Stuart Frankel & Co.
Business Continuity Plan (BCP)

Introduction and Disclaimer

Stuart Frankel & Co., Inc.(the "Firm") has put together the following Business Continuity Plan ("BCP") pursuant to FINRA Rule 3510 and 3520 and NYSE rule 446.

Stuart Frankel & Co., Inc. (the "Firm") asserts that, to the best of its knowledge, all of the information contained in this document is accurate, and that the Firm has created business continuity plans that meet or in its opinion exceeds, industry standards and regulatory requirements. In the event of an actual significant business disruption, the Firm will make every reasonable effort to enact these plans as written. However, the plans summarized below are highly dependent upon critical infrastructure and resources that the Firm maintains no control over, including, but not limited to: electricity, telecommunications, water, external exchanges, market utilities, transportation infrastructures and clearing houses. The Firm cannot guarantee that it will be able to fully implement the plans summarized herein if a significant business disruption results in substantial loss of life.

I. Emergency Contact Persons

Customers can access the Firm by calling 212-943-8787. The emergency contacts for the Firm are: Jeffrey Frankel and/or Andrew Frankel. These names will be updated in the event of a material change and reviewed within 17 business days of the end of each quarter to assure compliance with the rules enumerated above.

II. Firm Policy

Our Firm's policy is to respond to a Significant Business Disruption (hereafter referred to as "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. In the event that we determine we are unable to continue our business, we will assure customers prompt access to their funds and securities.

A. Significant Business Disruptions (SBD's)

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

B. Approval and Execution Authority

Mr. Jeffrey Frankel, a registered principal, is responsible for approving the plan and for conducting the required annual review. Mr. Frankel has the authority to execute this BCP.

C. Plan Location and Access

Our firm will maintain copies of its BCP plan and the annual reviews, and the changes that have been made to it for inspection. We will provide copy of our plan to FINRA in the upcoming months. An electronic copy of our plan is located on the Firms network accessible to all employees of the Firm locally and at the contingency site.

III. Business Description

Stuart Frankel & Co., Inc. (the "Firm") is a registered broker/dealer under the exchange act of 1934. The Firm is principally engaged in buying and selling securities for a diverse group of institutional and individual investors. The Firm is a member of the New York Stock Exchange ("NYSE") and the Financial Industry Regulatory Authority ("FINRA").

The Firm is an introducing broker dealer and clears all transactions on a fully disclosed basis with two clearing firms. The Firms are Pershing, LLC located at One Pershing Plaza (www.pershing.com), Jersey City, NJ 07399 and Goldman Sachs Execution & Clearing, LP, located at 120 Broadway 212-433-7060 21st Floor New York, NY 10271 (www.clearing.gs.com).

Our BCP also relies on the clearing firms to release customer funds and securities. This information is provided in the attached BCP marked Pershing and Goldman.

IV. Office Location

The Firm's primary location is located at 22 Bayview Avenue, 2nd Floor, Manhasset, NY 11030. Our employees may travel to that office by means of foot, car, subway, train, ferry boat or bus. We engage in order taking and entry at this location.

V. Alternative Physical Location(s) of Employees

In the event of an SBD that closes the NYSE. We will move our key personnel from affected NYSE Floor operation to any alternative site designated by the Exchange. All other floor staff will go to our primary office location.

VI. Customers' Access to Funds and Securities

The Firm is an introducing broker dealer and clears all transactions on a fully disclosed basis. As such, the Firm does not maintain custody of customers' funds and securities. Our clearing firms, Pershing, LLC and Goldman Sachs Executions & Clearing, LP, maintain customer funds and are able to deliver funds and securities to our customers. 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 firm on their behalf. Should there be access to the web, our firm will have instruction posted on our website www.stuartfrankel.com on how customers may access their funds and securities. The Firm will make this information available to customers through its disclosure policy at least annually or at their request.

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)

Our firm maintains its primary hard copy books and records and its electronic records at its' primary location referenced above.

The Firm has extensive back-up policies, procedures and process in place designed to handle recovery activities with minimal firm interruption in services if a critical system failure should occur.

Periodically we upgrade the server at the Disaster Recovery site ("DR") with the backup information using the Internet or by a manual upgrade procedure (e.g., the IT rep visits the DR to check and upgrade systems).

In the event the Firm would lose electronic records due to the loss of our main office, we can continue operations from our back-ups at an alternate location.

VIII. Financial and Operational Assessments

A. Operational Risk

In the event of an SBD, the Firm will immediately analyze and identify what means will permit us to communicate with our customers, employees, critical business constituents, critical banks, critical counter-

parties, and regulators. Although the effects of an SBD will determine the means of alternative communication, the communications options we will employ will include the telephone, emails, the Internet etc. In addition, we will retrieve our key activity records as described in the section above.

B. Financial and Credit Risk

In the event of an SBD, we will determine the value and liquidity of our investments and other assets to evaluate our ability to continue to fund our operations and remain in capital compliance. We will contact our clearing firm, critical banks, and investors to apprise them of our financial status. If we determine that we may be unable to meet our obligations to those counter-parties or otherwise continue to fund our operations, we will request additional financing from our bank or other credit sources to fulfill our obligations to our customers and clients.

IX. Mission Critical Systems

Mission Critical Systems are those that the Firm utilizes for trading, Market information, comparison, allocations, order entry, order taking, order management, and those systems utilized ensure the fast and accurate processing of securities transactions.

During a SBD, the Firm expects to have connectivity to all mission critical systems either locally, at the alternative site, through the clearing firms or through the Internet. The systems used by the Firm are not location specific and therefore should be accessible for operations and trading.

Many of these systems are provided through our Clearing firm. Their contact information is attached below.

X. Alternate Communications Between the Firm and Customers, Employees, and Regulators

A. Customers

We now communicate with our customers using the telephone, e-mail, instant messaging, our Web site, fax, U.S. mail, and in person visits at our firm or at the other's location. 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 chose the next best means of communication available.

B. Employees

We now communicate with our employees using the telephone, mobile phones, e-mail, instant messaging, 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 and oral) to the means that we have used in the past to communicate with the other party.

C. Regulators

We communicate with our regulators using the telephone, e-mail, fax, 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.

XI. Critical Business Constituents, Banks, and Counter-Parties

A. Business Constituents

We have contacted our critical business constituents (business 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 and external SBD. We will consider establishing 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.

B. Banks

We have contacted our banks and lenders to determine if they can continue to provide the financing that we may need in light of the internal or external SBD. The bank maintaining our operating account is: Mr. Marc Cohen from JP Morgan Chase, 55 Water Street New York, NY 10041, phone number 212-638-1962 and Raffaella Marciari 330 Plandome Road, Manhasset NY 11030 516-627-3013. The clearing firms maintaining our Proprietary Account of Introducing Brokers/Dealers (PAIB account) are Pershing, LLC and Goldman Sachs.

C. Counter-Parties

We have contacted our critical counter-parties, such as other broker-dealers or institutional customers, to determine if we will be able to carry out our transactions with them in light of the internal and external SBD.

Where the transactions cannot be completed, we will work with our clearing firm or contact those counter-parties directly to make alternative arrangements to complete those transactions as soon as possible.

XII. Regulatory Reporting

Our firm is subject to regulation by: the Financial Industry Regulatory Authority (FINRA), the New York Stock Exchange (NYSE) & the Securities & Exchange Commission. We now file 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, NYSE 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.

XIII. Disclosure of Business Continuity Plan

We disclose our BCP to customers at account opening and mail it to customers upon request.

Updates and Annual Review

Our firm will review an update, if necessary, this plan whenever we have a material change to our operations, structure business or location or to those of our clearing firm. In addition, our firm will review this BCP at least annually, to modify it for any changes in our operations, structure, business, or location.

XIV. Senior Manager Approval

Senior management has approved this Business Continuity Plan as reasonably designed to enable our firm to meet its obligations to customers in the event of an SBD.

Pershing LLC

Business Continuity Disclosure

http://www.pershing.com/business_continuity.html

DISCLOSURE REQUIRED BY NEW YORK STOCK EXCHANGE RULE 446(D) Pershing maintains a business continuity plan, including redundant data centers and alternate processing facilities, to address interruptions to its normal course of business. These plans are reviewed annually and updated as necessary. The plans outline the actions Pershing will take in the event of a building, city-wide, or regional incident, including relocating technology and operational personnel to preassigned alternate regional facilities. Technology data processing can also be switched to an alternate regional data center. All Pershing operational facilities are equipped for resumption of business and are tested several times per year. Pershing's recovery time objective for business resumption, including those involving a relocation of personnel or technology, is four (4) hours. This recovery objective may be negatively affected by the unavailability of external resources and circumstances beyond our control.

In the event that your financial organization experiences a significant business interruption, you may contact Pershing directly to process limited trade-related transactions, cash disbursements, and security transfers. Instructions to Pershing must be in writing and transmitted via facsimile at (201) 413-5368 or by postal service as follows:

Pershing LLC
P.O. Box 2065
Jersey City, New Jersey 07303-2065

For additional information about how to request funds and securities when your financial organization cannot be contacted due to a significant business interruption, please visit the Customer Support section or call (201) 413-3635 for recorded instructions. If you cannot access the instructions from the web site or the previously noted telephone number, Pershing may be contacted at (213) 624-6100, extension 500, as an alternate telephone number for recorded instructions.

Pershing LLC
Contingency Planning

Introducing Broker–Dealer
Executive Summary

December 2009

Pershing®
A BNY MELLON COMPANY

Table of Contents

A. Purpose

The purpose of this document is to provide Pershing's customers with an overview of its business continuity and disaster recovery plans, including a high-level definition of the policies and procedures that will be employed in the event of a business interruption. Please note that this document may be amended by Pershing, at its sole discretion, as material changes are made to Pershing's infrastructure, operations, and contingency plans.

B. Goal

Pershing's goal is to deliver continuous, reliable service to its customers while maintaining regulatory compliance.

C. Basic Assumptions

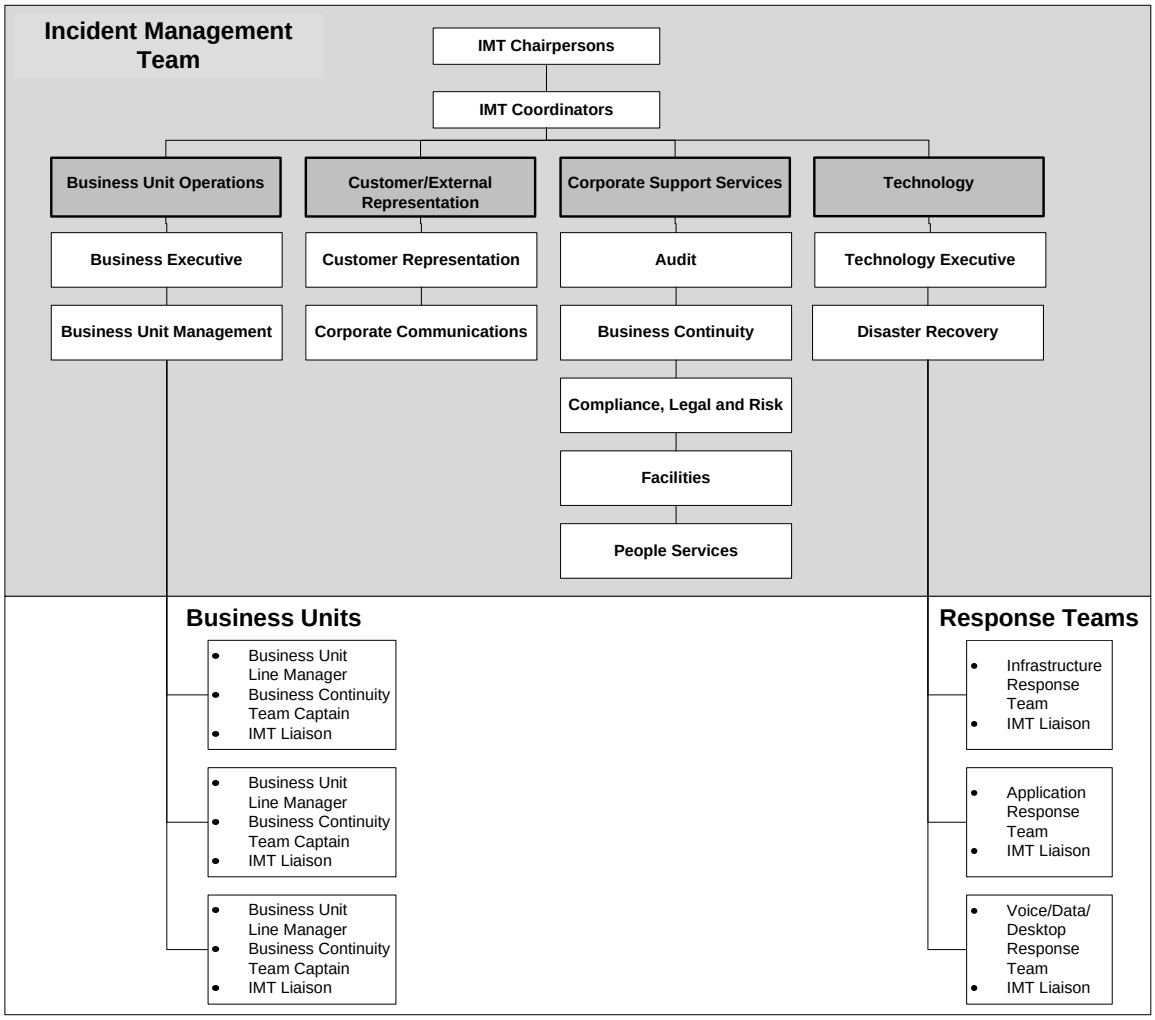
The business continuity plan is based on the following assumptions:

1. Based on the redundancy and geographical dispersion of Pershing's facilities, Pershing assumes that no more than one of its critical facilities will be affected at one time and that alternate facilities will remain accessible and operational.
2. Based on Pershing's efforts to safeguard its facilities (for instance, Pershing's maintenance of redundant generators, chillers, etc.), Pershing assumes that its critical infrastructure (including electricity, water, heat, ventilation, air conditioning, etc.) will remain operational as long as the facility is accessible.
3. If an incident causes the evacuation of one of Pershing's operations centers, Pershing will declare a business continuity event and activate its business continuity plan and facilities.
    a. Pershing has reserved a four-hour recovery window to allow for the comprehensive switching of all related regional fax and voice communications to the alternate, in-region business continuity location; and to allow for the transiting of critical staff to the relocation site if necessary.
    b. While in-region critical staff is relocating, out-of-region processing facilities will continue to provide uninterrupted service wherever possible.
4. If an incident causes the closing of the primary data center, Pershing will declare a disaster recovery event and activate its disaster recovery plan. This may result in an outage up to four hours while our mainframe processing is transferred to the alternate data center.
5. Pershing assumes that the customer's primary or alternate facilities and supporting critical infrastructure (such as electricity, water, heat, ventilation, air conditioning, etc.) are accessible and operational.
6. Pershing assumes critical industry utilities and counter-parties (such as the Depository Trust & Clearing Corporation [DTCC], Security Industry Automation Corp. [SIAC], etc.) are operational.
7. Pershing assumes that it will have adequate staffing available during the event.
8. Pershing assumes that customer-supplied data communication lines between its primary and alternate data centers are redundant.

D. Incident Management Structure

Pershing's incident management response structure includes a multi-disciplined team, scripted processes, and a series of workflows developed from testing, planning, and historic response scenarios. The Incident Management Team (IMT) will be activated during any business continuity or disaster recovery event and will manage operations through recovery to business as usual (BAU).

The accompanying diagram illustrates Pershing's IMT composition.



XV.

XVI. Incident Management Team

IMT members and their alternates are key subject-matter experts whose extensive experience at Pershing allows them to understand the requirements of specific business units, while maintaining a corporate-wide, customer-focused perspective. The IMT:

- Obtains the operational statuses of departments or the customer groups they represent
- Assesses incidents to determine a "right-size" response, which may include activating either the business continuity or disaster recovery plan
- Coordinates with essential business personnel, for instance managers and Business Continuity Team Captains
- Ensures the response is implemented correctly

- Ensures departments comply with the requests of the IMT in a timely manner
- Provides timely and accurate status and recovery information to Customer Relationship Managers and Corporate Communications
- Manages the incident and recovery activities through closure
- Documents post-event analyses and findings

IMT Chairperson ***(Leadership)***

Senior Manager – focal point for IMT decision-making and the execution of strategies

- Acts as a liaison with the Executive Committee
- Coordinates activities at the corporate, business, and technology unit levels

IMT Coordinators ***(Incident Facilitation)***

- Coordinates the flow of information to the IMT, structures meetings, documents event, etc.

Technology ***(Infrastructure)***

- Ensures technology environments are thoroughly assessed and information is presented to IMT in a timely manner
- Establishes priorities and coordinates the allocation of Pershing's technology resources, third-party technical vendors and service providers
- Ensures that IMT directives are implemented
- Acts as a liaison with third-party technical vendors and service providers

Business Unit Operations

- Ensures that appropriate information is collected about the incident and determines the status of the business unit's operational readiness
- Assesses operational and credit risk environments to assist in determining contingency actions
- Makes decisions on contingency actions and drives implementations

Customer/External Representation ***(Customer Relationship Management)***

- Represents the customer's interest in the decision-making process
- Ensures that communications, messages, or both, from Pershing's management and the IMT are delivered promptly and accurately
- Manages outbound communications and inbound requests for information

Corporate Support Services ***(Operations and Oversight)***

- Provides information on impact of the incident
- Supports and facilitates the firm's contingency actions
- Ensures contingency actions undertaken are compliant with laws, rules, and regulations, and provides sufficient controls
- Acts as a liaison with industry and regulatory agencies
- Manages Pershing employee notifications

XVII. Response Teams

The Pershing Technology Group has dedicated teams of technologists to advise on and respond to events, as directed by the IMT. These teams are organized by area of expertise and relevant skill sets.

XVIII.

XIX. Business Units

Each of Pershing's business units has dedicated teams of associates to perform the specific recovery and resumption functions identified in their business continuity plans.

Line Managers

The Line Managers are responsible for activating their business continuity plans, as instructed by the Incident Commander.

Business Continuity Team Captains

The Business Continuity Team Captains and alternates have developed the business continuity plans and managed test scenarios. Their primary responsibility during an incident is to provide their subject-matter expertise to the Line Managers.

IMT Liaison

The IMT Liaison is responsible for communicating the statuses of the business units to the IMT and providing the Line Managers with current IMT decisions.

A. Communications With Customers

XX. Outbound Communications

Pershing Account Managers, Relationship Managers, and the Customer Service Group will work with the Customer Communications Team within Global Marketing to contact customers with information or instructions via e-mail.

XXI. Inbound Communications

It is expected that customers will continue to use existing communication channels with Pershing.

- Relationship Managers will answer general status questions.
- Customers who wish to notify Pershing of technology problems will continue to call Pershing's Technology Customer Service at (201) 413-2001.

A. Security Policies

XXII. Data Security

Disaster recovery access to Pershing's systems during a disaster remains consistent with normal production access. This is achieved by using mirrored or replicated images of the security rules and systems.

XXIII. Physical Security Access

If there is a security system failure at Pershing's facilities, the following guidelines will be implemented:

- Only Pershing associates and authorized vendor support personnel will be allowed access to the facility and all access will be monitored. All associates will be required to show a valid Pershing identification card and authorized vendor support personnel will be required to sign in with Lobby Security each time they enter the facility.
- Access to restricted areas (such as the data center) will only be authorized after the requestor of access has been verified by Security, and only if all designated approvals from accompanying department directors, senior managers, or both, are in place.

- Security will maintain an up-to-date database of all approved associates with programmed card access rights and a sign-in authorization listing for privileged access to these restricted areas.
- Any access required by associates, vendors, or consultants will require approval by their immediate department's director, senior management, or both, of the restricted areas involved.
- Vendors that must be on site in order to perform any required maintenance or repairs will be accompanied by a Pershing associate at all times while onsite.

A. Business Continuity (People and Processes)

Pershing defines business continuity as the firm's ability to provide continuous, reliable and uninterrupted service to the company's introducing broker-dealers and their clients during and after an unplanned business disruption. Integral to the success of Pershing's business continuity program is Pershing's investment in geographically dispersed redundant processing centers as well as the ability to relocate staff and resume business functions at one of several alternate work sites.

XXIV. Business Continuity Plans and Risk Assessments

Consistent with the Financial Industry Regulatory Authority (FINRA) Rule 4370 (formerly NASD Rules 3510 and 3520), Pershing maintains formal business continuity plans that detail the business continuity strategies and processes for each business unit. These plans are updated annually at a minimum or whenever there is a material change to the business, operations, or infrastructure.

Pershing's business continuity plans are designed to be flexible enough to address any of a number of contingencies. They include strategies addressing the loss of a facility, a technology outage and/or a staff shortage, including a pandemic. Whether the event is local, city-wide, or regional in nature, Pershing is confident that it will be able to meet its obligations to its introducing broker-dealers.

Current copies of Pershing's business continuity plans are maintained within each business unit, on the internal network, in IMT command centers, and in secure offsite locations.

XXV. Geographically Dispersed Processing

Pershing operates multiple redundant processing centers in New Jersey, California, Central Florida and Pennsylvania. Critical processing is divided across two or more of these locations in an effort to minimize business interruption in the event of an incident affecting one of the facilities and/or geographies.

XXVI. Alternate Work Sites

Pershing maintains alternate work sites for critical staff that, when combined, accommodate the relocation of over 900 trading, processing, customer service and application development personnel.

- Each operations desktop or trading position is outfitted with the required application software, requisite network access, and telecommunication equipment.
- The internal phone systems have been designed to allow calls to be routed to Pershing's geographically dispersed processing centers, alternate work sites or both.
- Centralized fax and on-line application printer rooms are maintained in these locations and tested regularly.

In addition to alternate work sites, authorized staff across the organization are equipped with remote access capabilities allowing them to access company systems applications remotely through a secured gateway.

XXVII. Testing

Geographically Disbursed Processing

Cross-regional work transfer testing is performed by critical business units with geographically dispersed capabilities.

Alternate Work Sites

Workstations at the alternate work sites are tested at least twice a year.

- One annual test engages approximately 650 processing and 250 trading associates at the in-region alternate facilities. Employees are required to log in to the workstations and telephones to test functionality.
- A second annual test involves performing the business line's daily work from the alternate work sites during normal business hours.

Remote access testing is performed during the annual production from alternate work site test by authorized staff.

A. Disaster Recovery (Technology)

XXVIII. Overview

Pershing defines disaster recovery as the orderly return to normal technology operations at an alternate site, at the direction of Pershing's senior management, after an unplanned technology interruption at the primary site. The process includes the recovery of the technology infrastructure and the technology personnel responsible for supporting it.

XXIX. Sites

Our approach begins with disaster avoidance by housing production and recovery systems within geographically dispersed internal Pershing data centers. The disaster recovery site in the Northeastern U.S. region (New Jersey) is located approximately 800 miles from the production data center located in the mid-southern United States (Tennessee). The data center is available immediately at time of disaster (ATOD) to support the initiation of recovery efforts. These centers are state-of-the-art, hardened facilities with capabilities such as separate power grids, dual power feeds from redundant substations, generator backup, secure facility access, etc. Pershing can operate indefinitely in its recovery site.

XXX. Systems

System and application backup is supported via various replication processes based on the underlying technology used in production. Methods employed include active-active/load-balanced systems, asynchronous disk-mirroring infrastructure, and database replication technology between the data centers.

The recovery process is disk/direct access storage device (DASD)–based and does not require restoration from tape. A complement of redundant virtual tape subsystems (VTS) and native automated tape libraries (ATLs) exists in both the primary and alternate sites in support of local and remote tape backups.

As a result, it is our objective that our systems can be restarted and operational in less than four hours (recovery time objective or RTO), with less than five minutes of data loss, (recovery point objective or RPO).

Linking our customers to their data is equally important, so we build internal redundancy into our network design, as well. Our North American geographically dispersed data centers are designed to support the network in the event of a disaster at either location.

XXXI. Plans and Testing

Pershing's disaster recovery plans and testing program fully comply with FINRA Rule 4370 (formerly NASD Rules 3510 and 3520).

The disaster recovery team is responsible for the creation, maintenance, and testing of all disaster recovery plans. Testing is a formal full-cycle process that encompasses scheduled quarterly tests, ad-hoc testing, and external exercises that addresses business, technology, audit, and compliance requirements. Tests are internal, customer-facing or industry-facing (or both) in scope, and include participation from internal users, our customers, and utilities or exchanges (or both). The focus of these tests is to re-create the flow of information to and from the recovery systems to the end users as seamlessly as possible.

After each test, a written assessment is prepared documenting any problem that is encountered during the test or areas where improvement may be necessary. Action plans are developed and implemented to remediate any issue that is identified. Pershing customers are invited and encouraged to participate in these important exercises.