McNally
Financial Services Corporation
MEMBER FINRA/SIPC

Business Continuity Plan (BCP)

I. Emergency Contact Persons

Our firm's two emergency contact people are: David D. McNally, President, dmcnally@mcnallyfinancial.com at the primary contact number of (210) 545-7080 and Barrett Schultz, Vice President Compliance and Operations, bschultz@mcnallyfinancial.com at the primary contact number of (210) 394-8513. These names will be promptly updated in the event of a material change.

Rule: FINRA Rule 3520.

II. 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. 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)

The firm's plan anticipates two 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, 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 firm.

Approval and Execution Authority

David D. McNally, President, a registered principal, is responsible for approving the plan and for conducting the required annual review. David D. McNally has the authority to execute this BCP.

Plan Location and Access

Our firm will maintain copies of its BCP plan, the annual reviews, and the revised and updated changes that have been made. We have given FINRA District #6 a copy of our plan. An electronic copy of our plan is located on our website at www.mcnallyfinancial.com under the About Us section on the home page.

III. Business Description

Our firm conducts business in equity, fixed income, and derivative securities. Our firm is an introducing firm and does not perform any type of clearing function for itself or others. Furthermore, we do not hold customer funds or securities. We accept and enter orders. All transactions are sent to our clearing firm, which executes our orders, compares them, allocates them, clears and settles them. Our clearing firm also maintains our customers' accounts, can grant customers access to them, and delivers funds and securities. Our firm services retail and institutional customers. We do not currently engage in any private placements.

Our clearing firm is Pershing, LLC and our contact person at that clearing firm is Tanisha Branch, (321-249-4369). Our clearing firm has also given us the following alternative contact in the event it cannot be reached: Pershing, LLC, Post Office Box 2065, Jersey City, New Jersey 07303-2065, telephone contact number (213) 624-6100, extension 500, facsimile number (201) 413-5368 and email address at www.pershing.com/about.htm.

IV. Office Locations

16414 San Pedro Ave, Suite 930, San Antonio, TX 78232

Our firm location at 16414 San Pedro Ave, Suite 930, San Antonio, TX 78232 is the main office. Its main telephone number is (210) 545-7080. Our employees may travel to that office by means of foot, vehicle, and public transportation. We engage in order taking and entry at this location.

1115 Tranquil Trail Drive, San Antonio, Texas 78232-5185

Our backup location, 1115 Tranquil Trail, San Antonio, Texas 78232 is a backup location in the event of significant business interruption at the primary address above. We also can conduct business at any on the non-registered branches of the firm's independent contractor residences or places of employment.

Independent Contractors Locations

Our independent contractors maintain non-registered branches at their residences and places of employment. Their names and locations are attached as enclosure (A).

V. Alternative Physical Location(s) of Employees

In the event of an SBD, we will move our staff from affected offices to the closest of our unaffected office locations. If none of our other office locations are available to receive those staff, we will move them to 1115 Tranquil Trail Drive, San Antonio, TX 78232-5185.

Rule: *FINRA Rule 3510(c)(6).*

VI. Customers' Access to Funds and Securities

Our firm does not maintain custody of customers' funds or securities, which are maintained at our clearing firm, Pershing, LLC. 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, and if our Internet access is available, our firm will post on its website that customers may access their funds and securities by contacting Pershing, LLC, Post Office Box 2065, Jersey City, New Jersey 07303-2065, telephone (213) 624-6100, ext. 500 and facsimile (201) 413-5368. The firm will make this information available to customers through its 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.

Rules: *FINRA Rule 3510(a);*
Securities Exchange Act Rule 15c3-1; 15 U.S.C. 78eee (2003).

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 16414 San Pedro, Suite 930, San Antonio, Texas, 78232. David D. McNally, President, (210) 545-7080 and Barrett Schultz, Chief Compliance Officer, (210) 394-8513 are both responsible for the maintenance of these books and records. Our firm maintains the following document types and forms that are not transmitted to our clearing firm: Customer new account forms and associated documents.

The firm maintains its back up and data protection of all online electronic correspondence records with SMARSH. SMARSH hosts and archives all electronic correspondence (e-mails). SMARSH has multiple locations through the world and can be reached at www.smarsh.com or 1-866-SMARSH-1 (866)-762-7741.

The firm utilizes ShareFile for its secure server backup. The server is backed up nightly and is accessible from any secure device and or computer. ShareFile also has multiple locations through the world and they can be reached at www.ShareFile.com or 800-441-3453

Rule: FINRA Rule 240.17a-4(f).

In the event of an internal or external SBD that causes the loss of our paper records, we will physically recover them from our back-up at ShareFile. If our primary site is inoperable, we will continue operations from our back up site or an alternate location. For the loss of electronic records, we will either physically recover the storage media or electronically recover data from our back-up site, or, if our primary site is inoperable, continue operations from our back-up site or an alternate location.

Rule: FINRA Rule 3510(c)(1).

VIII. Financial and Operational Assessments

Operational Risk

In the event of an SBD, we will immediately 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 firm's website, telephone and voice mail with Time Warner Cable, and email through SMARSH. In addition, we will retrieve our key activity records as described in the section above, Data Back Up and Recovery.

Rules: FINRA Rules 3510(c)(3) & (f)(2).

Financial and Credit Risk

In the event of an SBD, the firm 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. If we cannot remedy a capital deficiency, we will file appropriate notices with our regulators and immediately take appropriate steps.

Rules: FINRA Rules 3510(c)(3), (c)(8) & (f)(2).

IX. Mission Critical Systems

Our firm's "mission critical systems" are those that ensure prompt and accurate processing of securities transactions, including order taking, entry, 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. More specifically, these systems include: all the systems provided by Pershing, LLC, through access to NetExchange Pro™ www.netxpro.com.

The firm has primary responsibility for establishing and maintaining the business relationships with our customers and has sole responsibility for our mission critical functions of order taking, entry and execution. Our 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.

Our clearing firm contract provides that our clearing firm will maintain a business continuity plan and the capacity to execute that plan. Our clearing firm represents that it will advise us of any material changes to its plan that might affect our ability to maintain our business and presented us with an executive summary of its plan, which is attached as at the end of this document. In the event our clearing firm executes its plan, it represents that it will notify us of such execution and provide the firm with equal access to services as its other customers. If we reasonably determine that our clearing firm has not or cannot put its plan in place quickly enough to meet our needs, or is otherwise unable to provide access to such services, our clearing firm represents that it will assist us in seeking services from an alternative source.

Our clearing firm represents that it backs up our records at a remote site. Our clearing firm represents that it operates a back up operating facility in a geographically separate area with the capability to conduct the same volume of business as its primary site. Our clearing firm has also confirmed the effectiveness of its back up arrangements to recover from a wide scale disruption by testing, and it has confirmed that it tests its back up several times each year.

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. Our clearing firm has the following SBD recovery time and resumption objectives: recovery time period of four hours; and resumption time of the same business day.

a. The Firm's Mission Critical Systems

Order Taking

Currently, our firm receives orders from customers via telephone, facsimile, email, and in-person visits by the customer. During an SBD, either internal or external, we will

continue to take orders through any of these methods that are available and reliable, and in addition, as communications permit, we will inform our customers when communications become available to tell them what alternatives they have to send their orders to us. The firm's customers will be informed of alternatives by telephone. If necessary, the firm will advise its customers to place orders directly with our clearing firm at Pershing, LLC, Post Office Box 2065, Jersey City, New Jersey 07303-2065 at telephone number (213) 624-6100, extension 500 and facsimile at (201) 413-5368.

Order Entry

Currently, the firm enters orders by recording them on paper and electronically and sending them to our clearing firm electronically or telephonically.

In the event of an internal SBD, we will enter and send records to our clearing firm by the fastest alternative means available, which include telephone and facsimile. In the event of an external SBD, we will maintain the order in electronic or paper format, and deliver the order to the clearing firm by the fastest means available when it resumes operations. In addition, during an internal SBD, we may need to refer our customers to deal directly with our clearing firm for order entry.

Order Execution

The firm currently executes orders by electronic transmission through Net Exchange Pro™. They can be contacted at www.netxpro.com. In the event of an internal SBD, the firm will execute orders through mobile telephone and facsimile. In the event of an external SBD, the firm would utilize mobile telephone and facsimile.

Other Services Currently Provided to Customers

We do not currently provide any other services to customers not already covered by the preceding procedures.

b. Mission Critical Systems Provided by Our Clearing Firm

Our firm relies, by contract, on our clearing firm to provide order execution, order comparison, order allocation, and the maintenance of customer accounts, delivery of funds and securities, and access to customer accounts.

Rules: FINRA Rules 3510(c) & (f)(1).

X. Alternate Firm Communications Among Customers, Employees, and Regulators

Customers

We now communicate with our customers using the telephone, email, the firm's web site, facsimile, U.S. postal mail, and in-person visits at our firm or at the other's location. In the event of an SBD, we will assess whatever means of communication are still available to us, and use the means closest in speed and form 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 email but the Internet is unavailable, the firm will call the party on the telephone and follow up where a record is needed with paper copy via the U.S. postal mail.

Rule: FINRA Rule 3510(c)(4).

Employees

We now communicate with our employees using the telephone, email, and in-person visits at our firm or at the other's location. In the event of an SBD, we will assess whatever means of communication are still available to us, and use the means closest in speed and form to the means that we have used in the past to communicate with the other party. We will also employ a call tree so that senior management can reach all employees quickly during an SBD. The call tree includes all staff home and office phone numbers. We have identified persons, noted below, who live near each other and may reach each other in person:

The person to invoke use of the call tree is David D. McNally, President of McNally Financial Services Corporation.

Caller	Call Recipients
David D. McNally	All listed on enclosure A

Rule: FINRA Rule 3510(c)(5).

Regulators

We are currently members of the following SROs: FINRA, MSRB. We communicate with our regulators using the telephone, email, facsimile, U.S. postal mail, and in-person visits at our firm or at the other's location. In the event of an SBD, we will assess whatever 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.

Rule: FINRA Rule 3510(c)(9).

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

Business Constituents

The firm has contacted 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. See the firm's major suppliers on the Vendor List Enclosure©.

Rules: FINRA Rule 3510(c)(7).

Banks

The firm has contacted our banks and lenders to determine if they can continue to provide the financing that we will need in light of the internal or external SBD. The bank maintaining our operating account is: Comerica Bank, 13750 San Pedro, San Antonio, Texas 78232. The bank can be reached at (210) 277-3123 or (800) 925-2160.

The firm does not maintain a Proprietary Account of Introducing Brokers/Dealers (PAIB account).

Rules: FINRA Rule 3510(c)(7).

Counter Parties

The firm has 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 or 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.

Rules: FINRA Rules 3510(a) &(c)(7).

XII. Regulatory Reporting

Our firm is subject to regulation by: FINRA, SEC, MSRB, and the Texas State Securities Board. We now file reports with our regulators using paper copies in the U.S. mail, and electronically using fax, email, 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.

Rule: FINRA Rule 3510(c)(8).

XIII. Disclosure of Business Continuity Plan

The firm discloses, in writing, a summary of its Business Continuity Plan to customers at account opening and annually. The firm also posts the summary on our web site and by U.S. postal mail, to customers upon request. The firm's BCP 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 citywide 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) provides general information on our intended

response. The firm's BCP summary discloses the existence of back up facilities and arrangements.

Rule: *FINRA Rule 3510(e).*

XIV. Updates and Annual Review

Our firm will update 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 Business Continuity Plan annually, on June 30th, to modify it for any changes in our operations, structure, business, or location or those of our clearing firm.

Rule: *FINRA Rule 3510(b).*

XV. Senior Manager Approval

I have approved this Business Continuity Plan as reasonably designed to enable our firm to meet its obligations to customers in the event of a Significant Business Disruption.

Rule: *FINRA Rule 3510(d).*

McNally Financial Services Corporation

Signed: 

Name: David D. McNally

Title: President

Date: July 20, 2016

Pershing LLC, a BNY Mellon company

Contingency Planning
Executive Summary

January 2016

Pershing®

BNY MELLON

Table of Contents

Purpose....1
Goal....1
Basic Assumptions....1
Incident Management Structure....1
- Incident Management Team....2
  - IMT Executive Commanders....3
  - IMT Coordinators (Incident Facilitation)....3
  - Business Unit Operations....3
  - Client/External Representation....3
  - Corporate Support Services....3
  - Technology....3
- Response Teams....3
- Business Units....4
  - Line Managers....4
  - Business Continuity Team Captains....4
  - IMT Liaison....4

Communications With Clients....4
- Outbound Communications....4
- Inbound Communications....4

Security Policies....4
- Data Security....4
- Physical Security Access....4

Business Continuity (People and Processes)....5
- Business Continuity Plans and Risk Assessments....5
- Geographically Dispersed Processing....5
- Alternate Work Sites....5
- Testing....5

Disaster Recovery (Technology)....6
- Overview....6
- Sites....6
- Systems....6
- Plans and Testing....6

Purpose

The purpose of this document is to provide Pershing's clients 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.

Goal

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

Basic Assumptions

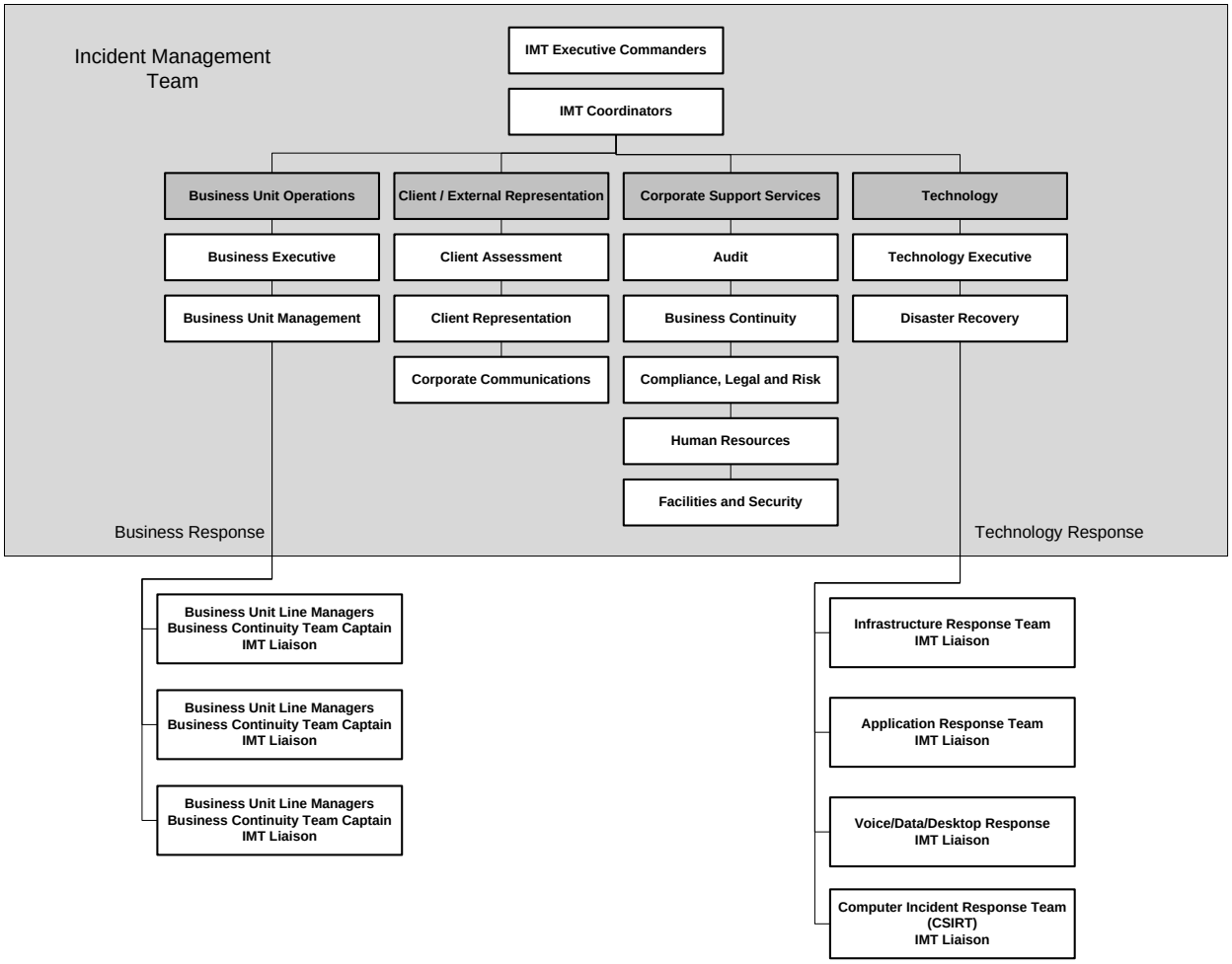
The business continuity plan is based on the following assumptions:

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.
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. We anticipate that in the event of an interruption affecting one of our facilities, our remaining processing facilities will continue to provide uninterrupted service while the critical staff from the affected site relocates to an alternate facility. However, depending on the severity of the interruption, there may be a slight degradation of our services during this time.
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 critical industry utilities and counterparties (such as the Depository Trust & Clearing Corporation [DTCC], Security Industry Automation Corp. [SIAC], etc.) are operational.
6. Pershing assumes that it will have adequate staffing available during the event.
7. Pershing assumes that client-supplied data communication lines between the client and Pershing's primary and alternate data centers are redundant.

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 declared 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.



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, client-focused perspective. The IMT:

- Obtains the operational statuses of business and technology departments and the client liaison teams
- 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 Account Management, Relationship Management and Corporate Communications personnel
- Manages the incident and recovery activities through closure
- Documents post-event analyses and findings

IMT Executive Commanders

- Liaison to the Executive Committee
- Focal point for decision-making and the execution of strategies for the IMT
- Coordinates activities at the corporate, business and technology unit levels

IMT Coordinators (Incident Facilitation)

- Launches notification to IMT members, structures meetings, documents meeting minutes, etc.

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

Client/External Representation

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

Corporate Support Services

- Liaison to industry and regulatory agencies
- Provides information on impact of the incident
- Supports and facilitates the firm's contingency actions
- Ensures implemented contingency actions are compliant with laws, rules and regulations, and provide sufficient controls
- Manages Pershing employee notifications

Technology

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

Response Teams

Pershing's technology group has dedicated teams of technicians to advise on and respond to events, as directed by the IMT. These teams are organized by area of expertise and relevant skill sets.

Business Units

Each of Pershing's business units has dedicated teams of employees 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 develop the business continuity and test plans and perform testing. 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.

Communications With Clients

Outbound Communications

The business unit subject matter expert and a representative(s) member(s) of Pershing's Global Client Relationship Management teams will work with the Client Communications team within Corporate Communications to contact clients with information or instructions via an appropriate communications forum.

Inbound Communications

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

- Global Client Relationship Management, (primarily Account Managers and Client Service) will answer general status questions.
- Clients who wish to notify Pershing of technology problems will continue to call Pershing's Technology Client Service at (888) 878-3142 within the U.S. and (732) 622-2150 outside the U.S.

Security Policies

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.

Physical Security Access

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

- Only Pershing employees and authorized vendor support personnel will be allowed access to the facility and all access will be monitored. All employees will be required to show a valid Pershing identification card and authorized vendor support personnel will be required to sign in with Corporate Security personnel 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 Corporate Security, and only if all designated approvals from accompanying department directors, senior managers, or both, are in place.
- Corporate Security will maintain an up-to-date database of all approved employees with programmed card access rights and a sign-in authorization listing for privileged access to these

restricted areas.

- Any access required by employees, vendors or consultants will require approval by their department's senior manager 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.

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 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.

Business Continuity Plans and Risk Assessments

Consistent with Financial Industry Regulatory Authority® (FINRA®) Rule 4370, 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. While Pershing plans for events of varying impact, not all events with the potential to impact our business can be anticipated. 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 clients.

Current copies of Pershing's business continuity plans are maintained within each business unit, as well as in a repository on the internal network.

Geographically Dispersed Processing

Pershing operates multiple redundant processing centers in New Jersey, California, Central Florida, Pennsylvania and Chennai, India. 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.

Alternate Work Sites

Pershing maintains alternate work sites for critical staff that, when combined, accommodate the relocation of over 650 trading, processing, client service and application development personnel. Each operations desktop or trading position is outfitted with the required application software, requisite network access and telecommunication equipment.

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

Testing

Geographically Dispersed Processing

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

Alternate Work Sites

Workstations at the alternate work sites are tested at least twice annually during normal business hours. These tests involve the performance of daily production activities by the business units at the alternate site. Remote access testing may also be performed during the annual production from alternate work site test by authorized staff.

Disaster Recovery (Technology)

Overview

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

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 U.S. (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.

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-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 clients 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.

Plans and Testing

Pershing's disaster recovery plans and testing programs fully comply with FINRA Rule 4370.

The disaster recovery team is responsible for coordinating 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 address business, technology, audit and compliance requirements. Tests are internal, client-facing or industry-facing (or both) in scope, and include participation from internal users, our clients, vendors, utilities and/or exchanges. 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 clients are invited and encouraged to participate in these important exercises.