

**SF Investments, Inc.**  
**Business Continuity Plan**  
**Table of Contents**

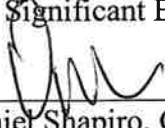
	<u>Page</u>
Introduction.....	2
Emergency Contact Persons .....	3
Firm Policy.....	4
Business Description.....	5
Office Locations.....	5
Alternative Physical Location(s) of Employees .....	5
Customers' Access to Funds and Securities .....	5
Data Back-Up and Recovery .....	6
Financial and Operational Assessments.....	7
Mission Critical Systems .....	8
Clearing Firm Summary .....	9
Alternate Communications .....	11
Critical Business Relationships.....	12
Regulatory Reporting.....	14
Disclosure of BCP.....	16
Updates and Review .....	16
Customer Disclosure.....	17
RIA WorkSpace Technology Plan.....	18

This "Business Continuity Plan" has been created to meet the requirements described in FINRA Rules 4370. This Business Continuity Plan is reasonably designed to enable our firm to meet its obligations to customers in the event of a Significant Business Disruption.

Authorized Approval Signature: \_\_\_\_\_

Printed Name & Title: \_\_\_\_\_

Date: \_\_\_\_\_

  
Daniel Shapiro, CEO

3/29/23

This Plan is effective from the date approved until the date of its authorized revision, update or replacement (see below).

Date this Plan was no longer effective (date of revision, update or replacement): \_\_\_\_\_

Recordkeeping: Discard after \_\_\_\_\_ (date three years from termination of use).

## **Introduction**

In September 2009, the Securities and Exchange Commission approved FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) as part of the FINRA rulebook consolidation. Rule 4370 requires each member to create and maintain a business continuity plan that identifies procedures relating to an emergency or significant business interruption that are “reasonable designed to enable the member to meet its existing obligations to its customers.” In addition, the plan must address the firm’s existing relationships with other members and counterparties. This plan must be promptly made available to the FINRA staff upon request.

Rules 4370 requires that each member review its plan at least annually to determine if any changes are needed and update its plan more frequently in the event of any material change to its operations, structure, business or location.

The plan should reflect the firm’s business and operations. Therefore, the requirements of the plan, as identified in Rule 4370, are flexible and should be tailored to the firm’s size and needs.

However, at a minimum, SF Investments, Inc.’s plan must address the following areas:

- Data back-up and recovery (hard copy and electronic).
- All mission critical systems.
- Financial and operational assessments.
- Alternate communications between customers and the member.
- Alternate communications between the member and its employees.
- Alternate physical location of employees.
- Critical business constituents, banks, and counterparty impact.
- Regulatory reporting.
- Communications with regulators; and
- How the member will assure customers’ prompt access to their funds and securities in the event that the member determines that it is unable to continue its business.

Each firm is required to only address the elements applicable to its business, but the plan must contain an explanation if any element above is not included.

Rule 4370 requires each member to designate two individuals as emergency contacts that the FINRA may contact in the event of a significant business disruption. Each contact must be a registered principal or member of senior management. However,

- If the member has only one principal but has other employees, the second contact should be another firm employee, or
- If the firm has only one principal and no other employees, the second contact may be someone who has knowledge of the firm’s business, such as an accountant, attorney, etc.

Rule 4370 also requires that each member enter this information into the FINRA Contact System which is accessed through the FINRA Firm Gateway and that required changes are made promptly.

## **1. Emergency Contact Persons**

SF Investments, Inc. has designated the following individuals to act as contact persons for the firm as required under Rule 4370:

### **Primary Contact**

Name, Title: Danny Shapiro, CEO  
Address: 799 Central Ave. Suite 350 Highland Park, IL. 60035  
Telephone Number: (847) 926-5711  
Fax Number: 847-926-5701  
E-mail Address: danny@sfinv.com

### **Secondary Contact:**

Name, Title: Steven A. Shapiro, VP, CIO  
Address: 799 Central Ave. Suite 350 Highland Park, IL. 60035  
Telephone Number: (847)926-5712  
Fax Number: 847-926-5702  
E-mail Address steve@sfinv.com

These contacts will be reported through FINRA's Contact System on the FINRA Firm Gateway and must be updated in the event of a material change. In addition, SF Investments, Inc.'s Executive Representative or his written designee must review and update this information, if necessary, within 17 business days of the end of each quarter.

### **Executive Representative:**

SF Investments, Inc.'s Executive Representative is Daniel Shapiro.

### **Disaster Recovery Coordinator/Team:**

The Company has designated Danny Shapiro, CEO as the "Disaster Recovery Coordinator." In his absence, Steve Shapiro, Vice President will assume his responsibilities. The Company has appointed an Emergency Management Team "EMT" that will be responsible for administering and executing various sections of this plan. The EMT will follow the direction of the "Disaster Recovery Coordinator" or his designee in carrying out assigned duties. The EMT is made up of the following people: Gary Just and Rosina Mahabeer.

The "Disaster Recovery Coordinator" has the responsibility to make an immediate preliminary assessment of the nature and extent of the disruption by assessing the following: electricity supply; condition of computer network/phones; damage to the building; HVAC in extreme weather; and other hazards; pandemics and State orders/guidelines.

If the Coordinator determines that personnel should evacuate the affected location or work from home, he must make an announcement to all personnel as appropriate. The announcement may be given via personal contact, e-mail, phone, text or other methods as appropriate given the systems available and size of staff and building. This announcement should be short and concise, should calmly identify the situation and should provide instructions to employees on how to respond. This

announcement should be repeated as often as necessary to avoid confusion and to ensure all employees are aware of the situation. After ensuring the physical safety of Company personnel, the Coordinator and the EMT must then implement this BCP.

If the situation does not merit evacuation, steps should be taken to alert designated persons (the EMT) of necessary actions to facilitate ongoing operations in the face of limited disruption. In this case, the Coordinator will determine which, if any, procedures in this BCP should be implemented.

In the event, the SBD has directly affected other areas of the building but has not directly impacted the Company's office, the Coordinator will contact building security or emergency personnel for instructions on how the Company should respond and proceed accordingly.

## **2. Firm Policy**

SF Investments, Inc.'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 the firm's books and records, and allowing our customers to transact business. In the event that we determine we are unable to continue our business, we will assure customers prompt access to their funds and securities.

### **Significant Business Disruptions (SBDs):**

SF Investments, Inc.'s plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only the Company's ability to communicate and do business, such as a fire or loss electrical power in the office or building.

External SBDs prevent the operation of the securities markets or a number of firms, such as a terrorist attack, a natural disaster, or another event that causes a wide-scale, regional disruption in essential services. The Company's response to an external SBD will rely more heavily on other organizations and systems, especially on the capabilities of the clearing firm, the issue sponsors, federal emergency authorities, local officials and utility companies.

### **Approval and Execution Authority:**

Daniel Shapiro, CEO, a registered principal, is responsible for approving the plan and for conducting the required annual review.

Steven Shapiro, Vice President, in addition to Daniel Shapiro *has* the authority to execute this BCP.

### **Plan Location and Access:**

SF Investments, Inc. will maintain copies of its BCP plan, a record of the firm's annual reviews, and the changes that have been made to the BCP for inspection by regulators. A hard copy of the Company's Plan is located in its main business location and may be accessed by contacting Daniel Shapiro at (847) 926-5700 or [danny@sfinv.com](mailto:danny@sfinv.com). An electronic copy of the Company's plan is located internally on the firm's server under Firm Compliance.

A copy of the BCP will be provided to FINRA District Office #8 located in Chicago, IL upon request.

### **3. Business Description**

SF Investments, Inc. conducts business in equity, fixed income, and derivative securities. The Company is an introducing firm and does not perform any type of clearing function for itself or others. Furthermore, the Company does not hold customer funds or securities.

SF Investments, Inc. accepts and enters orders. All transactions are sent to the clearing firm, which executes, compares, allocates, clears and settles them. The Company's clearing firm also maintains our customers' accounts, can grant customers access to them, and delivers funds and securities.

The Company's clearing firm is Pershing LLC, a subsidiary of The Bank of New York Mellon Corporation. The mailing address for Pershing is One Pershing Plaza, Jersey City, New Jersey 07399 and their web address is [www.pershing.com](http://www.pershing.com).

### **4. Office Locations**

The Company or its registered personnel currently operate from the following locations:

Type of Location, Registered or Unregistered	Address and Main Phone Number	Located in a Personal Residence? (Y or N)	Means of Transportation Employees Use to Reach Office	Mission Critical Systems Taking Place at Office
Home Office – registered	799 Central Ave. Suite 350 Highland Park, IL. 60035	No	Car, train, bus	Order taking, entry, execution comparison, access to customer accounts, process cash movement requests.

#### **Alternative Physical Location(s) of Employees:**

In accordance with Rule 4370 requires that each member designate a location at which business will be conducted in the event the primary office of the Company must be evacuated.

SF Investments, Inc. has no other office locations, therefore, in accordance with this requirement; members of the Company's staff will work from home via our Microsoft Azure cloud access, set-up through Inhouse CIO, our IT manager.

### **5. Customers' Access to Funds and Securities**

SF Investments, Inc. does not maintain custody of customers' funds or securities. Customer accounts are maintained at our clearing firm, Pershing, LLC.

In the event of an SBD:

1. If telephone service is available, our registered persons will take customer orders or instructions and contact our clearing firm on their behalf, and
2. If Internet access is available, we will post a notice on our website, [www.sfinvestments.com](http://www.sfinvestments.com), which includes procedures for customers to use in contacting the clearing firm directly to access their funds and securities or to place orders.
3. If telephone service and internet access are unavailable, customers can receive information on how to request funds and securities by visiting the Pershing website, [www.pershing.com](http://www.pershing.com), under the “Customer Support” section. Customers can also call (201) 413-3635 for recorded instructions.

The Company will make this and additional information regarding accessing funds and/or securities available to customers through our disclosure policy (below).

If SIPC determines that the Company is unable to meet its obligations to its customers or if the Company’s liabilities exceed its assets in violation of Securities Exchange Act Rule 15c3-1, SIPC may seek to appoint a trustee to disburse the Company’s assets to its customers. SF Investments, Inc. will assist SIPC and the trustee by providing applicable books and records identifying customer accounts subject to SIPC regulation.

## **6. Data Back-Up and Recovery (Hard Copy and Electronic)**

SF Investments, Inc. maintains its primary books and records in hard copy and electronic format at 799 Central Ave. Suite 350 Highland Park, IL. 60035, Gary Just, FINOP, 847-926-5700 is responsible for the maintenance of these books and records.

SF Investments, Inc. maintains the following document types and forms that are not transmitted to the clearing firm: financial information, contracts, invoices, bank statements and checks.

### **Back-up of Paper Records:**

SF Investments, Inc. copies its paper records monthly, and the back-up copies are maintained at 799 Central Ave. Suite 350 Highland Park, IL 60035, while electronic copies are available on our servers. Gary Just, FINOP, 847-926-5700 is responsible for the maintenance of these back-up books and records.

Because the Company does not hold customer funds, an internal or external SBD affecting the Company’s office should not pose a threat to customer records or financial holdings. While the Company may lose access to some or all FINRA or SEC required records in an external SBD or may permanently lose some or all such records in an internal SBD (such as a fire), we believe our customers would not suffer as a result.

### **Back-up of electronic records:**

The firm maintains all servers with electronic files/records and all required software/programs through the RIA WorkSpace Microsoft Azure “cloud” platform. The firm maintains no physical servers or electronic records onsite at its office. The RIA Workspace Technology Plan is available upon request. All employees can access all critical work functions through any

configured internet connection by connecting through Microsoft Office 365 online portal. All employees have company laptops that are configured to access all company servers and work applications.

## **7. Financial and Operational Assessments**

### **Operational Risk:**

In the event of an SBD, SF Investments, Inc. will immediately identify any methods available that will permit personnel to communicate with customers, other employees, critical business constituents, critical banks, critical counterparties, and regulators.

Although the effects of an SBD will determine the means of alternative communication, the communications options the Company may employ will include Website, cell/smart phone, telephone, voice mail and secure e-mail. In addition, SF Investments, Inc. will retrieve key activity records as described in the section above, Data Back-Up and Recovery (Hard Copy and Electronic).

### **Financial and Credit Risk:**

In the event of an SBD, SF Investments, Inc.'s FINOP will determine the value and liquidity of its investments and other assets to evaluate the Company's ability to continue to fund its operations and remain in capital compliance.

SF Investments, Inc. will contact its clearing firm, critical banks, and investors to apprise them of the Company's financial status. If the Company determines that it may be unable to meet its obligations to those counterparties or otherwise continue to fund its operations, SF Investments, Inc. will request additional financing from our bank or other credit sources to fulfill its obligations to our customers and clients. If SF Investments, Inc. cannot remedy a capital deficiency, the FINOP will file appropriate notices with applicable regulators and immediately take appropriate steps, including contacting the FINRA immediately and ceasing business until a business plan is executed to reduce expenses and infuse additional capital to meet the net capital requirement.

In the event there is suspension or termination of the Company's business, the Company will attempt to notify customers regarding the situation and provide them with instructions for accessing their funds or securities, if applicable, for verifying transactions in process or for conducting future business. Notification will be based on the circumstances and in a form permitted by regulatory authorities. The form of notification may include telephone calls, letters or a posting on the Company's website.

## **8. Mission Critical Systems**

### **Internal Mission Critical Systems**

SF Investments, Inc.'s "mission critical systems" are those that ensure prompt and accurate processing of securities transactions, including order taking, entry, the maintenance of customer accounts, and access to customer accounts.

The Company has primary responsibility for establishing and maintaining business relationships with customers and has sole responsibility for the Company's mission critical functions of order taking and entry.

#### **Order Taking**

Currently, the Company receives orders from customers via telephone. During an SBD, we will continue to take orders through any methods that are available and reliable.

The Company will inform our customers what alternatives they have to send their orders to us in the event traditional methods are interrupted. Customers will be informed of alternatives by disclosure information provided when a new business relationship is established and by calls from personal cell phones, through email messages or via a notification posted on the Company's website or any other means available.

#### **Order Entry/Submission**

Currently, SF Investments, Inc. enters/submits orders by recording them on paper and/or electronically and sending them to our clearing firm electronically and by telephone.

In the event of an internal SBD, the Company will send orders to its clearing firm by the fastest alternative means available, which may include cloud access, alternative telephone facilities, including cell phones; smart phone access to Pershing's trading system; messenger or courier; or external e-mail connections.

In addition, during an internal SBD, the Company may refer customers directly to the clearing firm for placing orders.

In the event of an external SBD, the Company will maintain the order in electronic or paper format and deliver the order to the clearing firm product or issuer by the fastest means available when it resumes operations.

#### **Order Execution**

The Company does not execute orders. All orders are executed through the Company's clearing firm. See below for information on the clearing firm's mission critical systems.



### **Mission Critical Systems Provided by Our Clearing Firm**

The Company's clearing firm provides, through contract, the execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts, and the delivery of funds and securities.

SF Investments, Inc.'s clearing agreement, or addendum thereto, provides that the clearing firm will maintain a business continuity plan and the capacity to execute that plan. Pershing will provide SF Investments, Inc. with an executive summary of its plan upon request.

### **Summary of Pershing's Business Continuity Plan:**

To address interruptions to Pershing's normal course of business, Pershing maintains a business continuity plan, which includes geographically dispersed data centers and processing facilities. The plan is reviewed annually and updated as necessary.

The plan outlines the actions Pershing will take in the event of a building, city or regional incident, including:

- Continuous processing support by personnel located in unaffected facilities.
- Relocating technology or operational personnel to alternate regional facilities.
- Switching technology data processing to an alternate regional data center

All Pershing operational facilities are equipped for resumption of business and are tested. Regarding all circumstances within our control, Pershing's Critical Service recovery time objective for business resumption, including those involving a relocation of personnel or technology, is four (4) hours or less, depending upon the availability of external resources.

If your firm experiences a significant business interruption, you may contact Pershing directly to process limited trade-related transactions, cash disbursements and security transfers.

### **Trades**

Pershing will process the following closing security transactions:

- Sale of security position held long in the client's account
- Buy of security to close-out short security position

Pershing will process closing security transactions upon receipt of written instructions that must include the following information:

- Client brokerage account number
- Client name (as registered on the brokerage account)
- Security description, including symbol or CUSIP® number
- Number of shares

Note: All orders will be handled as market orders

Instructions to Pershing must be in writing and transmitted via facsimile to (201) 413-5368 or by postal service as follows:

BNY Mellon | Pershing  
P.O. Box 2065  
Jersey City, NJ 07303-2065

Please note that this fax number is for business interruption-related issues only, and should not be used for any other purposes, such as change of address notices, account transfers and credit verification. Information received on this fax that is unrelated to business interruption issues will not be acted upon.

### **Cash Disbursements**

Pershing will process cash disbursements upon receipt of signed written instructions that must include the following information:

- Client brokerage account number
- Client name (as registered on the brokerage account)
- Exact amount to be disbursed
- Method of disbursement (as follows), and provide the information indicated:
  - a) Check
    - o Indicate name and address of record to which the check is to be mailed
  - b) Federal Funds
    - o Indicate receiving bank name, ABA number and receiving bank account number

Note: The receiving bank account name and brokerage account name must be identical unless we have a letter of authorization on file indicating alternate instructions.

Instructions to Pershing must be in writing and transmitted via facsimile or postal service as follows:

BNY Mellon | Pershing  
P.O. Box 2065  
Jersey City, NJ 07303-2065  
Fax: (201) 413-5368

Please note that this fax number is for business interruption-related issues only, and should not be used for any other purposes, such as change of address notices, account transfers and credit verification. Information received on this fax that is unrelated to business interruption issues will not be acted upon.

### **Securities Transfers**

Pershing will process security transfer requests upon written instructions that must include the following information:

- Client brokerage account number
- Client name (as registered on the brokerage account)
- Description of security(ies) to be transferred, including symbol(s) or CUSIP number(s)
- Quantity to be transferred
- Receiving account information for securities, as follows:
  - a) Transfer to another brokerage account at Pershing
    - Provide receiving account number at Pershing (name and address on both accounts must be the same)
  - b) Transfer to another financial organization
    - Name of the receiving financial organization
    - DTC number (if the receiving financial organization is a registered broker-dealer)
    - Name of the receiving financial organization

Instructions to Pershing must be in writing and transmitted via facsimile or postal service as follows:

BNY Mellon | Pershing  
 P.O. Box 2065  
 Jersey City, NJ 07303-2065  
 Fax: (201) 413-5368

Please note that this fax number is for business interruption-related issues only, and should not be used for any other purposes, such as change of address notices, account transfers and credit verification. Information received on this fax that is unrelated to business interruption issues will not be acted upon.

## **9. Alternate Communications Between the Firm and Customers, Employees, and Regulators**

### **Customers**

The Company currently communicates with our customers using the telephone, U.S. mail, email, and in person.

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 customer. 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 via U.S. mail.

### **Employees**

The Company currently communicates with its employees using the telephone, cell phones, e-mail, and in person. 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.

The company can communicate with all employees through Microsoft Teams, which is part of our Microsoft Azure cloud.

The Company will also employ a call tree so that senior management can reach all employees quickly during an SBD, if telephone service is available. The Disaster Recovery Coordinator and/or Emergency Management Team will be responsible for invoking the call tree. The call tree will include all staff home and office phone numbers.

Caller	Call Recipients
Daniel Shapiro	Gary Just, Steve Shapiro, Nate Shapiro, Mike George, InhouseCIO, Dee Dee Silverstein, Steve Virgili, Rosina Mahabeer, Mansoor Zakaria, Jaclyn Lerman

### **Regulators**

The Company is currently a member of the FINRA, registered with the SEC and registered to conduct business in the following states: AZ, CA, CT, FL, IL, IN, MD, NJ, NY, TX, & WI.

SF Investments, Inc. communicates with applicable regulators using the telephone, e-mail, U.S. mail, and in person.

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.

## **10. Critical Business Constituents, Banks, and Counterparties**

### **Business Constituents**

SF Investments, Inc. has contacted our critical business constituents (businesses with which the Company has an ongoing commercial relationship in support of its operating activities, such as vendors providing critical services), and determined the extent to which the Company can continue its business relationship with these businesses in light of the internal or external SBD. The Company has entered into a supplemental contract with certain critical business constituents to provide such services. The alternative suppliers are disclosed below.

Our major suppliers are:

Business Constituent	Address, Phone Number	Alternative Supplier	Address, Phone Number
Pershing LLC	1 Pershing Plaza Jersey City, NJ 07399 888-367-2563	None	

Bloomberg	499 Park Ave., New York, NY 10022, (212) 318-2540	Refinitiv	312-682-1100
Refinitiv	311 S. Wacker Chicago, IL 312-682-1100	Bloomberg	499 Park Ave New York, NY 10022 (212) 318-2540
InhouseCIO	8770 W. Bryne Ave Suite 1300 Chicago, IL 60631 (773)-530-1234	None	
AT&T	(800) 727-2273 Land (847) 778-9381 Fiber	Comcast (back-up internet)	(800) 391-3000
Avaya/SRU Communications	847-417-0666		

## Banks

SF Investments, Inc. has contacted its banks and lenders to determine if they can continue to provide the financing that the Company may need in light of the internal or external SBD. The Company's accounts are currently with the following institutions:

<b>Types of account (i.e., checking, savings, PAIB, escrow)</b>	<b>Name of Financial Institution</b>	<b>Address of Financial Institution</b>	<b>Telephone Number</b>	<b>Contact Name</b>
Checking	First Bank of Highland Park	1835 First Street, Highland Park, IL 60035	847-432-7800	Lesley Prestegaard Courtney Olsen
Various accounts	Pershing LLC	1 Pershing Plaza Jersey City NJ	888-367-2563	

If our banks and other lenders are unable to provide the financing, we will seek alternative financing immediately.

## **Counterparties**

SF Investments, Inc. has contacted our critical counterparties, such as other broker-dealers, to determine if we will be able to carry out our transactions with them in light of the internal or external SBD. Where the transactions cannot be completed, we will work with our clearing firm or contact those counterparties directly to make alternative arrangements to complete those transactions as soon as possible.

## **11. Regulatory Reporting**

SF Investments, Inc. is subject to regulation by the FINRA and SEC, as well as various state and other securities regulators (see list of states in Part 10 – Regulators)

The Company currently files reports with our regulators using paper copies in the U.S. mail, and electronically using fax, e-mail, and the Internet. In the event of an SBD, we will check with the SEC, FINRA, and other regulators to determine which means of filing are still available to us and use the means closest in speed and form (written or oral) to our previous filing method. In the event that we cannot contact our regulators, we will continue to file required reports using the communication means available to us.

The Company's current regulators can be reached as follows:

FINRA District Number #8:  
55 west Monroe Street, Suite 2700,  
Chicago, IL 60603-5001  
(312) 899-4400

SEC Midwest Region:  
175 W. Jackson Blvd., Suite 900,  
Chicago, IL 60604  
(312) 353-7390  
E-mail : [chicago@sec.gov](mailto:chicago@sec.gov)

State of Arizona  
1300 W. Washington St., 3rd Floor;  
Phoenix, AZ 85007  
602-542-4242

STATE of California  
320 West 4<sup>th</sup> Street, Ste. 750,  
Los Angeles, CA 90013-1105  
(213) 576-7643

STATE of Connecticut  
260 Constitution Plaza,  
Hartford, CT 06103-1800  
(860) 240-8299

STATE of Florida  
101 East Gaines Street, Plaza Level, The Capital,  
Tallahassee, FL 32399-0350  
(850) 410-9805

STATE of Illinois  
17 North State St, Ste. 1100  
Chicago, IL 60601  
(312) 793-3384

STATE of Indiana  
302 west Washington Street, Room E-111,  
Indianapolis, IN 46204  
(317) 232-6681 or (800) 223-8791

STATE of Maryland  
200 St. Paul Place, 20<sup>th</sup> Floor  
Baltimore, MD 21202-2020  
(410) 576-6360

STATE of Nevada  
2250 Las Vegas Blvd. N. Suite 400  
North Las Vegas, NV 89030  
(702)-486-2440

STATE of New Jersey  
153 Halsey Street, 6<sup>th</sup> Floor,  
Newark, NJ 47029  
(973) 504-3600

STATE of New York  
120 Broadway, 23<sup>rd</sup> Floor,  
New York, NY 10271  
(212) 416-8000

STATE of Texas  
Rusk Building, 208 E. 10<sup>th</sup> Street, 5<sup>th</sup> Floor,  
Austin, TX 78711-3167  
(512) 305-8300

STATE of Washington  
PO Box 9033  
Olympia, WA 98507-9033  
(360) 902-8760

STATE of Wisconsin  
B41 West, State Capitol,  
Madison WI 53702  
(608) 266-2211

## **12. Disclosure of Business Continuity Plan**

The Company will disclose in writing a summary of our BCP to customers at account opening or at the time a business relationship is established. The Company will notify customers in writing when material changes are made to the Plan that may affect their business relationship with the Company. The Company will also post the summary on our Web site and mail it to customers upon request.

The summary addresses the possibility of a future SBD and how we plan to respond to events of varying scope. In addressing the events of varying scope, the summary:

1. Provides specific scenarios of varying severity (e.g., a firm-only business disruption, a disruption to a single building, a disruption to a business district, a city-wide business disruption, and a regional disruption).
2. States whether we plan to continue business during that scenario and, if so, our planned recovery time; and
3. Provide general information on our intended response.

Our summary also discloses the existence of back-up facilities and arrangements. A copy of the Company's disclosure statement is included at the back of this Plan.

## **13. Updates and Annual Review**

The Company will update this plan whenever there is a material change to its operations, structure, business or location or to those of the clearing firm.

The Company's BCP will be reviewed and modified, if necessary, at least annually, to take into account any changes in the Company's operations, structure, business, or location or those of our clearing firm.



## **Customer Disclosure Statement**

### **SF Investments, Inc.**

The Company's plan considers two kinds of Significant Business Disruptions (SBDs), internal and external. Internal SBDs affect only the Company's ability to communicate and do business, such as a fire or loss electrical power in the office or building.

External SBDs prevent the operation of the securities markets or a number of firms, such as a terrorist attack, a natural disaster, or another event that causes a wide-scale, regional disruption in essential services.

**Contact information:** Any questions regarding the Company's Business Continuity Plans should be addressed to: Dan Shapiro, 799 Central Ave. Suite 350 Highland Park, IL. 60035; (847) 926-5700.

**Internal SBDs:** In the event of a disruption in the Company's business operations due an internal SBD, the Company will attempt to continue to conduct business as usual by utilizing alternative communication methods (if available), such as the Internet, smart/cell phones, etc., or by moving its operations to an alternative location.

**External SBDs:** In the event of a disruption in the Company's business operations due to an external SBD, the Company will attempt to continue to conduct business as usual by moving its operations to an alternative location outside the affected area, if possible, or by providing customers with alternative arrangements.

The Company will resume normal business operations as soon as it is able to do so, based on the type and the extent of the disruptive event.

**Communications:** In the event you are unable to reach the Company, customers should proceed as follows:

1. Email: [operations@sfinv.com](mailto:operations@sfinv.com)
2. Call (847) 926-5700 or (800) 691-9273
3. Call Pershing (201) 413-3635 or visit the Customer Support section of the Pershing website.

All critical records related to the Company's business operations are backed-up daily and stored in a secure offsite location (RIA WorkSpace Microsoft Azure "Cloud" Platform). These back-up files can be used to restore Company systems to ensure that business can be back to normal as quickly as possible after the disruption.

The Company's clearing firm, Pershing, LLC, maintains a business continuity plan in the event of an SBD. For more information on their plan, visit their website at [www.pershing.com](http://www.pershing.com)





**RIA WorkSpace  
Technology Plan for  
SF Investments Inc.**

## Contents

RIA WorkSpace.....	4
National Data Center Footprint .....	4
Infrastructure Protection .....	5
Physical security.....	5
Fire Suppression.....	5
Redundant Power Systems.....	5
Flood Control & Earthquake Management.....	5
Monitoring and logging.....	6
Update management.....	6
Antivirus and antimalware.....	6
Penetration testing.....	6
DDoS Protection.....	6
Network Protection .....	7
Network isolation.....	7
Virtual networks.....	7
VPN and Express Route.....	7
Encrypting communications.....	7
Data Protection .....	8
Data isolation.....	8
Protecting data at rest.....	8
Protecting data in transit.....	8
Encryption.....	8
Data destruction.....	8
Identity and Access .....	9
Enterprise cloud directory.....	9
Multi-Factor Authentication.....	9
Access monitoring and logging.....	9
Regulatory Compliance .....	9
Compliance Reports.....	9



SF Investments Inc. IT Narrative .....	10
Local Firewall.....	10
Servers .....	10
Anti – Virus Solution .....	10
Email.....	10
Additional Security.....	10
Backups .....	11
Where are the backups kept.....	11
Backup: There are two types of backup running .....	11
What is Backed up: .....	11
When is it backed up and how often:.....	11
How many versions of a document are kept: .....	12
Archive: .....	12
Due Diligence Report .....	13
General Information .....	13
Insurance.....	14
Business Continuity & Disaster Recovery .....	14
Cybersecurity & Information Security .....	14
SEC OCIE Cybersecurity Initiative RIA WorkSpace Analysis .....	15
Executive Summary.....	15
Disclaimer.....	15
Cybersecurity Preparedness .....	16
Identification of Risks/Cybersecurity Governance.....	16
Protection of Firm Networks and Information .....	19
Risks Associated with Remote Customer Access and Funds Transfer Requests .....	20
Risks Associated with Vendors and Other Third Parties .....	21
Detection of Unauthorized Activity .....	24



## RIA WorkSpace

The RIA WorkSpace Platform in partnership with Microsoft Azure was designed to offer small and mid-sized financial services firm maximum flexibility without compromising security. An intuitive dashboard makes all your business files, data, and applications - both windows and web-based - accessible. A secure, centralized management system works to protect your data and make it easier for your business to comply with regulatory requirements.

## National Data Center Footprint





### Infrastructure Protection

RIA WorkSpace is a Microsoft partner and leverages azure infrastructure includes hardware, software, networks, administrative and operations staff, and the physical data centers that house it all. RIA WorkSpace addresses security risks across its infrastructure.

**Physical security.** This runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

**Fire Suppression.** The Microsoft Azure fire protection approach includes the use of photoelectric smoke detectors installed below the floor and on the ceiling, which are integrated with the fire protection sprinkler system. Additionally, there are Xtralis VESDA (Very Early Smoke Detection Apparatus) systems in each colocation which monitor the air. VESDA units are highly sensitive air sampling systems installed throughout multiple high-value spaces. VESDA units allow for an investigative response prior to an actual fire detection alarm. 'Pull station' fire alarm boxes are installed throughout the datacenters for manual fire alarm notification. Fire extinguishers are located throughout the datacenters and are properly inspected, serviced, and tagged annually. The security staff patrols all building areas multiple times every shift. Datacenter personnel perform a daily site walk-through ensuring all fire watch requirements are being met. Areas containing sensitive electrical equipment (colocations, MDFs, etc.) are protected by double interlock pre-action (dry pipe) sprinkler systems. Dry pipe sprinklers are a two-stage pre-action system that requires both a sprinkler head activation (due to heat) as well as smoke detection to release water. The sprinkler head activation releases the air pressure in the pipes which allows the pipes to fill with water. Water is released when a smoke or heat detector is also activated. Fire detection/suppression and emergency lighting systems are wired into the datacenter UPS and generator systems providing for a redundant power source.

**Redundant Power Systems.** Redundant power includes uninterruptible power supplies (UPS) and backup generators, including on-site multiple-day fuel supply. Generator power is activated automatically in the event of a grid failure.

- Carrier diversity via multiple Tier 1 providers
- Redundant backup diesel generators, including on-site multiple-day fuel capacity.
- Redundant 208v/30amp power to each cabinet
- N+1 HVAC
- N+1 UPS
- N+1 generator
- N+1 power distribution unit (PDU)

**Flood Control & Earthquake Management.** All Azure Data Centers are above sea level, as well as 500-year flood plains. They have no basements, have tightly sealed conduits, and moisture barriers on the exterior walls. Every Azure Data Center contains dedicated pump rooms, drainage/evacuation systems, and moisture detection sensors. Azure Data Centers are built to meet or exceed seismic design requirements of local building codes for lateral seismic design forces.



**Monitoring and logging.** Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

**Update management.** Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure uses a combination of Microsoft and third-party scanning tools to run OS, web application, and database scans of the Azure environment.

**Antivirus and antimalware.** Azure software components must go through a virus scan prior to deployment. Code is not moved to production without a clean and successful virus scan. In addition, Microsoft provides native antimalware on all Azure VMs. Microsoft recommends that customers run some form of antimalware or antivirus on all virtual machines (VMs). Customers can install Microsoft Antimalware for Cloud Services and Virtual Machines or another antivirus solution on VMs, and VMs can be routinely reimaged to clean out intrusions that may have gone undetected.

**Penetration testing.** Microsoft conducts regular penetration testing to improve Azure security controls and processes. Microsoft understands that security assessment is also an important part of our customers' application development and deployment. Therefore, Microsoft has established a policy for customers to carry out authorized penetration testing on their own—and only their own—applications hosted in Azure.

**DDoS Protection.** Azure has a defense system against Distributed Denial-of-Service (DDoS) attacks on Azure platform services. It uses standard detection and mitigation techniques. Azure's DDoS defense system is designed to withstand attacks generated from outside and inside the platform.





### Network Protection

Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises data centers with Azure VMs. Because Azure's shared infrastructure hosts hundreds of millions of active VMs, protecting the security and confidentiality of network traffic is critical. In the traditional datacenter model, a company's IT organization controls networked systems, including physical access to networking equipment. In the cloud service model, the responsibilities for network protection and management are shared between the cloud provider and the customer. Customers do not have physical access, but they implement the logical equivalent within their cloud environment through tools such as Guest operating system (OS) firewalls, Virtual Network Gateway configuration, and Virtual Private Networks.

**Network isolation.** Azure is a multitenant service, meaning that multiple customers' deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.

**Virtual networks.** A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other through private IP addresses. Each virtual network is isolated from other virtual networks.

**VPN and Express Route.** Microsoft enables connections from customer sites and remote workers to Azure Virtual Networks using Site-to-Site and Point-to-Site VPNs. For even better performance, customers can use an optional ExpressRoute, a private fiber link into Azure data centers that keeps their traffic off the Internet.

**Encrypting communications.** Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on-premises data centers.



## Data Protection

Azure allows customers to encrypt data and manage keys, and safeguards customer data for applications, platform, system, and storage using three specific methods: encryption, segregation, and destruction.

**Data isolation.** Azure is a multitenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware.

**Protecting data at rest.** Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily and cost effectively streamline key management and maintain control of keys used by cloud applications and services to encrypt data.

**Protecting data in transit.** For data in transit, customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit, such as between two virtual networks. Azure uses industry standard transport protocols such as TLS between devices and Microsoft datacenters, and within datacenters themselves.

**Encryption.** Customers can encrypt data in storage and in transit to align with best practices for protecting confidentiality and data integrity. For data in transit, Azure uses industry-standard transport protocols between devices and Microsoft datacenters and within datacenters themselves. You can enable encryption for traffic between your own virtual machines and end users.

**Data destruction.** When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse. As part of our agreements for cloud services such as Azure Storage, Azure VMs, and Azure Active Directory, we contractually commit to specific processes for the deletion of data.



### Identity and Access

**Enterprise cloud directory.** Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management. Azure Active Directory makes it easy for developers to build policy-based identity management into their applications. Azure Active Directory Premium includes additional features to meet the advanced identity and access needs of enterprise organizations. Azure Active Directory enables a single identity management capability across on-premises, cloud, and mobile solutions.

**Multi-Factor Authentication.** Microsoft Azure provides Multi-Factor Authentication (MFA). This helps safeguard access to data and applications and enables regulatory compliance while meeting user demand for a simple sign-in process for both on premises and cloud applications. It delivers strong authentication via a range of easy verification options—phone call, text message, or mobile app notification—allowing users to choose the method they prefer.

**Access monitoring and logging.** Security reports are used to monitor access patterns and to proactively identify and mitigate potential threats. Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. Customers can turn on additional access monitoring functionality in Azure and use third-party monitoring tools to detect additional threats. Customers can request reports from Microsoft that provide information about user access to their environments.

### Regulatory Compliance

Every Data Center is SSAE16 SOC1 Type II compliant, meets Securities and Exchange Commission (SEC) requirements, complies with the Sarbanes-Oxley (SOX) Act, and Health Insurance Portability and Accountability Act (HIPAA) guidelines.

### Compliance Reports

All of the Compliance Reports for the platform can be found [here](#).

You will be prompted to sign into your cloud resources to view all the compliance reports.

