Accelar, Inc. DBA XoomFi Advisors
Business Continuity and Disaster Recovery Plan
Adopted July 2023

This document outlines the immediate and long-term business continuity and disaster recovery plan ("BCP" or the "Plan") for Accelar, Inc. DBA XoomFi Advisors ("XoomFi" or the "Firm"). The purpose of the Plan is to provide specific guidelines XoomFi, and its employees will follow in the event of a disruption or failure of any critical business capability whether due to an emergency, disaster or otherwise. A copy of this BCP is accessible to each Supervised Person of XoomFi for reference. This BCP is the property of XoomFi, and its contents are confidential.

Summary

The Investment Advisers Act of 1940 (the "Advisers Act"), as amended, imposes a fiduciary duty upon registered investment advisers to act in the best interest of their clients. As part of that fiduciary duty, it is critical for XoomFi to be able to provide continuous, uninterrupted services to its clients. This document outlines policies and processes to assure that XoomFi can continue to provide such service in the event of a disaster or other unexpected event.

Risks

In developing this Plan, XoomFi considered various risks associated with its inability to continue its operations in the event of a disruption or failure or any critical business capability, including:

- Company and client assets may not be protected from loss or damage.
- XoomFi may not have access to mission critical systems to perform daily functions.
- Employees may not know what to do in the event of an emergency.
- XoomFi does not have an alternative work site(s) in place.
- Unavailability or loss of key management personnel.
- Unavailability or loss of key staff personnel.
- The Plan becomes ineffectual or inaccurate.

Goals and Objectives

The goal of this Plan is to provide uninterrupted service to XoomFi's clients or to minimize service interruptions should a disaster result in any of the risks noted above. The Plan has been developed to meet the following objectives:

- Provide for immediate, accurate and measured response to emergency situations;
- Ensure the safety and well-being of the firm's personnel;
- Protect against the loss or damage to organizational assets;

- Ensure all data processing systems, communication facilities, client information and business functions can be restored in 24 hours or less;
- Provide our clients with continuous portfolio management services.

Key Concept

XoomFi built an infrastructure of computer systems and processes that allows the Firm to function from anywhere and at any time, all within the cloud. With access to the Internet—which is available from home, public access sites, wireless "air cards," or tethered cell phones—personnel can perform all portfolio management functions remotely (e.g., portfolio monitoring, trade allocation, trading, trade settlement, reconciling); maintain electronic communications; retrieve company research; process client billing; conduct HR functions; and process company payables. All connections to company servers are encrypted, which enables the Firm to operate securely, even if it has to connect from open, unsecured public networks. XoomFi's systems and their backups run on Office 365 which are accessible from anywhere in the world. This is a key concept of XoomFi's Business Continuity Plan.

Safety and Mobility of Employees

XoomFi's first commitment is to the health and safety of its employees. XoomFi maintains an Emergency Contact List set forth in Appendix A, which includes the current contact information for all employees. The CCO or designee will distribute that list to all employees on a regular basis to ensure that all employees can be contacted and accounted for in the event of an emergency. Employees are directed to ensure that such information is always available to them. This is accomplished through storing this information in employee cell phones and/or PDAs; and making the Plan (including Appendix A) available to all employees.

Facilities

In the event XoomFi's office building at 111 N. Market Street, Suite 300 San Jose, CA 95113 (the "Office"), cannot be entered or used for any reason, the CCO or designee will contact all employee to work remotely at home until further notice.

The CCO or his designee is responsible for coordinating with the Office landlord and local emergency services as necessary. Specific emergency services numbers are set forth on Appendix B.

The Office is protected by both alarm and fire systems, including sprinklers. The system includes fire sensors, internal motion detectors, and camera/video surveillance.

Remote Facilities

All employees have the ability to work remotely. In the event their main working location cannot be entered or used for any reason, the individual will immediately notify the CCO. The individual will continue working remotely from a different location, as applicable.

Client Communications

As an internet advisor, XoomFi has minimal communications with clients. Employees of XoomFi have personal devices (cell phones) to communicate with each other for work related services. In the event XoomFi's website is down, clients will be notified of how to further contact XoomFi.

Third Party Vendors

Because key, third-party vendors provide mission-critical services to XoomFi in its functioning, the firm will take the following actions to ensure these vendors maintain their own disaster recovery plans:

As applicable, the CCO will conduct due diligence to support the disaster recovery plans for XoomFi's mission-critical third-party vendors. The CCO is responsible for reviewing these vendors and documentation the reviews to adequately address the security and confidentiality of all client data; backup of technology systems, facilities, and communications; recovery procedures; and the use of alternate systems, facilities, and ability of their staff to respond to XoomFi needs in the event of a disaster.

The CCO maintains a detailed list of the emergency contact information for each of XoomFi's third-party vendors as set forth in Appendix C. If either XoomFi or any of its third-party vendors experiences a systems or business failure, the CCO or his designee will initiate immediate contact with affected firms to determine the cause, nature, and extent of the disruption.

Network Stability and Security

XoomFi utilizes a third-party cloud provider for all emails and data storage that have their own redundancies.

Preservation of Critical Data and Recovery

Critical Data is defined as all Books and Records required by the Investment Advisers Act of 1940, Rule 204-2. XoomFi maintains all these records electronically.

XoomFi's CCO maintains a programmed backup routine for all firm data and applications. The process runs daily. Backup data is replicated in a geographically dispersed location and is regularly checked and tested by the CCO.

Personnel

XoomFi recognizes that all employees play an essential role within the organization. XoomFi attempts to reduce the potential for disruption to its business should any employees suddenly become incapacitated or unavailable for an extended period. Currently, there is only one employee at XoomFi, the owner. When additional employees are hired, all employees will be cross trained for similar positions to cover absent employees' responsibilities due to vacation, sickness, hospitalization, injury or extended leave of absence.

The following procedures have been developed in the event XoomFi has to wind down the business or transition the business to another party because it is unable to continue providing advisory services. The objective is to minimize any adverse effects on their clients and fund investors.

- All assets of the clients are held at a qualified custodian that is independent of XoomFi Asset Management, therefore, there is no physical transition of assets necessary. This will minimize the risk. The accounts can also remain fully funded during the transition to limit any market impacts.
- Clients will be notified promptly if the firm is to wind down the business to allow them enough time to determine the appropriate steps for their personal accounts. If client assets are to be reassigned to another party, consent will be provided to inform the client and/or fund investor of the transfer.
- If transferring responsibility to another party, documents containing non-public client information will be transferred to the appropriate party in a secure fashion to protect the client.

Insurance contact information is maintained in Appendix D.

Examples of Trigger Events

While it is impossible to cover all events that would trigger the implementation of the Plan, the examples below demonstrate how to utilize the procedures listed above:

Earthquake while in remote working location:

1. Take cover under a desk or table, or leave the building
2. If necessary, notify the CCO

Fire in office while in remote working location:

1. Leave the building
2. Call 9-1-1
3. If necessary, notify the CCO

Power outage in remote working location or location is inaccessible:

1. Continue working remotely, where possible.
2. If necessary, notify the CCO

Pandemic Illness:

1. Stay home! Continue working remotely where possible.
2. If necessary, notify the CCO
3. The CCO will determine the procedures listed above that need to be implemented.

Injury or Death of Employee:

1. As necessary, call 9-1-1
2. Notify the CCO
3. The CCO will determine the procedures listed above that need to be implemented (e.g., Emergency Contact, Personnel).

Plan Maintenance and Testing

The CCO is responsible for reviewing, updating, distributing, and testing the Plan as necessary, but at least annually.

As part of the CCO's periodic review of the Plan, at least annually, the CCO, in consultation with key personnel, will review the Plan to ensure that any business and technological changes of the firm have not rendered any portion of the plan ineffectual or inaccurate.

The CCO is responsible for initial and ongoing training of the firm's employees regarding the Plan and for answering employee questions about the Plan. The CCO will distribute the Plan to all employees upon employment and annually thereafter or earlier, if necessary, upon a material update to the plan made during a given year.

The CCO is responsible for organizing periodic (no less than annually) testing of the Plan to determine the firm's ability to implement the Plan in an organized fashion.

The CCO will maintain written records of each review, distribution, training, and testing undertaken in accordance with this Plan and any modification of this Plan.

APPENDIX A

Employee Emergency Contact List

APPENDIX B

Third-Party Vendor Contact List

Local Emergency Services Contact List

Emergency Service	Phone Number	Address
Police		
Fire	911	
Ambulance	911	
Hospital		

APPENDIX C

Other Key Contact Information