure Internet access to connect to the Advisor's technology systems to perform their job responsibilities.

5. Maintenance, Protection, Recovery, and Backup of Key-Systems and Data

The Advisor has implemented the following procedures to ensure the availability of critical data in the event of a business interruption where data must be replicated or restored:

The Advisor primarily utilizes third-party vendors for maintenance of books and records and business activities. Additionally, most third-party vendors leverage cloud-based storage systems. As such, the continuity of the Advisor's services is heavily dependent on cloud-based systems. Cloud-based systems are backed-up periodically by the service provider. These backups generally occur daily. Third-party vendors have their business continuity plans and maintain highly available systems that are accessible from any location where an Internet connection is present.

Phone System

The Advisor utilizes a hosted VOIP phone system (Voice Over Internet Protocol) for its office phones. If there is a business interruption, all inbound calls will automatically forward to mobile devices. Should the expected duration exceed one (1) business day, the DRC shall assess the impact of continued use of alternate methods of communication and determine the best course of action.

Internet and Email

If the Advisor's Internet or email services are not functioning and the expected duration is four (4) hours or less to restoration, the Advisor may opt to utilize telephones as an alternative means of conducting all necessary business activities. Should the expected or actual duration exceed four (4) hours, the DRC may decide to relocate some or all Supervised Persons to the alternate worksite.

6. Restricted Information Log

During an SBD, the Advisor may have to provide sensitive information to those outside of the Advisor. The Advisor will make every reasonable effort to ensure protection and privacy, resulting from this necessary sharing of information. The CCO or Delegate shall make the formal determination as to whether any information is to be shared outside of the Advisor, and what will be the protective measures taken (i.e., password change, confirmation of document destruction, etc.).

Date	Provided To	Details	Protective Measures

7. Key Person Risk and Succession Planning

The continued operations of the Advisor is heavily contingent upon the availability of key personnel ("Key Person[s]"), and business owner has successors in place to take over the business ("Succession Plan"). The primary goal of this BCP is to ensure Client interests are protected. The long-term unavailability or loss of Key Persons and the lack of a Succession Plan is a risk to the Client's experience with the Advisor.

To address this risk, the Advisor has taken the following steps:

- *Security of Accounts*. All Client accounts shall be maintained at a qualified custodian.
- *Suitability*. Clients shall not be invested in any securities that the Client does not understand.
- *Access*. Clients shall, at all times, have access to their accounts.
- *Books and Records*. The Advisor shall maintain organized records of Client information in the Advisor's cloud-based systems.

In addition, the Advisor has engaged a compliance consulting firm, AdvisorAssist, LLC (www.AdvisorAssist.com) to help facilitate ongoing compliance and continuity planning. In the event of the incapacitation or death of Sean McDonough, AdvisorAssist will take action to assist the estate of Sean McDonough with ensuring the continued protection of Client accounts and communication with Clients and regulators, as applicable. Additionally, AdvisorAssist's Principal maintains all appropriate licensing to promptly become registered with the Advisor to assist with any Client transactions.

AdvisorAssist will contact the applicable securities regulators to assist with the transition of responsibilities or the proper wind-down of the Advisor.

AdvisorAssist may be contacted as follows:

AdvisorAssist, LLC
Christopher E. Winn (Primary Contact)
892 Plain Street, Suite 10
Marshfield, MA 02050
www.advisorassist.com
support@advisorassist.com
(617) 800-0388

This Key Person Risk and Succession Planning language contained in the BCP shall be reviewed regularly in order to incorporate any changes in the Advisor's business operations that would impact the document, as applicable.

8. Testing the BCP

The CCO is responsible for testing the integrity of the BCP and making any required modifications given the results of the testing, as applicable.

Alternate Work Sites

On an at least annual basis, Supervised Persons will work from their alternate work site to ensure that each Supervised Person can resume all critical business functions and day-to-day operations. The review will be documented within the Advisor's books and records.

Third-Party Vendor Due Diligence

On an annual basis, the CCO or Delegate will request BCP information from its vendors to ensure they maintain an adequate contingency plan to support the activities of the Advisor. Any deficiencies will be addressed with the vendor and documented in a memorandum to be placed in Advisor's books and records and/or the Advisor's annual review of the effectiveness of the Compliance Program.