Pandemics, Epidemics, & Outbreaks

O'Haver Wealth Management, LLC (OWM) recognizes that pandemics, epidemics, and other types of outbreaks constitute business disruptions of a special nature. These situations impact not only OWM as a company, but also its personnel, clients, and vendors. Accordingly, OWM intends to implement the following procedures during such a situation.

General Business Operations

Promptly, and then intermittently thereafter, OWM will conduct a high-level assessment of the situation's impact on business and operations. Specifically, OWM will identify and address:

- any weaknesses or unforeseen issues
- any inability to conduct essential operations or operate essential systems
- any inability to monitor third party vendors

Information Security & Remote Operations

OWM will also alert personnel to the increase likelihood of phishing attempts and client impersonation schemes related to the situation. For example, bad actors may target individual staff members with requests for wire transfers posing as a client, emails related to state or federal work from home updates, changes to healthcare benefits, changes in information security policy related to working from home, software required to install on computers in order to work from home, the latest epidemic statistics, or even discounted offers on items in short supply. Accordingly, the firm will refer personnel to OWM's cybersecurity best practices and ensure that those practices are up to date.

If necessary, ABBREV will also conduct training for its personnel to address (i) potential information security issues commonly associated with remote work and (ii) the importance of protecting non-public client information at all times. In particular, advisory personnel are instructed to:

- access the internet only from secure WiFi connections or via a virtual private network ("VPN")
- avoid using public WiFi networks, which are vulnerable to exploitation
- store any sensitive, non-public information on non-company devices only after taking the proper security protections and obtaining authorization

If having personnel work remotely, then OWM will also:

- catalogue systems that cannot be accessed remotely, if any
- shut down non-essential hardware (e.g., computers)
- lock its physical storage (e.g., file cabinets) and all office access
- check in with building management, if applicable, to determine current security at the facility

- require that firm personnel continue following advertising guidelines for applicable communications
- ensure electronic cataloguing of communication is still taking place
- continue to document all interactions with clients, regardless of the medium of interaction
- update OWM's business continuity plan as needed

Third Party Vendors

If appropriate, OWM will endeavor to discuss with vendors the following:

- the vendor's business continuity efforts
- the vendor's disaster recovery plans
- the vendor's reliance on, and communications to date with, the vendor's vendors

Company Personnel

If appropriate, OWM will limit or altogether avoid in-person meeting with clients and advisory personnel and allow or require (as appropriate) personnel to work remotely. Any personnel that is limited in their ability to work remotely, will immediately inform their supervisor. Limitations include but are not limited to:

- Inadequate hardware, software, or other systems
- Need to perform caregiving services for children or other persons
- Physical incapacity

If essential personnel are limited in their ability to work remotely, then the firm will determine if alternate or temporary personnel are available to perform necessary functions. Additionally, OWM will conduct check-ins with advisory personnel no less than weekly regarding remote work conditions.