Business Continuity and Disaster Recovery Plan

NobleBridge Wealth Management, LLC
d/b/a: NobleBridge Wealth™
December 23, 2021

Background

Investment advisers owe a fiduciary duty to their clients to have disaster recovery plans in place in the event of a natural disaster, accident, death, or other event that would disrupt the normal business flow of the adviser and the services it provides to its clients.

A disaster recovery plan must detail the steps that an adviser and each of its Associated Persons will take in the event of a disaster. This plan, including all contact information for clients, Associated Persons, regulators, custodians, and service providers, should be updated regularly and each revision should be communicated to Associated Persons as applicable.

Policies and Procedures

The Company's Business Continuity and Disaster Recovery Plan ("the Plan" or "Plan") is an essential part of its operations. All Associated Persons are responsible for understanding their role in the event of a disaster or major disruption. The Primary Disaster Recovery Coordinator ("DRC") for the Company is the CCO, who has the overall responsibility for the Company's response to a major disruption, is responsible for ensuring that the Company's Plan is tested annually and is updated when regulatory or operational changes occur. The DRC will maintain and distribute copies of the Plan, including updates, to all Associated Persons for review and acknowledgement. The DRC may designate one or more persons to assist with their duties. In the event the DRC is unavailable or unable to perform their duties, the following Alternate Contact Persons are as follows:

- Alternate Contact #1: Aimee Luers-Franco/Research Associate
- Alternate Contact #2: Robert Schaff/Operations Consultant

Significant Business Disruptions

A Significant Business Disruption ("SBD") is any event that renders the Company unable to provide its usual level of service without immediate recovery. The physical location of the Company may or may not be affected.

The Company's Plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only the Company's ability to communicate and conduct business, such as a fire or power outage in the building. External SBDs prevent the operation of the securities markets in their entirety or impact specific critical operations of the Company, resulting from natural or manmade disasters including, but not limited to; weather, pandemics, terrorist attacks, or other regional and national disruptions. The

Company's response to an external SBD relies more heavily on other organizations and third-party vendors, including the Company's custodian as well as federal emergency authorities, local officials and utility companies.

Depending on the severity of the external SBD, the Company's response may include a notice to clients via regular mail or electronic communication.

If the SBD does not affect the Company's ability to continue to operate from the primary or a branch location(s) of the Company, the DRC will provide Associated Persons with instructions based on the impact of the disruption.

If the SBD affects the primary or a branch location(s) of the Company, the DRC will notify all critical personnel of next steps and provide direction to each Associated Person as to whether or not they will be required to report to the alternate recovery location.

In the event the SBD does not prevent Associated Persons from working remotely, Associated Persons may be required to telecommute from their private residence.

The DRC will determine the steps necessary to resolve the SBD, to the extent possible. This may include contacting the facilities manager for the building where the Company's office is located and the Company's technology support person/team, including offsite data storage provider and email retention provider, to determine next steps and expected length of time for resolution.

Building Evacuation Procedures
In the event of an office building evacuation, all Associated Persons should immediately leave the building. Go immediately to our designated meeting location or contact the DRC directly, so that the DRC may confirm everyone is safe and accounted for. If a building evacuation occurs and an Associated Person is on the phone, the Associated Person should inform the caller that the building is under mandatory evacuation, and immediately terminate the call in a professional manner.

Because every building and situation has unique characteristics and circumstances, below are some general guidelines to follow for building evacuation:

1. Do NOT use the elevators.
2. Make yourself aware of the closest exit, and go to it.
3. Instruct others in your area to also leave the building.
4. Sound any alarms, e.g. fire alarms, if needed.
5. Proceed to the designated meeting location, if applicable.

Temporary Operation Location/Recovery Site
If an Associated Person's primary office is inaccessible, the Associated Person will temporarily relocate to their respective alternative address(es). The DRC maintains a full list of primary office locations and alternative locations.

In the event that it is not practical to relocate, the Company may determine that all Associated Persons will work remotely from their homes ("telecommuting"). Client data is easily accessible through the Company's network and at any remote location with Internet access. Client data, including e-mail correspondence and pertinent books and records, is backed up and archived Daily . The archive is maintained away from the Company's primary business location to allow for retrieval of client records where the primary office location is not accessible.

Contacting Associated Persons

Should Associated Persons not be at work when the major disruption occurs, Associated Persons will be contacted using the most effective and available means including; telephone, text, e-mail or in-person. The Company maintains a list of its Associated Persons and contact information as part of human resources records. In the event of an SBD, the DRC will assess which means of communication are still available.

The Company may also utilize a call tree to reach all Associated Persons quickly during an SBD. The call tree includes all staff personal or alternative contact phone numbers including residential addresses and personal e-mail addresses. The DRC and Associated Persons are responsible for retaining an accessible copy of the most current call tree with Associated Persons' contact information as maintained by the Company or the DRC at a location other than the Company's primary business office. The call tree is maintained as a separate document outside of the Plan and is updated periodically.

Company Social Media Site(s)
The following social media site(s) can be updated remotely and will be updated, as needed, to provide direction to clients who wish to contact the Company or their Custodian and to provide the summary disclosure of the Plan.

- www.noblebridgewealth.com
- www.nbwm-carolinas.com
- www.northernvirginiawm.com/
- www.twitter.com/noblebridgewm
- www.linkedin.com/company/noblebridge-wealth-management-llc

Telephone Service/Fax
Our main telephone number is 866-798-0354 and fax number of 973-265-7677. In the event the Company's main telephone line is disrupted, Associated Persons will forward their direct lines to their personal cell phones, if necessary. Any incoming faxes go directly to the DRC's email address.

Notification of Proper Authorities
After an emergency has been declared, the DRC shall notify the proper regulatory authorities of the nature of the emergency, and the temporary location of the Company, and notify the local public utilities, the telephone company, the post office and any other vendor as deemed necessary.

Equipment/Hardware
The Company will maintain a list of all equipment, hardware and software, used by the Company. The list shall provide identifying information for the item, including the serial number, the manufacturers and serial/registration number as applicable. The CCO will notify the Company's insurance company of any damage.

If an essential part of the Company's support system, including servers, computers and hardware, is deemed unusable for any reason, the Company will procure the necessary equipment at that time. Time constraints for the purchase, delivery, and installation of the equipment will depend on a number of outside factors such as the retailer, delivery services, and the consultant hired to install the equipment, but it is expected that the Company will only be without the necessary equipment or hardware for a maximum of two business days. Once the new equipment is installed, the last backup will be restored to the new system.

Mail Service
If the Company is unable to receive mail at its business office, the Company will either forward mail to an alternate location, or submit a mail hold request to the post office.

Client Information and Client Trading Records, and Other Books & Records
Client agreements, contracts, profiles, and other documentation related to each client as well as trading records, the Company's financial information and other required books and records are maintained at the principal place of business in accordance with the Company's Books and Records policies and procedures as referenced in the Company's Compliance Manual.

Copies of pertinent client information shall be kept at a secure off-site location, approved third party vendor, or cloud service provider. Periodically, the DRC will review the Plan pertaining to client's records to assure that these records will be adequately maintained in the event of a disaster or emergency. In addition, the DRC may use encrypted and password protected portable hard drives or thumb drives with client contact information.

Client Notification
If an SBD occurs that requires client contact, every effort will be made by the Company to contact all clients. This may be accomplished via phone calls, emails, general mailing, posting a message on the Company website, or by other means. A list of all clients is maintained in the Company's account management system and can also be received by contacting the relevant account custodian.

Client Access to Funds and Securities
The designated custodian(s) maintains custody of customers' funds or securities. If a client needed immediate access to their account, and for any reason could not contact the Company, the client could contact his or her custodian(s) directly. The Company will use the most efficient and available forms of communication to provide instructions on how clients can contact the custodian(s) directly and the DRC maintains a list of contact instructors that can be provided to a client at their request . If available, the Company will post on the Company website the contact information for the designated custodian(s). Copies of certain client records are also maintained by the custodian(s) holding the client's assets. The Company can access client records from the custodian as needed.

Regulatory Reporting and Filing
The Company is subject to regulation by federal and/or state regulatory agencies. Depending upon the impact of the SBD, the DRC is responsible for informing the governing regulatory bodies when required by law. The DRC will determine which means of filing are available to the Company. In the event filing deadlines are extended, the CCO will be responsible for documenting the rationale for utilizing the extension and ensuring the regulatory filing is submitted by the new deadline.

- SEC Contact Information - https://www.sec.gov/contact-information/sec-directory
- State Regulator Contact Information - https://www.nasaa.org/contact-your-regulator/

Key Vendors
The operational resiliency practices of our third party vendors, services providers, and business partners (collectively, "Key Vendors") is a critical component of our Company's Plan. The Company Plan incorporates by reference other policies and procedures intended to address important due diligence factors, specifically, the Oversight of Service Providers section of the Company's Compliance Manual.

Key Personnel
In the event key personnel are unable to work, or only able to work part-time during an active SBD, the Company has assessed the key personnel and their critical job functions that require a backup plan. The Company will ensure the necessary system access and cross training has taken place to effectively implement the Plan.

In the event both the key personnel and backup are affected by the SBD, the Company may maintain a password recovery tool or application for all Associated Persons through an approved third party vendor. The DRC will be responsible for monitoring the password recovery tool or application and maintain the master password for such tool or application.

Sucession Planning
In the event of Mr. Franco's death or incapacity the following persons will conduct the necessary efforts to ensure continuity or a wind-down of the Company; Mrs. Aimee Luers-Franco, Mr. Phillip P. D'Ambrisi, & Mr. Robert Schaff . This group will be responsible to ensure timely communications, client account management, risk controls of the firm, and day to day management of both Mr. Franco's personal business dealings and that of the adviser entity, including to the necessary regulatory bodies and clients of the Company. Communications to all clients shall occur within five (5) business days of occurrence via all available means of communications. Additional continuity plan agreements have been executed to provide the additional details and authorizations and are retained as separate documents.

Updates and Annual Review
The Company will update this Plan whenever there is a material change to the Company's operations, structure, business or location or to those of our custodian (or any other critical service providers). In addition, the Company will test the Plan, at least annually, and update the Plan as needed, to ensure the Plan remains consistent with the Company's policy and overall business operations. Associated Persons are required to acknowledge updates to the Plan.

Telecommuting
Equipment
In the event the Company determines to require or permit telecommuting, the Associated Person will supply information to the DRC concerning the appropriate equipment needs (including hardware, software, modems, phone and data lines and other office equipment) for the telecommuting arrangement. Equipment supplied by the Company will be maintained by the Company. Equipment supplied by the Associated Person, if deemed appropriate by the Company, will be maintained by the Associated Person. The Company accepts no responsibility for damage or repairs to Associated Person-owned equipment. The Company reserves the right to make determinations as to appropriate equipment, subject to change at any time. Equipment supplied by the Company is to be used for business purposes only. The telecommuter must take appropriate action to protect the items from damage or theft. Upon termination of employment, all company property will be returned to the Company, unless other arrangements have been made.

Bring Your Own Device
Equipment supplied by the Associated Person must be approved and deemed appropriate by the Company. The DRC is responsible for retaining an accessible copy of the most current Associated Person owned device list and updating that list on an ongoing basis or during the annual testing of the plan.

Supplies
The Company will supply the Associated Person with appropriate office supplies (pens, paper, etc.) as deemed necessary. The Company will also reimburse the Associated Person for business-related expenses, such as phone calls and shipping costs that are reasonably incurred in carrying out the Associated Person's job when the Company requires the Associated Person to telecommute.

Work Environment
The Associated Person will establish an appropriate work environment within his or her home for work purposes. The Company will not be responsible for costs associated with the setup of the Associated Person's home office, such as remodeling, furniture or lighting, nor for repairs or modifications to the home office space.

Security
Consistent with the Company's expectations of information security for Associated Persons working at the office, telecommuting employees will be expected to ensure the protection of proprietary company and customer information accessible from their home office. For example, when Associated Persons use Video-teleconferencing (VTC) platforms it will be expected that meetings are private, either by requiring a password for entry, muting controls, controlling guest access from a waiting room, disabling chat, and limiting screen sharing. In addition to these controls, telecommuting Associated Persons should include the use of locked file cabinets and desks, regular password maintenance, and any other measures appropriate for the job and the environment.

Safety
Associated Persons are expected to maintain their home workspace in a safe manner, free from safety hazards. Injuries sustained by the Associated Person in a home office location and in conjunction with his or her regular work duties are normally covered by the company's workers' compensation policy. Telecommuting Associated Persons are responsible for notifying the employer of such injuries as soon as practicable. The Associated Person is liable for any injuries sustained by visitors to his or her home worksite.

Members of the Associated Person's Household
Telecommuting is not designed to be a replacement for appropriate childcare. Although an Associated Person's schedule may be modified to accommodate childcare needs, the focus of the arrangement must remain on job performance and meeting business demands. Prospective telecommuters are encouraged to discuss expectations of telecommuting with family members prior to telecommuting.

Key Vendors

Our service providers provide business continuity plans including the availability of redundant data centers and alternate processing facilities to address interruptions to the normal course of business. These plans are often reviewed annually and updated as necessary by providers.

Contingency plans for providers will often outline the actions they will take in the event of a building, citywide, or regional incident that disrupts its normal processes. These actions can include relocating technology and operations personnel to pre-assigned alternate regional or country facilities and switching technology data processing to an alternate regional data center.

Operational facilities are equipped for resumption of business. The recovery-time objective for resuming business is often up to a few hours, even in situations involving a relocation of personnel or technical equipment. The ability to meet these recovery objectives may be impaired by the unavailability of external resources or by other circumstances beyond its control.

The DRC maintains a list of principal service providers and their contact information. The DRC is responsible for both maintaining the list and retaining a physical copy of the most current version of the list at a location other than the Company's primary business office.