Business Continuity Plan

Summary

January 2026

I. Overview of This Document

Advisors Asset Management, Inc. (AAM) maintains a comprehensive Business Continuity Plan (BCP). The BCP is an internal document that is not available to the public. This document, the Business Continuity Plan Summary is intended to provide our customers and other interested parties with information regarding our BCP.

II. Contacting Us

If after a significant business disruption you cannot contact us as you usually do at (800) 697-7220, you should call our alternative number (800) 347-5128 or go to our web site at www.aamlive.com. If you cannot access us through either of those means, you should contact our clearing firm; Pershing, at (201) 413-3635, or www.pershing.com, for instructions on how they may assist you with some types of security, cash disbursement, and security transfer transactions for your customers.

III. Firm Policy

Our firm's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and firm property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the firm's books and records, and allowing our customers to transact business with minimal disruption.

Significant Business Disruptions (SBDs)

Our plan anticipates various kinds of SBDs, internal and external. Internal SBDs affect only our firm's ability to communicate and do business, such as a fire in our building. External SBDs prevent the operation of the securities markets or a number of firms, such as a terrorist attack, a city flood, earthquake, or a wide-scale, regional disruption. Our response to an external SBD relies more heavily on other organizations and systems, especially on the capabilities of our clearing firms, Pershing, or NFS.

It is impossible to list every type of event that might trigger an SBD. Generally speaking, any event that disrupts any of our branches could become an SBD. The senior corporate managers together with managers at an affected branch will determine on a case by case basis the expected extent of the disruption in order to decide whether or not to begin execution of this plan.

Examples of potential SBDs include fire, earthquake, flood or other events that can destroy or incapacitate one of our offices. Also, power outages and loss of communications that last longer than an hour could become an SBD. In many cases it may be difficult to determine whether or not an outage should trigger our Business Continuity Plan. In the event of a power outage or communications failure, our CEO and/or CCO will determine whether or not to implement this plan based on the expected duration of the outage, the time of day, and all other information available to them at the time.

Note that we do not consider a computer failure to be an SBD. All critical servers are virtualized and running in a clustered virtual host environment. Therefore, in the event that one or more virtual instances or servers fail, it should not cause an SBD. The AAM Internal Backup and Recovery Plan documents all of our servers, and the backup and recovery plans in place.

IV. Plan Training & Testing

Training for and testing of the incident response and recovery procedures will be performed annually. Primary objectives of the testing include ensuring completeness and accuracy of the procedures within the plan, identifying weaknesses in the plan that require modifications to improve plan effectiveness, providing training and practice for business continuity team members, and ensuring ability to recover critical functions in acceptable timelines. Additionally, awareness training will be provided to all employees on incident handling protocols, communications, and relevant instructions for better incident preparedness.

V. Key Employee Procedures

The Business Continuity Team (BCT) is responsible for the strategic and tactical response to any event that disrupts business operations. In the event of a significant incident, the BCT will ensure that the appropriate elements of the plan are implemented to minimize the impact to the firm. The BCT is also responsible for ongoing maintenance of the plan. Additionally, our firm maintains a succession plan that provides an interim and process to reach a long-term solution in the event that certain key executives are unable to perform their duties.

VI. Customers' Access to Funds and Securities

Our firm does not maintain custody of customers' funds or securities, which are maintained at our clearing firms, Pershing and National Financial Services LLC (NFS). In the event of an internal or external SBD (if telephone service is available) our registered persons will take customer orders or instructions and contact our clearing firms on their behalf. If Web access is available, our firm will post on our Web site instructing Retail customers that they may access their funds and securities by contacting Pershing at (201) 413-3635 or (213)-624-6100 extension 500. Pershing LLC requires all instructions from clients in writing and transmitted via email to general.customer.service@bny.com or postal services - Pershing LLC, P. O. Box 2065, Jersey City, New Jersey 07303-5368. Pershing LLC will be able to process limited trade-related transactions, cash disbursements and security transfer. AAM will make this information available to customers through our disclosure policy.

If SIPC determines that we are unable to meet our obligations to our customers or if our liabilities exceed our assets in violation of Securities Exchange Act Rule 15c3-1, SIPC may seek to appoint a trustee to disburse our assets to customers. We will assist SIPC and the trustee by providing our books and records identifying customer accounts subject to SIPC regulation.

VII. Data Back-Up and Recovery (Hard Copy and Electronic)

Electronic Data

Our primary data center is in our San Antonio area, TX branch. Our database servers and other mission critical servers are all located in our San Antonio area, TX data center.

Data on all of our mission critical servers is backed up to backup servers in our Monument, CO backup data center either throughout the day or at least each night (depending on the type of data and its importance). AAM uses a combination of cloud storage, individual machine backups (code 42), and Unitrends.

Data from our branch office locations are backed up to cloud storage solutions.

In the event of an SBD in any of the branches other than San Antonio, the San Antonio data center will provide a backup system for the affected branch. In the event of an SBD in our San Antonio branch, we will shift to our backup data center in our Monument branch.

Our recovery objectives address Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). Our RPO for critical data is 15 minutes, meaning that we should not lose more than 15 minutes of transactions in the case of an SBD at our data center. Our RTO is 4 hours, meaning that if we have to shift to our backup data center in Monument, our goal is to have our critical systems operational within 4 hours. Our goals are based on an SBD that is local to our office area. Widespread disruptions such as terrorist attacks or national communications disruptions could adversely affect our ability to continue processing from our backup data center.

Hard Copy

Our firm maintains its primary hard copy books and records at our Monument branch. Important documents are kept in a fireproof vault with offsite copies kept at a storage facility.

VIII. Operational Assessments

AAM has offices located in separate regions across the country and the primary data center resides in the Boerne office. In the event of an SBD in any one city, the firm will be able to continue operations in the other cities. Additionally, the firm has available alternate work sites for each AAM office. AAM personnel will communicate with clients using our website, email, and/or telephones.

IX. Mission Critical Systems

Our firm's "mission critical systems and vendors" are those that ensure prompt and accurate processing of securities transactions, including order taking, entry, execution, comparison, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts, and the delivery of funds and securities. Both AAM and our clearing firms Pershing and NFS perform mission critical tasks for our customers.

A. Pershing Mission Critical Systems

Our clearing firm, Pershing, maintains customer accounts and is responsible for delivery of funds and securities to our customers. Pershing has its own Business Continuity Plan which we have reviewed, and we expect that Pershing will be able to recover from an SBD at their primary office.

Recovery-time objectives provide concrete goals to plan for and test against. They are not, however, hard and fast deadlines that must be met in every emergency situation, and various external factors surrounding a disruption, such as time of day, scope of disruption, and status of critical infrastructure—particularly telecommunications—can affect actual recovery times. Recovery refers to the restoration of clearing and settlement activities after a wide-scale disruption; resumption refers to the capacity to accept and process new transactions and payments after a wide-scale disruption. Pershing has the SBD recovery time and resumption objective of 4 hours.

B. National Financial Mission Critical Systems

Our clearing firm, NFS, maintains customer accounts and is responsible for delivery of funds and securities to our customers. NFS has its own Business Continuity Plan which we have reviewed, and we expect that NFS will be able to recover from an SBD at their primary office.

Recovery-time objectives provide concrete goals to plan for and test against. They are not, however, hard and fast deadlines that must be met in every emergency situation, and various external factors surrounding a disruption, such as time of day, scope of disruption, and status of critical infrastructure—particularly telecommunications—can affect actual recovery times. Recovery refers to the restoration of clearing and settlement activities after a wide-scale disruption; resumption refers to the capacity to accept and process new transactions and payments after a wide-scale disruption.

C. Our Firm's Mission Critical Systems

AAM uses a proprietary software system called Bailey to manage all trade related activity. Telephone orders are received by our registered reps and they enter the order into Bailey. Web orders are automatically set up in the Bailey order system. Orders are sent to our traders who allocate bonds from our inventory to the customer placing the order, or in the event where we do not already own the bonds, our trader will attempt to buy the bonds from other dealers.

Bailey handles the communications between our registered reps and our traders. When a trade is executed, Bailey sends the trade information to our clearing firms, Pershing or NFS.

In the event of an SBD, orders could still be taken by phone from one of the unaffected branches. We have registered reps engaged in customer service in multiple branches. We also have traders in multiple branches, and traders in an unaffected branch could execute trades on behalf of traders in a branch where an SBD occurred.

Our website, which could run from San Antonio or from our backup facility in Monument, CO will advise our customers that a branch is experiencing an SBD. Customers will be advised to call an alternate branch for service. Our registered reps in any branch have the information and skills they need to fill in for the reps in any branch affected by an SBD.

In order to operate, Bailey requires a number of computer servers. These servers are located in our San Antonio data center. The servers are virtualized in our San Antonio, TX data center and also backed up to our alternate data center in our Monument, CO branch.

In the event of an external SBD that prevents us from trading with other firms, we will enter the orders into Bailey and execute the orders by phone as soon as we and other firms are able to conduct business again.

Moxy

Moxy is the mission critical order management system for the registered investment advisory services (specifically Separately Managed Accounts) for SMA Operations and is provided by Advent. Advent maintains its own BCP and AAM periodically verifies that plan is tested and aligns with AAM's recovery time objective. Moxy is run on AAM's Microsoft Azure cloud to ensure business continuity in the event of localized network issues. To that effort, all SMA Operations employees, who are based in either the Boerne (TX) or Monument (CO) office, have the laptop computers and VPN tokens necessary to access Moxy from anywhere with a network connection (including their homes and designated emergency meeting facilities). In the event Moxy is unavailable, all SMA order entry personnel have log-in credentials for each of the sponsors utilized.

Moxy Initial Incident Response - All

In the event of any Moxy disruption, Jayme Fox, Chris Genovese, and Jim Costas (AAM's Moxy Team, "AMT") must be notified immediately. It is incumbent upon these individuals, with the assistance of AAM's IT Department and/or the vendor where necessary, to promptly determine, to the extent possible, the cause/source of the disruption, the expected impact, the estimated recovery time, and whether the firm's Business Continuity Team ("BCT") must be convened.

Moxy Incident Response – Other Primary Advisor

In the event of any Moxy disruption greater than 15 minutes, the AMT must notify the primary advisor's designated contact(s) in the manner specified by that advisor within 45 minutes of the start of the incident. At or about that time, a communication plan should be established with the advisor to ensure they have all relevant information in a timely manner throughout the outage. The advisor may, at any time, direct AAM to implement the Moxy back-up system and/or modify the trading rotation for their accounts.

Business Continuity Events – Rothschild & Co Asset Management US, Inc. ("R&C")

It is incumbent for the AMT to notify the designated contact at R&C within 45 minutes of discovering any actual or imminent (e.g., approaching fires or flooding at a key office) business continuity event that has affected or has the substantial likelihood to affect the level of service provided to R&C. At or about that time, a communication plan should be established with R&C to ensure they have all relevant information in a timely manner throughout the event.

X. Alternate Communications

Alternate Employee Communications

In the event of a significant business disruption, AAM will coordinate and align all employees with notifications around events via emails, call trees, and voicemail.

Alternate Communications Between Firm and Customer

We now communicate with our customers using the telephone, e-mail, our Web site, fax, and U.S. mail. In the event of an SBD, we will assess which means of communication are still available to us and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. For example, if we have communicated with a party by e-mail but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the U.S. mail or fax. Client contact information is located in the hosted CRM system that can be accessed remotely.

Alternate Communications Between Firm and Vendors

AAM maintains a list of critical service providers with contact information for each vendor.

Regulatory Reporting

Our firm is subject to regulation by FINRA and the SEC. We now file reports with our regulators using paper copies in the U.S. Mail, and electronically file using fax, e-mail, and the Internet. In the event of a significant business disruption, we will check with FINRA, the SEC, and other regulators to determine which means of filing are still available to us, and use the means closest in speed and format to our previous filing method.

XI. Critical Business Constituents

We have assessed the products and services provided to us by our critical business constituents (businesses with which we have an ongoing commercial relationship in support of our operating activities, such as vendors providing us critical services), and determined the extent to which we can continue our business relationship with them in light of the internal or external SBD. We will quickly establish alternative arrangements if a business constituent can no longer provide the needed goods or services when we need them because of a SBD to them or our firm.

- Bloomberg, LP
- ADP, Inc.
- Financial Firms
- Bank of New York
- Moxy/Advent
- Zoom Video Communications

XII. Updates and Annual Review

Our firm will update this plan whenever we have a material change to our operations, structure, business or location. An annual BCP review will assess incident management protocols, assigned responsibilities, critical functions and dependencies, priorities, new risks, and recovery strategies.

XIII. For More Information

If you have questions about our Business Continuity Plan you can contact us at (800) 697-7220.