



**USAID**  
FROM THE AMERICAN PEOPLE

# RECOMMENDATIONS FOR IMPROVING THE COMPLIANCE OF THE JORDANIAN FINANCIAL SERVICES FIRMS

June 17, 2008

This publication was produced for review by the United States Agency for International Development. It was prepared by Karen Steffens/ Subcontractor to BearingPoint Inc.

# **RECOMMENDATIONS FOR IMPROVING THE COMPLIANCE OF THE JORDANIAN FINANCIAL SERVICES FIRMS**

USAID JORDAN ECONOMIC DEVELOPMENT PROGRAM (SABEQ)

CONTRACT NUMBER: 278-C-00-06-00332-00

BEARINGPOINT, INC.

USAID/OFFICE OF ECONOMIC GROWTH

JUNE.17, 2008

AUTHOR: KAREN STEFFENS

DELIVERABLE NO: 1.4.1.9.11.1 DIAGNOSTIC OF CURRENT  
COMPLIANCE REGIME AND RECOMMENDATIONS TO IMPROVE  
PROCESS.

## **DISCLAIMER:**

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

# CONTENTS

GLOSSARY OF TERMS AND ACRONYMS.....	1
ACKNOWLEDGEMENT.....	2
EXECUTIVE SUMMARY.....	3
BACKGROUND AND SOW.....	4
OBJECTIVES .....	5
METHODOLOGY .....	6
CONCLUSION:.....	12
APPENDICES.....	13

## **GLOSSARY OF TERMS AND ACRONYMS**

CO: Compliance Officer

The Instructions: Instructions of Financial Services Licensing and Registration for the Year 2005

JSC: Jordan Securities Commission

LID: Licensing and Inspections Department of the JSC

SABEQ: USAID Jordan Economic Development Program

SOW: Scope of Work

## **ACKNOWLEDGEMENT**

The author wishes to acknowledge the support of the SABEQ Team who committed their time and resources to all aspects of the review process.

My sincere thanks to all members of the LID and in particular to Ms. Amal Zayad, Saleh Fleifel, Lana Nsour and Khaled Jaber for providing extensive information and assistance regarding the compliance and inspections process.

## **EXECUTIVE SUMMARY**

In an effort to increase investor confidence and market integrity, the Jordan Securities Commission is seeking to raise the proficiency standards for compliance officers responsible for the regulatory aspects of the financial services firms.

Based on meetings with regulatory staff and financial industry officials as well as research and analysis conducted by the SABEQ Capital Markets Advisor, the following key actions by the JSC (with SABEQ assistance, if the JSC wishes) are recommended:

- Conduct training with the compliance officers and senior managers of financial services companies to codify the role of the compliance officer
- Prepare a workshop that provides guidance to compliance officers in preparing the compliance manual required under Article 68 of the Instructions.
- Provide tools for the Inspections and Licensing Department of the Jordan Securities Commission (“JSC”) to improve the process of examining companies and management’s oversight of those reviews. These tools may include developing examinations modules, providing additional technical training and creating databases containing comprehensive examination and investigation information.

To launch the process, a compliance workshop presentation and reference material were provided to the JSC on June 11 and 12, 2008 that specifically addressed the first two recommendations. Implementation of these first two recommendations with financial industry counterparts should be conducted immediately so there will be no additional delay in meeting the regulatory requirement.

## **BACKGROUND AND SOW**

The USAID Jordan Economic Development Program (“SABEQ”) is working with the Jordan Securities Commission (“JSC”) as part of its initiative to develop the financial sector in Jordan through its various segments including the capital market. The objective of SABEQ activities with the JSC is to accelerate business expansion through private sector access to non-bank sources of funding, and to build investor confidence in the Jordanian capital market.

In order to further the goal of building investor confidence, the JSC adopted Article 68 of the Instructions of Financial Services Licensing and Registration for the Year 2005 (“the Instructions”). According to the Instructions, financial services companies (“FSCs”) are obligated to appoint a compliance officer (“CO”) to ensure that the law and all regulations of the capital market are observed. Thereafter, the Board of Commissioners issued minimum qualifications for the CO and stated that a CO should complete a training course and accreditation before being acknowledged as a CO for the financial services company. The JSC implemented the instructions related to the compliance officer and gave the first training in late 2006.

While this initial training provided the articles and directives that FSCs needed to comply with the securities law, the JSC believed there was a need to improve the training given to COs prior to their accreditation.

Based on meetings with key capital markets stakeholders at the JSC there were several expectations placed on this consultancy. First, and as outlined in the Statement of Work (“SOW”), the JSC seeks an improved training program for the COs. Second, the JSC requested that a compliance manual be developed for COs. Third, the JSC seeks to empower the inexperienced COs and to familiarize them with both the law and with compliance best practices. Finally, the JSC wants Senior Management at the FSCs to have a clear understanding of the role of CO. This lack of clarity on behalf of FSCs’ senior managers has resulted in the diminished authority of COs and rendered the position less effective than intended.

## **OBJECTIVES**

To align the Statement of Work as outlined by SABEQ with the additional requirements outlined to the Advisor during these meetings, it was determined, with the approval and authorization of JSC officials that (1) a training workshop would be provided to JSC staff that would instruct COs in developing their compliance manual (train-the-trainers), (2) this training workshop would also provide instruction regarding compliance best practices that in turn could be provided to COs (train-the-trainers) and (3) the training workshop would address empowering the CO. JSC counterparts were provided an outline of the workshop and requested to make comments or changes on content (See Appendix A). This workshop “Compliance Basics Workshop” was presented to JSC staff on June 11 and 12, 2008 and is included as an enclosure with this report. Also included as an Appendix to this report is the reference materials provided to workshop participants approximately four days prior to the workshop. Fieldwork for the assessment and training was undertaken from May 21 through June 17, 2008.

## **METHODOLOGY**

To assist in developing recommendations and the resulting training program for COs, the Advisor adopted the following methodology to accomplish the stated goals:

Meetings were conducted in Jordan with various JSC departments, officials from the Securities Depository Company (“SDC”) and the Amman Stock Exchange and several FSC senior managers during May 25 through June 10. Additionally, the Advisor interacted with Licensing and Inspections Department (“LID”) personnel during the term of the consultancy on a continuous basis. This proved to be a valuable exercise not only in trust building, but it also allowed the consultant to observe the daily routine of the examiners. While the examiners conducted their business in Arabic, the Advisor was still privy to the daily dynamics of the department. Additionally, this provided the Advisor with immediate access to staff for questions and inquires. Documents gathered and analyzed during the term were directive-based documents and an electronic file provided by SDC that included a presentation and related materials. The previous JSC presentation offered to COs was also provided to the Advisor but was not translated. JSC staff indicated that this training provided only for the rules and a description of JSC departments. An examination memorandum or report was not requested by the Advisor to be translated but, in retrospect, this would have been a useful document for review.

Based on the feedback received during these meetings, personal observation and subsequent analysis, recommendations for improvements related to compliance officer training and implementation are described below

## **SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS**

The following section presents a summary of the findings and related recommendations resulting from review of the current compliance training and meetings with counterparts. The findings and recommendations are related to three principal areas including development of the compliance manual, additional training for COs and financial services firms and, general recommendations for improvements within the LID and JSC:

### **Training for CO's and Financial Services Companies Officers**

1. Role of the Compliance Officer and Empowering the COs. Most COs were hired in response to the regulatory initiative contained in Article 68 of the Instructions, requiring FSCs to retain a CO. These COs are often recent business, finance or accounting graduates with little or no experience in the brokerage industry and unsure of their responsibilities. Because of this, the COs are uncertain as to how to proceed with the JSC's intended mission for them or what their role is within the organization. Equally important, senior management of FSCs that employ these COs are also unclear of the requirements of the CO position. COs may not be granted the authority necessary to carry out the compliance function nor may certain COs be allowed to participate in policy making decisions for the organization that employs them. Too often the COs are given other clerical duties in addition to their compliance duties. In a small firm, this may not be significant but in a medium to large firm it may impede the development of the compliance function. To assist with the increasing the visibility of the CO, the following course of action is recommended
  - Require the position of CO to be a senior position preferably a "Chief" position. In this way, the CO may be more likely to be involved with policy decisions at the organization. Or, the JSC may choose to relax requirements and allow the CO or CCO to be General Counsel (if an attorney), a principal in the Internal Audit Department or even the Financial Controller. This will allow the CO to perform multiple yet similar, high level functions.
  - Conduct a training session with senior management of all financial services firms and brokerages explaining the role of the compliance officer (see workshop slides 2 through 10) and senior management's role in creating a culture of compliance (see workshop slide 11). During this training, senior management will be

encouraged by the JSC to elevate the CO position if not in title, then in purpose. This training can be conducted with the cooperation of the Legal, Monitoring and Inspections departments, all of which have an interest in developing a culture of compliance and promoting ethics at the highest level of the organizations.

- Conduct training with COs. In addition to what is provided to the senior management of the FSCs (see above), training should also be offered regarding the basics of risk management (see workshop slides 12 through 13) and development of the CO manual (see workshop slides 14 through 87)
  - Advanced training. Sessions should be provided for more experienced COs as well as JSC staff. This educational effort could be provided by local or international trainers or by translating Webcasts and Podcasts offered by FINRA.
2. New initiatives: Information dissemination and training. To ensure full assimilation of all new initiatives, including the compliance officer and manual initiative, notices, bulletins or circulars should be published to clarify interpretations of the laws and directives. Many of the JSCs directives are, in fact, written in “plain English/Arabic,” thus are relatively easy to understand. However, regulatory agencies have never been accused of providing too much information to its constituents. Issuing informational or regulatory bulletins can only facilitate the understanding by FSCs and COs as to their responsibilities under the law. Importantly, if a requirement falls under commercial law instead of securities law, it can be outlined by the JSC as a requirement of their regulatory program as well as the trade and commerce laws.

Training should be implemented for all new initiatives including systems like the financial reporting system which was recently introduced as a way for FSCs to transmit their weekly financial data electronically. Staff resources are spent with individual one-on-one effort with the FSCs to ensure that firms have passwords, logins and can navigate the system. While this effort may ensure a higher success factor, it may also drain the limited resources of the department. Training for these types of initiatives should be conducted as a workshop and taught as a single event with the assistance of other departments, if applicable. Also, this example illustrates the benefit of issuing informational and interpretative bulletins.

## **Development and Implementation of the Compliance Manual**

While the requirement for FSCs to have a compliance manual has been in place for at least two years, the FSCs have not actively created their manuals. It has been suggested by JSC staff that international experts, with JSC input, produce the manual for the FSCs. If this approach were followed, all FSCs would have the same compliance manual, mandated by the JSC.

However, there are multiple reasons and benefits to having the manual developed firm-by-firm, in-house, by each CO. First, a compliance manual is not a “one size fits all” endeavor. Firms have different business model and organizational structures, and therefore different risks and compliance parameters. While one set of procedures may be entirely suitable for one FSC, it may be completely inadequate for another. Also, the purpose and intent behind Article 68 was to provide additional investor and market protections and not proposed as a draconian measure with inflexible edicts required by a regulator’s version of the manual. The intent was to have the FSCs conduct an insightful review of their organizations, with an eye to promoting both business and thoughtful regulation. This is unlikely to occur if a particular manual is mandated and created by the JSC. Additionally, one of the goals of the consultancy was to provide input for empowering the CO. There may be no better means for the CO to gain self-empowerment than if a CO creates, develops and delivers their own manual to the organization. If the CO were to have a compliance manual that merely allowed for them to fill in the blanks, the ability to gain valuable experience from the process of compliance development would be diminished.

That being said, there are advantages to the CO and JSC if “minimum standards” templates are developed and furnished by the JSC on global matters such as anti-money laundering and insider trading. Many of the templates that are currently used by US regulators and/or COs were provided during the workshop as reference materials and could be re-designed for use by the JSC.

A workshop for COs such as the one delivered to the JSC during the consultancy and as described above would assist in the development of the manual and provide clarity to the participants.

### Alternatives to compliance manual creation by the CO and in-person workshops

- As discussed above, the JSC may use the reference materials provided in the compliance workshop to create a “minimum standards” manual. The CO would be responsible for completing the manual with any additional risks and procedures necessary for full compliance with laws. This method should be introduced with a workshop for the COs with essentially the same elements discussed in the compliance workshop.
- Development of the manual can be entirely outsourced to technical experts. This method is not recommended but is included only because it is a potential alternative, albeit one that, in my opinion, would provide the least value to the COs and FSCs. Even with this alternative, implementation must include a workshop devoted to the material presented in the manual.
- As an alternative to in-person workshops, videos can be created in English with Arabic sub-titles or entirely in Arabic that can provide the instruction that was offered during the workshop of this consultancy. While this alternative is not interactive and thus not the ideal form of delivery, it allows for greater flexibility for recipients as well as the possibility for these videos to become part of the library for the Institute of Financial Studies once the Institute is realized. As a less expensive and more flexible alternative to videos, “e-briefings” (essentially PowerPoint slides with voice-overs) can be created in modular format. Each required participant can watch the e-briefing at his/her own workstation. Brief tests can be inserted into these e-briefings, with minimum scores in order to pass to the next e-briefing, and viewings and results of the tests can be electronically monitored.

### Recommendations associated with general review of the Licensing/Inspections

#### Department and the JSC

- **Administrative Recommendations**

**Examinations manual.** The Inspections and Licensing Departments of the JSC have procedures but not an operational inspection or examination manual. The examination manual could provide chapters or modules in areas such as internal controls, anti-money laundering, customer accounts, disclosure, books and records; insider trading etc. that

would provide objective and equivalent standards for inspections. Furthermore, exam modules would provide new examiners with needed training materials.

**Job description.** Examiners would benefit from a job description to align expectations with their actual responsibilities and functions. The descriptions could include various positions within the department depending on experience, education or job skills allowing for a career path and potentially pay grade increases. For example an examiner with 5 to 10 year experience within the department could be designated as a Senior Examiner with more supervisory oversight than the Examiner title with 0 to 5 years experience.

**Centralized Database of Inspections, Investigations and Examinations.** Currently the Inspections and Licensing Department maintains a limited scope database of FSCs that is used primarily as an examination scheduling tool. A centralized database, that crosses several departments would provide all JSC management with a useful tool for determining not only inspections schedules but also particular regulatory problems at firms, completion time of investigations/examinations, when and why matters are referred to other departments, examination focus areas of investigations/examinations etc. This would be an internal data management tool and not necessarily part of any current electronic initiative.

**Training for JSC staff and their counterparts.** A common theme expressed by most departments was the need for additional training in technical areas. JSC staff indicated interest in topics such as options and other derivatives trading, financial statement analysis and net capital computation and adequacy. There were also requests for training programs for judges and prosecutors regarding securities related issues. Additional training can be provided by local or international experts but should be timely and mandatory if provided.

**JSC Jurisdictional Issue.** There exist in Jordan multiple financial and brokerage firms that are currently unregulated by the JSC, or any other authority, merely because those firms trade international securities or securities not traded on the Amman Stock Exchange. Apparently this issue is under review by the industry and JSC officials and/or Commissioners. Therefore, discussion here is limited to a strong recommendation to have the JSC resolve this jurisdictional issue to have authority over these unregulated

## **CONCLUSION:**

The JSC has taken the initial steps to improve the stature of Jordan's newly assigned COs. However the JSC recognizes that the training must be enhanced and provided not only to COs but also to senior managers of FSCs. In order to ensure the successful implementation of the compliance function and the required manual, it is recommended that:

- Additional training be provided for COs and senior managers of financial services companies describing the role of the compliance officer
- Guidance be provided to compliance officers in preparing a compliance manual. While in-house development of the manual is the most desirable method, alternatives may also be employed.
- Bulletins and circulars that communicate new initiatives as well as current, amended and interpretations of the law should be provided as a means of educating the industry.
- Development of an inspections manual

The JSC should continue its vigorous effort to educate the financial community it regulates while increasing the tools JSC staff require to effectively regulate the marketplace.

# APPENDICES

## Workshop for JSE Examiners – The Compliance Function at Brokerage Firms

### Draft Outline and Topics

#### I. Role of the Compliance Officer (“CO”)

- Develop a culture of compliance.
- Uphold the securities laws
  - Ethical Issues vs. laws
- Identify risk areas, internal control issues and conflicts of interest.
- Educate all organizational staff to ensure they are familiar with securities laws.
- Create a manual to guide the firm, employees and CO with conduct consistent with the securities laws of Jordan.
- Primary contact between the regulators with the firm.
- Update personnel with any new regulations - provide advice and counsel
- Act as a primary consultant within the organization for all matters effecting the organization including hiring and firing, establishing new lines of business, IT/clearing firm/operational matters.
- Take corrective action immediately when violations or potential violations are discovered by the CO.

#### II. Developing and Examining a Compliance Program

- Will include a document discussing the elements of an effective compliance program including risk assessment

#### III. Preparing the Compliance Manual

- The starting point: the Firm’s registration and the securities laws/directives
- Begin with the Table of Contents - example will be provided
- Consider the Firm’s business model
- Consider all the risks uncovered in the exercise of developing a compliance program, those should be detailed and mitigated by procedure in the manual.
- A sample will be provided of:
  - Attestation page
  - Table of contents
  - Business description

- Organizational Chart: officers, traders, assistants, etc.
- Template of a Firm-specific procedure
- FINRA – checklist of written supervisory procedures

#### IV. Compliance Manual Basics

- Internal Controls: will vary for Firms. COs should perform the exercise described in II. in order to understand their potential control issues. Examples may include:
  - Proprietary trading – Employee Personal Trading
  - Too few personnel with too many types of responsibility
  - Ability to override systems
  - Personal relationships between customers and brokers
  - Affiliated businesses or subsidiaries
- Anti-Money Laundering Program and Customer Information Program (AML/CIP) – example will be provided
- Insider Trading – example will be provided
- Business Continuity Plans (BCP) – example will be provided, many US exams have discovered that firms
  - Failure to prepare for, and test operations during human or natural emergencies;
  - Failure to provide for availability of critical personnel and systems;
  - Failure to verify continuity plans of third party providers; and
  - Failure to protect records from unplanned destruction.
- Financial Controls - staff to provide the workshop material
  - Solvency
  - Artificial transactions to boost solvency ratios
  - Margin Requirements
- Books and Records –maintenance requirements – will provide sample of requirements used in the USA
  - Financial Records
  - Phone records – recording
  - Email and instant messaging – currently no specific requirement to maintain or review – discussion item with examiners
  - Trade records – order tickets, cleared trade records etc.
  - Customer Account records - opening documents, authorizations, verifying customer information, account statements, confirms etc.

- Systems issues: systems are not robust and do not maintain proper date/time code
- Sales practice basics
  - Suitability and recommendations
  - Misappropriation of customer funds
  - Addressing customer complaints
- Best Execution
  - Brokers have a fiduciary responsibility to provide customer orders with the best execution.
- Failure to provide or produce information for the Regulator

#### V. Tools for compliance and best practices

- Document, Document, Document!
- Review of the regulator's website (JSE, ASE, SDC)
- Review of other regulators' websites including FINRA's disciplinary actions see [www.finra.org](http://www.finra.org)
- Become a member of an association
- Take training – while may not always be available in Arabic there are short programs that could be easily translated (see [www.finra.org](http://www.finra.org) )
- Review the completed compliance manual at least once a year
- Communication - regular compliance meetings with brokers and salespeople
- Reports to management
  - Require an annual meeting with the CEO to discuss compliance matters
  - Provide quarterly reports of regulatory issues to senior management
- Test and Audit areas of compliance manual and procedures
- Continuing Education for all personnel
- When a violation is discovered, CO must act.
- CO must be firm in their delivery of requirements – if the CO has any problem being persistent, dealing with conflict or acting as the “bad guy” this may be the wrong job for them. These same qualities need to be present in examination staff.

VI. Additional Topics (if time permitting)

1. Case Studies – Recent examples of how/when things go bad
  - a. Deep, systemic insider trading violations by Michael Guttenberg, a UBS trader and more importantly, Randi Collotta, a compliance officer
  - b. Poor Internal Controls by Societele Generale in connection with trading activity of its trader Jerome Kerveil
  - c. Misuse of customer funds by FINRA Board member



## USAID Jordan Economic Development Program (SABEQ)

### COMPLIANCE MANUAL BASICS WORKSHOP

JUNE 11-12, 2008

The purpose of this workshop is to provide the staff of the Jordan Securities Commission (“JSE”) with the basic instruction necessary to present a compliance workshop to Jordanian compliance officers employed at brokerage firms. Specifically, this workshop will address how to develop a compliance program at a brokerage/securities firm and the minimum standards required for a compliance manual.

#### PRE-WORKSHOP DOCUMENTS

##### A. Background: Developing a Compliance Program

##### B. Sample Documents

1. Financial Industry Regulatory Authority (“FINRA”) Checklist (cover and page 1 only)
2. Table of Contents, Attestation, Business Description
3. Organizational Chart
4. Anti-Money Laundering Procedure
5. Anti-Money Laundering Training
6. Insider Trading Procedure
7. Business Continuity Plan
8. Books and Records Maintenance Schedule
9. Firm-Specific Procedure: Error Accounts

##### C. Case Studies – Current Compliance Topics

1. Guttenberg – Insider Trading
2. SocGen – Internal Controls
3. Goble/NACI- misuse of customer funds

#### WORKSHOP HOMEWORK

To prepare for a workshop exercise, participants are encouraged to read “Background – Developing a Compliance Program” and “Firm-Specific Procedure: Error Accounts.” Before the workshop, participants are asked to prepare a brief document describing how they would guide compliance officers in preparing the *capital adequacy* and *margin* sections of the compliance manual.

WRITTEN SUPERVISORY PROCEDURES MANUAL (“WSP”s)  
COMPLIANCE MANUAL

Firm Name Here

These written supervisory procedures were approved by (name here), Compliance Officer. These procedures are effective from the date approved until the date of their authorized revision, update or replacement (see below).

Authorized Approval Signature:

Date these procedures became effective: **(Date here)**

Date these procedures were no longer effective (date of revision, update or replacement): **Revised (revised date here)**

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

## **ACKNOWLEDGMENT OF PRINCIPALS, ASSOCIATED PERSONS AND SUPERVISORY PERSONNEL**

The undersigned recipient of this Written Supervisory Procedures Manual acknowledges that he/she has received the Manual, is responsible for knowing its contents and has read and understood its contents to the level of being able to put its principles into practice. The undersigned understands that the Manual is continually updated and agrees to take responsibility for obtaining, reviewing and understanding any updates or supplements published or distributed by *Firm name here* ("THE FIRM.")

Included in this Manual are special Firm Policies on the following subjects:

- SUPERVISION AND COMPLIANCE
- DESIGNATION OF PRINCIPALS
- LICENSING
- REGISTERED REPRESENTATIVE AND ASSOCIATED PERSON CONDUCT
- OUTSIDE BUSINESS ACTIVITIES AND PRIVATE SECURITIES TRANSACTIONS
- MONITORING OF TRADING
- PERSONAL ACCOUNTS AND TRADING
- INSIDER TRADING, ANTI-MONEY LAUNDERING, BANK SECRECY
- ADVERTISING
- RECORD KEEPING AND REPORTING
- SUPERVISORY CONTROLS
- CERTIFICATIONS
- COMPLAINTS

The undersigned acknowledges by his/her signature on this page he/she has read and understands all THE FIRM policies and procedures contained in this Written Supervisory Procedures Compliance Manual, and is responsible for abiding by their provisions.

---

Name

---

Signature

---

Date

**Firm Name Here**

**List of Officers, Registered Persons, and Supervisory Personnel**

January 1, 2008

President/CEO: Name here

Financial and Operations Principal ("FinOp"): Name Here

Chief Compliance Officer ("CCO"): Name here

Sales Supervisor/Home Office Supervisor  
("SS" or "HOS"): Name here

FINRA Exec. Representative/Registrations Supervisor: Name here

Compliance Registered Options Principal: Name Here

Senior Registered Options Principal: Name Here

This list will be updated at least yearly or upon the occurrence of a significant change.

## **TABLE OF CONTENTS**

### **PART 1: INTRODUCTION AND GENERAL DESCRIPTION OF THE FIRM'S SUPERVISORY PROCEDURES**

#### ***I. FIRM POLICY***

- A. Description of THE FIRM's Business
- B. Supervision Pursuant to the Conduct Rules of FINRA
- C. Firm Statement
- D. Emergency Preparedness and Contingency Plans
- E. Use and Distribution of Manual and Review of WSPs
- F. Services Offered by THE FIRM

#### ***II. SUPERVISORY PERSONNEL***

- A. President/CEO
- B. Chief Compliance Officer
- C. Sales Supervisor
- D. Executive Representative
- E. FinOp and Safeguards of Financial Controls
- F. Review of FinOp
- G. Standards of Supervision
  - 1) Supervisory Review System
  - 2) Independent Function of CCO
  - 3) Qualifications of Supervisory Personnel
  - 4) Overall Supervision
  - 5) Supervision of Home Office Personnel
  - 6) Monitoring of Trading Activity

## **PART 2: WSP CHECKLIST**

### ***I. General Administrative***

#### **A. Form Filing (FINRA RULE 1140)**

- 1) Form BD Amendments
- 2) Form U4/U5
- 3) Fingerprint Cards
- 4) Designation of Executive Representative
- 5) Principals responsible for supervision of form filings

#### **B. General B/D Activities**

- 1) Advertising and Sales Literature; email and Web Sites
- 2) Cold Callers/Telemarketing Scripts
- 3) Correspondence: Incoming, Outgoing, and Electronic
- 4) Institutional Sales Literature and Correspondence
- 5) Customer Complaints
- 6) Material Event and Complaint Reporting
- 7) Errors
- 8) Distribution of Procedures and Amendments
- 9) Gifts and Gratuities
- 10) Outside Business Activities and Personal Trading Accounts
- 11) Periodic Review of Business and Supervisory Systems
- 12) Private Securities Transactions
- 13) Regulation SP
- 14) Speaking Engagements and Scripts
- 15) Books and Records – General Requirements
- 16) Fidelity Bond

#### **C. Registered Rep Activities/Associated Persons**

- 1) All Associated Persons Are Properly Registered
- 2) Investigations of Background and Qualification
- 3) Records for Associated Persons and Assigned Supervisors
- 4) Required Annual Compliance Meeting

- 5) Heightened Supervision and Disqualified Individuals Screening
- 6) Annual written attestation for Associated Persons
- 7) Outside Accounts
- 8) Parking, Sharing, and Lending to Customers
- 9) Use of Exception Reports
- 10) Investment Adviser Activities of Associated Persons
- 11) Products Offered

#### D. Branch Office Activities

#### E. Supervisory Controls

- 1) Designation of Chief Compliance Officer
- 2) CEO's Annual Certification
- 3) Designation of Individual Responsible for Supervision
- 4) Supervisory Procedures to test Firm's WSP
- 5) Supervisory Procedures for Updating WSPs
- 6) Principal Annual WSP Report to Management
- 7) Supervision of Customer Funds Transfers
- 8) Supervision of Customer Information

#### F. Financial Reports/Books and Records

- 1) Maintenance of Financial Books and Records
- 2) Maintenance of Operational Books and Records in General
- 3) Net Capital Rule & Requirements (Withdrawals, Subordinated Loans, Annual Audit)
- 4) Customer Protection Rule
- 5) Financial Reporting: FOCUS
- 6) FINRA Fees and Assessments
- 7) Margin Requirements
- 8) Clearing Agreements

- 9) Bank Secrecy and Reporting Suspicious Transactions
- 10) Taping Rule
- G. Business Continuity Plan
- H. Anti-Money Laundering (“AML”) Procedures

## ***II. Continuing Education***

- A. CE Contact Person
- B. Regulatory Element
- C. Firm Element

## ***III. All Securities Related Activities***

- A. Best Execution
- B. Customer Funds & Designated Securities Use
- C. Discretionary Accounts
- D. Fair Pricing
- E. Investor Education
- F. New Account Review and Approval
  - 1) Opening Accounts for Persons Associated with B/Ds
  - 2) Periodic Customer Account Review
  - 3) Parking of Securities
  - 4) Prohibition against Guarantees
  - 5) Securities Transactions for Personal and Family Accounts
  - 6) New Account Approval
    - 1. Suitability
    - 2. Customer Identification Program (“CIP”)
  - 7) THE FIRM policy regarding Customer documentation
  - 8) Commissions

- G. OATS Requirements
- H. Order Tickets/Confirmations
- I. Research Analysts
- J. Restricted/Controlled Securities
- K. Suitability
- L. Third Party Accounts
- M. Fair Dealing with Customers and the Front running Prohibition
- N. Transactions Involving FINRA and AMEX Employees

#### ***IV. Fixed Income Securities***

#### ***V. Options***

- A. Allocation Procedures
- B. Uncovered Short Options Contracts
- C. Position Limits/Exercise Limits
- D. Reporting Options Positions
- E. Verification of Customers and financial information
- F. Review/Approve New Accounts
- G. Clearing, Confirmations and Delivery of Disclosure Documents
- H. Supervision
- I. Discretionary Accounts
- J. Branch Office Option Business
- K. Maintenance of Records
- L. Customer Grievances/Complaints
- M. Options Communications with the Public

#### ***VI. Investment Firm Products and Variable Contracts***

#### ***VII. Underwriting Activities***

#### ***VIII. Insider Trading***

A. Supervisory Procedures and Firm Policy on Insider Trading

***IX. Trading***

A. ACT Compliance

B. Affirmative Determination (Sort Selling)

C. Alternative Trading Systems and ECNs

D. Confirmation Disclosure

E. Designated Securities

F. Due Diligence

G. Fair Pricing

H. Firm Quote/Backing Away

I. Front Running/Trading Ahead of Research

- 1) Unusual Trading Patterns
- 2) Block Trade Reports
- 3) Complaints/Investigation of Trading

J. Limit/Market Order Handling

K. Locked and Crossed Markets

L. Non-FINRA Securities

M. Order Audit Trail System

N. Order Execution Reports and Order Routing Information

O. Order Ticket/Trade Run procedures

P. Passive Market Making

Q. Payment for Order Flow

R. Position Limits

S. Anti-Competitive Practices

- 1) Pricing and Size Conventions
- 2) Coordination of Quotations
- 3) Anti-Competitive Behavior/Harassment: Firm Statement

- 4) Exchange of Proprietary Information
- 5) Coordination of Market Maker Activities
- 6) Failure to Honor Quotations
- 7) Late/Inaccurate Trade Reporting

V. Prohibition of Payments for Market making

W. Registration of Trading Personnel

X. Short Sales and Short interest Reporting

Y. Stock Volatility

Z. SOES Trading Practices

AA. Trade Reporting

- 1) NASDAQ
- 9) DPP and NNOTC
- 9) SOES and Third Market
- 9) Trading Ahead in CQS Stocks

BB. Trading Halts

- 1) Declared on registered Exchanges
- 2) Withdrawal/Freezing Quotes and Trading

## ***X. Online Trading and Day Trading***

### ***XI. APPENDICES***

- A. Business Continuity Plan
- B. Gifts and Entertainment Policy
- C. Personal Securities Transactions and Outside Brokerage Accounts Policy
- D. Anti-Money Laundering (“AML”) Policy
- E. OATS Procedure
- F. Insider Trading Policy

## **PART 1: INTRODUCTION AND GENERAL DESCRIPTION OF THE FIRM'S SUPERVISORY PROCEDURES**

### **I: Firm Policy**

#### **A. Description of THE FIRM's Business**

##### Overview

THE FIRM became an FINRA member firm on XX, XXXX (Registration number here). THE FIRM is an agency firm that provides execution services to broker dealers, professional traders, institutional clients and hedge funds. THE FIRM does not execute orders on behalf of retail, public customers. THE FIRM is not self clearing and therefore, does not provide clients with a formal account statement or confirmation nor does THE FIRM maintain custody of client assets, funds or securities. THE FIRM does not provide research or recommendations to clients. THE FIRM business model is to broker options and option related transactions on behalf of our clients, locating liquidity and seeking price improvement in the process.

THE FIRM does not: (i) carry or maintain accounts for customers; (ii) receive or hold customer funds or securities; (iii) clear or settle transactions on behalf of customers, i.e. THE FIRM is not self-clearing; (iv) have payment for order flow or soft dollar arrangements; (v) engage in any investment banking, solicitation, underwriting, or private placement activities; (vi) trade options in a proprietary account, or (vii) engage in any other non-securities business.

##### Execution of Options Trades

For option trade execution, THE FIRM utilizes floor brokers on national exchanges including its affiliate Firm *Affiliate 1* and *other names here*. Electronic access is provided via the EBS/Belzberg execution platform (executing on all exchanges), Goldman's REDI system and the ISE via a PREcise terminal.

### Execution of Stock

For stock trade execution, THE FIRM customarily transmits stock orders to Cheevers & Co on the CHX , the EBS/Belzberg platform or Goldman's REDI system. Generally, EBS is used for execution on straight purchases or sales, or where the counterparty is not tied to a strategy.

### Clearing Options

THE FIRM utilizes Electronic Brokerage Services ("EBS")/Belzberg, Goldman or Man Securities to facilitate the allocation of options trades to the customer's clearing firm. (i.e. EBS, Goldman or Man will clear the trade to the client's clearing organization on a CMTA basis.) The client's clearing firm or prime broker maintain the customers' accounts, grant customers' access to them, and delivers funds and securities.

THE FIRM clears its error account through Goldman Sachs Execution & Clearing LP

### Clearing Stock

All stock orders are entered into the EBS or Goldman front-end system for clearing purposes. After trade information (or the order itself) is transmitted to EBS, EBS clears the trade to Pershing who has settlement instructions regarding the customer's prime broker(s). Stock is cleared on a delivery vs payment (DVP) basis. Clearance procedures for Goldman are similar minus the third party interaction (Pershing).

### Memberships

THE FIRM became A FINRA member on July 30, 2002, an Electronic Access Member ("EAM") of the International Securities Exchange ("ISE") on July 18, 2005 and an Option Trade Permit ("OTP") Holder of NYSE Arca, Inc. on August 1, 2006.

### Affiliated Business

THE FIRM is wholly owned by *Firm Affiliate I* an order execution firm on the options trading floor of the NYSE Arca Exchange (the "Exchange") that provides executions for both institutional and public customer orders. Approximately 80% of *Firm Affiliate I* clients are large multi-national banks or full service brokerage firms/broker dealers. A much smaller

portion of the *Firm Affiliate I* order flow, approximately 2%, consists of retail, public customer order flow. These orders are always routed electronically via the Exchange's Member Firm Interface ("MFI") to the trading floor of the Exchange. *Firm Affiliate I* is not a clearing firm. All Firm Affiliate I clients are either clearing members themselves or have agreements to clear through another authorized clearing member ("CMTA"). Man Securities, the *Firm Affiliate I* clearing firm, enables clients to CMTA trades to the clearing firm designated by the client.

## **B. Supervision Pursuant to FINRA Conduct Rules**

This Written Supervisory Procedures ("WSP") Manual of THE FIRM is maintained pursuant to the Conduct Rules of the Financial Industry Regulatory Authority (FINRA) and Notices to Members (NTM's) issued pursuant thereto, in particular NTM 99-45 relating to Supervisory responsibilities, at its main office in San Francisco, CA. The WSPs contained in this Manual are part of THE FIRM's supervisory system and are intended to enable designated supervisors to ensure compliance with the rules, regulations, and statements of policy of the SEC, FINRA, SROs, and applicable state jurisdictions in which its registered and associated persons, and its employees, are conducting business.

In the event, THE FIRM determines to conduct business at another location ("branch"), a copy of the WSP Manual will also be kept at any other location from which the Firm does business. Currently, THE FIRM only does business at its main office.

Each Principal assigned supervisory responsibility (also referred to throughout this Manual as the "Designated Principal") has the obligation to ensure that the rules, regulations, and policies applicable to the business of THE FIRM are maintained and followed in the specifically designated areas of his/her supervisory responsibility. This Manual serves as a guide in conducting the daily supervisory functions of THE FIRM's business as such.

## **C. Firm Statement**

THE FIRM strives to maintain high standards of commercial and ethical conduct and just and equitable principles in its dealings. Accordingly, it is the obligation of THE FIRM to supervise the activities of its registered and associated persons, and its employees. THE FIRM is

dedicated to complying with all regulatory requirements applicable to its business as a registered broker-dealer and as a member of registered exchanges.

**All THE FIRM personnel and associated persons are required to comply with the rules and regulations of the FINRA, SEC, and any SRO which may be applicable, as well as the policies and procedures set forth in this Written Supervisory Procedures Manual and Supplements that may be added hereto from time to time.**

Furthermore, THE FIRM will cooperate fully in any FINRA, SEC, or Self-Regulatory Organization (“SRO”) examination, inspection, or investigation.

#### **D. Emergency Preparedness and Contingency Plans**

THE FIRM has developed detailed procedures to ensure business continuity in the event an emergency causes a significant disruption in THE FIRM’s service or daily business. Among other things, these procedures describe the processes by which THE FIRM will re-establish its service in order to continue its operations. The Plan in its entirety may be found as an Appendix A to these WSP’s titled “THE FIRM Business Continuity Plan.”

#### **E. Use and Distribution of Manual and Review of WSPs**

The material in these WSP’s is intended to be a comprehensive summary of compliance procedures specific to THE FIRM and the persons responsible for overseeing these functions. This summary should be consulted for reference to the supervisory oversight in place with respect to a particular activity or function.

Each section of this manual has a Supervisory Procedures Checkbox or Action Plan, designating the “Who, What, When and How” of ensuring compliance with that section. Where applicable, there is also a cross reference to the applicable FINRA Rule(s). The letters “WSP” denote the term “Written Supervisory Procedures” throughout this manual.

**Each THE FIRM Principal, Associated Person, and Manager will be required to sign the Attestation (see page 2 above) stating that he/she has received the WSP Manual, is responsible for knowing its contents, and will abide by the policies and procedures set forth therein.**

This Manual is intended to be a set of specific supervisory directives, which shall be kept available for all principals and supervisory personnel for day-to-day reference. Registered representatives and associated persons are also required to have a copy of this Manual and to be familiar with its content.

This Manual focuses on those rules, regulations and policies that are applicable to supervision of THE FIRM's principals, registered representatives, associated persons, and employees conducting the business of THE FIRM as such. In order to be specifically familiar with the many rules and regulations affecting registered and non-registered personnel, Firm employees are encouraged to visit FINRA's Web site ([www.FINRA.org](http://www.FINRA.org)).

The most important rules and regulations that govern securities activity are the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Advisors Act of 1940, FINRA Conduct Rules, MSRB Rules and equivalent state laws. These statutes, rules and regulations are quite complex and all Registered Representatives and Associated Persons are advised to consult the Chief Compliance Officer for further clarification.

In accordance with NTM 99-45 and other FINRA pronouncements, these written supervisory procedures are to be applied in the context of an overall supervisory system specifically tailored to the business of THE FIRM under Code of Conduct Rule 3010. The procedures, together with other tools and systems in place, are intended to guide supervisory personnel in the steps they must take to oversee and review conduct and transactions of THE FIRM personnel and to detect any real or potential violations of the rules.

**Annual Review of WSPs Manual.** THE FIRM's WSPs ("WSP Manual" or "Manual") will be reviewed not less than annually by THE FIRM's Chief Compliance Officer or designee, and any significant changes to SEC, FINRA, and SRO rules, or Firm policies and procedures, will be reflected accordingly. However, during the course of the year, the Compliance Officer or designee will update the Manual as needed by consulting the FINRA and SEC websites for changes to applicable law or regulatory requirements. (See Section E.5. - Supervisory Procedures for Updating WSPs.)

## **F. Services Offered by THE FIRM**

THE FIRM's services fall into the following categories:

- 1) **Brokering and/or Executing Orders.** THE FIRM facilitates options order execution (forwards to another order execution platform/vehicle) for various Broker-Dealer and institutional clients, who may or may not be members of a registered exchange. Generally, these clients may use options for, among other things, a hedging mechanism for their portfolios and thus require rapid price discovery and executions at the best available price in the marketplace. THE FIRM accomplishes this by representing these orders on various trading floors and/or garnering interest from other broker dealers, institutional clients etc. Certain options strategies, including but not limited to buy-writes, synthetics, Flex options, butterflies, and conversions require careful individual oversight and extensive knowledge of the options marketplace by the traders who broker these orders. THE FIRM's registered representatives have the necessary experience, training, and order management tools to broker these highly complex orders efficiently. THE FIRM typically receives a per-contract fee for order execution, but may have other pricing arrangements depending on the activity or the customer. THE FIRM does not engage in payment for order flow or soft dollar arrangements.
- 2) **Clearing-related services.** Along with the execution of large and complex option orders comes the oversight of the settlement, balancing, and clearance of such trades. Even though THE FIRM does not carry accounts or clear transactions, THE FIRM provides these services to its clients on a "give-up" basis or via Clearing Member Trade Agreements ("CMTAs") through its clearing arrangement with EBS, Goldman and Man Securities.

3)

## II. Supervisory Personnel and Their Responsibilities

### Principal/Supervisor List

Last updated: April 2008

Name	Title	Location	Registrations	Supervisor
Name here	President, Sales Supervisor, Options Principal, Producing Manager, Trader	Main Office	Series 4, 7, 24 & 63	Name Here
Name here	Chief Compliance Officer ("CCO")	Remote Office	Series 4, 7, 24 & 63	Name Here
Name Here	Financial and Operations Principal ("FinOp")	Remote Office	Series 27	Name Here

***The following is the current list of the names of THE FIRM Registered Representatives, their licenses, location, and supervisor:***

***Last updated: January 2008***

Name	Licenses	Location	Designated Supervisor
Name here	Series 4, 7, 24 & 63	Main Office	Name Here
Name here	Series 7 & 63	Main Office	Name Here
Name Here	Series 7 & 63	Main Office	Name Here
Name Here	Series 7 & 63	Main Office	Name Here

### **Anti-Money Laundering ("AML") Procedures**

## **1. Firm Policy**

It is the policy of the Firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Firm is further committed to comply with all laws and regulations designed to combat money laundering activities, including those rules and regulations requiring broker-dealers to report transactions involving currency, certain monetary instruments and suspicious activity. Every Firm employee and associated person (known collectively as “employees” or “Firm staff”) has a part in protecting the Firm from money launderers and other criminal activities. Every employee will receive a copy of the Firm’s AML policies.

The Firm has adopted the procedures contained herein to ensure that it satisfies this commitment and to ensure that it complies with its statutory and regulatory obligations in this regard, including its compliance with the USA PATRIOT Act of 2001.<sup>1</sup> However, because the Firm neither carries customer accounts nor maintains a proprietary trading account, these procedures have been tailored to the business of the Firm.

### **Description of Firm’s Business:**

THE FIRM provides execution services to non-retail clients including hedge funds, proprietary traders of broker-dealers or broker dealer affiliate or other institutional/professional industry participants. The Firm holds no client funds or securities nor does it maintain a proprietary trading account. The Firm is not the clearing agent for the client; each the Firm client has a prime broker who clears the trades and further services the client’s account. Because of these relationships, the Firm’s AML program is tailored to reflect its limited business model.

*Resources: [NtM 02-21](#), page 5; [SIA Preliminary Guidance for Deterring Money Laundering Activity \(“SIA Guidance”\)](#), at pages 2-3 (Feb. 2002).*

## **2. Legislation Designed to Provide Appropriate Tools Required to Intercept and Obstruct Terrorism**

The governing legislation for “financial institutions” is the Bank Secrecy Act, 31 U.S.C. §5311, et seq. (the “BSA”). This legislation applies to U.S. financial institutions, which specifically includes securities broker-dealers. See, 31 U.S.C. §5312. The USA PATRIOT ACT expands the BSA’s reporting requirements and imposes additional information

---

<sup>1</sup> H.R. 3162, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001 (the “PATRIOT Act”), Pub. L. No. 107-56 (2001).

collection requirements for broker-dealers. The Treasury Department's regulations implementing the BSA requirements as amended by the USA PATRIOT ACT OF 2001 are codified at 31 C.F.R. Part 103.

These regulations require that all financial institutions at a minimum:

- Develop and implement internal anti-money laundering (“AML”) policy, procedures and controls;
- Designate a money laundering reporting officer;
- Establish an on-going AML training program; and
- Ensure that independent testing of the AML program occurs regularly.

### **3. Definition of Money Laundering**

Money laundering is generally defined as engaging in act designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the “placement” stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler’s checks, or deposited into accounts at financial institutions. At the “layering” stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the “integration” stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes. The legislation and accompanying regulatory initiatives of the financial service industry that have been noted above are designed to prevent this concealment of proceeds, both at the source and throughout the process. The Firm has established these procedures in order to cover five areas:

- To identify and understand the business purpose of transactions;
- To identify suspicious transactions;
- To report knowledge or suspicion of money laundering;
- To keep adequate records; and
- To ensure employees receive on-going training.

#### **4. AML Compliance Officer Designation and Duties :**

The firm designates *Name Here* as its Anti-Money Laundering Program Compliance Officer, with full responsibility for the firm's AML program. *Name Here* is qualified by experience, knowledge and training, including reviewing current procedures and requirements for compliance with AML Procedures. The duties of the AML Compliance Officer will include monitoring the firm's AML compliance, overseeing communication and training for employees. The AML Compliance Officer will also ensure that proper AML records are kept. When warranted, the AML Compliance Officer will ensure Suspicious Activity Reports (SARs) are filed. The Firm will provide FINRA with contact information for the AML Compliance Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number. The firm will notify the FINRA of any change to this information within 17 business days after the end of each calendar quarter. The AML Compliance Officer or designee will provide Firm staff, at least annually, training about the detection and reporting of money laundering and other suspicious activity. The AML Compliance Officer will ensure that an independent evaluation of its Anti-Money Laundering Compliance Program occurs on a regular basis.

#### **5. General Procedures Designed to Prevent and Detect Money Laundering**

##### **All Firm employees are required to adhere to these procedures:**

1. Background check (including fingerprints where appropriate) of all new Firm employees, and review of background information for current personnel.
2. Regular review of all personal information contained in personnel files to detect suspicious activity such as frequent large deposits of money or withdrawal of funds.
3. Requirement of all Firm personnel to document instances of suspicious or unusual activity that they may come across during the course of their normal job responsibilities or trading activity. The first obligation is to alert supervisory personnel of suspected activity. All Firm personnel including brokers and back office staff must inform his or her supervisor and the Firm's AML Compliance Officer of suspicious trading activity or other activities of a suspicious nature.
4. Under the guidance and judgment of the AML Compliance Officer, Firm personnel will inform appropriate regulatory organization of the suspicious activity.

## General Internal Policies and Procedures

**1. Currency Transaction Reports.** *The Firm's employees will be* required to report to the AML Compliance Officer any transaction with any organization involving currency that exceeds \$10,000. This includes all known receipts or transfers of currency by one entity or person that exceed, in the aggregate, \$10,000 in one day.

**2. Report of International Transportation of Currency or Monetary Instruments.** The AML Compliance Officer will file a "Currency or Monetary Instrument Transaction Report" with the Commissioner of Customs for transactions involving the movement of currency or monetary instruments over \$10,000 into or out of the United States. "Monetary instruments" include checks, promissory notes, traveler's checks, money orders, or securities in bearer form or otherwise when title passes on delivery.

**3. Suspicious Activity Reports.** All employees are required to report to the AML Compliance Officer any suspicious transaction (or series of transactions) that involves \$5000 or more that is effected or attempted by, at or through the firm. A transaction is "suspicious" when the person knows or has reason to know that the transaction entails a violation of federal criminal law that is committed or attempted against a broker-dealer or by means of it.

- Form SAR-BD. The Compliance Officer shall file a report of such suspicious activity with FinCEN on Form SAR-BD within 30 calendar days after the date of the initial detection of a suspicious transaction that is conducted or attempted by, at or through Associated.<sup>2</sup>
- Voluntary filing of Form SAR-BD. Even if not required to do so, the Compliance Officer may voluntarily file SAR-BDs or CTRs with FinCEN or directly contact law enforcement personnel upon detecting suspicious activity (such as a currency transaction of less than \$10,000 to or from a country considered a bank secrecy or tax haven, or a transaction of less than \$5000 involving illegal activity).

---

<sup>2</sup> **Please note:** In addition to the federal government, some States have enacted SAR-type reporting requirements. We have not analyzed relevant state law to determine whether the Firm will need to file a duplicate SAR or comparable form.

4. **Certification Relating to Information-Sharing. If, in the conduct of its anti-money laundering responsibilities, the Firm intends to share information regarding money laundering activity with any other financial institution, the Compliance Officer will file initial and annual certifications with FinCEN.**

**5. Detecting and Documenting Suspicious Activity**

All Firm personnel must inform his or her supervisor and the Firm's AML Compliance Officer of suspicious trading activity or other activities of a suspicious nature.

If illegal activity is suspected, the employee should immediately contact his or her supervisor, assemble all documents pertaining to the suspicious activity, and notify the Firm's AML Compliance Officer.

Generally, suspicious activity would include trading that (1) involves funds derived from illegal activity or is an attempt to hide or disguise funds or assets derived from illegal activity, (2) is designed to evade the requirements of any law, or (3) has no apparent lawful or business purpose or vary substantially from normal practice.

**6. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions:**

**a. FinCEN Requests Under PATRIOT Act Section 314**

Under Treasury's final proposed regulations (published in the Federal Register on September 26, 2002), we will respond to a Financial Crimes Enforcement Network (FinCEN) request about accounts or transactions by immediately searching our records, at our head office or at one of our branches operating in the United States, to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the FinCEN's request. Upon receiving an information request, we will designate one person to be the point of contact regarding the request and to receive similar requests in the future. Unless otherwise stated in FinCEN's request, we are required to search current accounts, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to

FinCEN by completing FinCEN's subject information form. This form can be sent to FinCEN by electronic mail at [sys314a@fincen.treas.gov](mailto:sys314a@fincen.treas.gov), (or if you don't have e-mail,) by facsimile transmission to 703-905-3660. If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time or limits the search to a geographic location), we will limit our search accordingly.

If we search our records and do not uncover a matching account or transaction, then we will not reply to a 314(a) request.

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, such as those established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act.

We will direct any questions we have about the request to the requesting Federal law enforcement agency as designated in the 314(a) request.

Unless otherwise stated in the information request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the request as a list for purposes of the customer identification and verification requirements. We will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the firm in complying with any requirement of Section 314 of the PATRIOT Act.

#### **b. Sharing Information with Other Financial Institutions:**

We will share information about those suspected of terrorism and money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain an account or engage in a transaction. We will file with FinCEN an initial notice before any sharing occurs and annual notices afterwards. We will use the notice form found at [www.fincen.treas.gov](http://www.fincen.treas.gov). Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even with respect to financial institutions *with whom*

*we are affiliated*, and so we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from the firm's other books and records.

In addition to sharing information with other financial institutions about possible terrorist financing and money laundering, we will also share information about particular suspicious transactions with our clearing broker for purposes of determining whether one of us will file a SAR-SF. In cases in which we file a SAR-SF for a transaction that has been handled both by us and by the clearing broker, we may share with the clearing broker a copy of the filed SAR-SF, unless it would be inappropriate to share the SAR-SF under some circumstances, such as if we filed a SAR-SF concerning the clearing broker or one of its employees.

#### **1.1 7. Checking the Office of Foreign Assets Control (“OFAC”) List**

At account opening, and on an ongoing basis, we will check to ensure that a customer does not appear on Treasury's OFAC “Specifically Designated Nationals and Blocked Persons” List (SDN List) (See the OFAC Web Site at [www.treas.gov/ofac](http://www.treas.gov/ofac), which is also available through an automated search tool on *the FINRA* website, and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. Because the OFAC Web Site is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated and we will document our review.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. We will also call the OFAC Hotline at 1-800-540-6322.

## 8. Customer Identification and Verification:

Note that this regulation applies only to "customers" who open new "accounts" with a broker/dealer. A "customer" is defined as (1) a person that opens a new account or (2) an individual who opens a new account for an individual who lacks legal capacity or for an entity that is not a legal person. **Because the Firm Customers will be primarily be broker-dealers or entities that have accounts with broker-dealer clearing firms, the above would not ordinarily apply.**

Additionally, the following entities, however, are excluded from the definition of "Customer:" a financial institution regulated by a Federal functional regulator or a bank regulated by a state bank regulator; a department or agency of the United States, of any State, or of any political subdivision of any State; any entity established under the laws of the United States, of any State, or of any political subdivision of a State that exercises governmental authority on behalf of the United States, any State, or any political subdivision of a State; any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or have been designated as a NASDAQ National Market Security listed on NASDAQ (but only to the extent of domestic operations for any such persons that are financial institutions, other than banks), and a person that has an existing account with a broker/dealer, provided that the broker/dealer has a reasonable belief that it knows the true identity of the person.

Broker/dealers will not be required to verify the identities of persons with existing accounts at the firm, as long as the broker/dealer has a reasonable belief that it knows the true identity of the Customer.

For purposes of this rule, an "account" is defined as a formal relationship with a broker/dealer established to effect transactions in securities, including, but not limited to, the purchase or sale of securities, securities loan and borrow activity, and the holding of securities or other assets for safekeeping or as collateral. The following are excluded from the definition of "account:" (1) an account that the broker/dealer acquires through any acquisition, merger, purchase of assets, or assumption of liabilities, and (2) an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974 ("ERISA").

In addition to the information that must be collected under FINRA Rules 2110 (Standards of Commercial Honor and Principles of Trade), 2310 (Recommendations to Customers - Suitability), and 3110 (Books and Records), and SEC Rule 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17)(Customer Accounts), we

have established, documented, and maintained a written Customer Identification Program (or CIP). We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide notice to customers that we will seek identification information and compare customer identification information with government-provided lists of suspected terrorists.

#### **a. Required Customer Information**

Prior to opening an account, we will collect the following information for all accounts, if applicable, for any person, entity or organization who is opening a new account and whose name is on the account: the name; date of birth (for an individual); an address, which will be a residential or business street address (for an individual), an Army Post Office ("APO") or Fleet Post Office ("FPO") number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office or other physical location (for a person other than an individual); an identification number, which will be a taxpayer identification number (for U.S. persons) or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

In the event that a Customer has applied for, but has not received, a taxpayer identification number, we will obtain all required information (filing forms, notices, etc.) to confirm that the application was filed before the Customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

When opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

#### **b. Customers Who Refuse To Provide Information:**

If a potential or existing customer either refuse to provide the information described above when requested, or appears to have intentionally provided misleading information, the Firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Officer will be notified so that we can determine whether we should report the situation to FinCEN (i.e., file a Form SAR-SF).

**c. Verifying Information:**

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. In verifying customer identity, we will analyze any logical inconsistencies in the information we obtain.

We will verify customer identity through documentary evidence, non-documentary evidence, or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever possible. We may also use such non-documentary means, after using documentary evidence, if we are still uncertain about whether we know the true identity of the customer. In analyzing the verification information, we will consider whether there is a logical consistency among the identifying information provided, such as the customer's name, street address, zip code, telephone number (if provided), date of birth, and social security number.

Appropriate documents for verifying the identity of customers include, but are not limited to, the following:

- For an individual, an unexpired government-issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

The following documents are appropriate for verifying the identity of businesses:

- A certificate of incorporation, a government-issued business license, any partnership agreements, any corporate resolutions, offering memorandum or similar documents.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- Contacting a customer;
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering or terrorist financing activity, we will, after internal consultation with the firm's AML compliance officer, file a SAR-SF in accordance with applicable law and regulation.

We recognize that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering concern or has been designated as non-cooperative by an international body. We will identify

customers that pose a heightened risk of not being properly identified. Therefore, we will attempt to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient such as obtaining information regarding the primary traders and any individuals with authority or control over such account.

**d. Lack of Verification**

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (A) not open an account; (B) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (C) close an account after attempts to verify customer's identity fail; and (D) file a SAR-SF in accordance with applicable law and regulation.

**e. Recordkeeping**

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will maintain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made. This information will be maintained in the client file.

**f. Comparison with Government Provided Lists of Terrorists and Other Criminals. :**

From time to time, we may receive notice that a Federal government agency has issued a list of known or suspected terrorists. Within a reasonable period of time after an account is opened (or earlier, if required by another Federal law or regulation or Federal directive issued in connection with an applicable list), we will determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. We will follow all Federal directives issued in connection with such lists.

We will continue to comply with Treasury's Office of Foreign Asset Control rules prohibiting transactions with certain foreign countries or their nationals.

**g. Notice to Customers:**

The firm will provide notice to customers that it is requesting information from them to verify their identities, as required by Federal law. The firm will telephone customers to provide notice. Generally, RR will inform each new client that: in order to help the government fight the funding of terrorism and money laundering, the Firm will be requesting information such as name, address, tax identification etc. to verify client identity. The CCO may also provide this information in the course of discussions with the customer while obtaining information.

**1.1.1 h. Reliance on Another Financial Institution for Identity Verification**

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our customer identification program with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions:

- When such reliance is reasonable under the circumstances;
- When the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. 5318(h), and is regulated by a Federal functional regulator; and
- When the other financial institution has entered into a contract with our firm requiring it to certify annually to us that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) specified requirements of the customer identification program.

**i. Additional Inquiries:**

We recognize our obligations under suitability and fair dealing requirements to collect customer identification information. Depending on the nature of the account, we will take the following additional steps, to the extent reasonable and practicable, when we open the account:

Inquire about the source of the customer's assets and income so we can determine if the inflow and outflow of money and securities is consistent with the customer's financial status. We note that this information is required from foreign private banking accounts and for foreign correspondent banking accounts where we have determined that a foreign correspondent banking account poses a significant risk of money laundering.

Additionally, gain an understanding of what the customer's likely trading patterns will be, so that any deviations from the patterns can be detected later on.

## **9. Foreign Correspondent Accounts and Foreign Shell Banks:**

### **a. Detecting and Closing Correspondent Accounts of Unregulated Foreign Shell Banks**

Broker/dealers are prohibited from establishing, maintaining, administering, or managing correspondent accounts for unregulated foreign shell banks. Foreign shell banks are foreign banks without a physical presence in any country. A "foreign bank" is any bank organized under foreign law or an agency, branch or office of a bank located outside the U.S. The term does not include an agent, agency, branch or office within the U.S. of a bank organized under foreign law. A "regulated affiliate" of a foreign bank is a foreign bank that (1) is an affiliate of a depository institution, credit union, or foreign bank that maintains a physical presence in the U.S. or a foreign country and (2) is subject to supervision by a banking authority in the country regulating such affiliated depository institution, credit union, or foreign bank.

The prohibition does not include foreign shell banks that are affiliates of a depository institution, credit union, or foreign bank that maintains a physical presence in the U.S. or a foreign country, and are subject to supervision by a banking authority in the country regulating that affiliated depository institution, credit union or foreign bank. Foreign branches of a U.S. broker/dealer are not subject to this requirement, and "correspondent accounts" of foreign banks that are clearly established, maintained, administered or managed only at foreign branches are not subject to this regulation.

Generally, the Firm does not establish, administer, or manage correspondent accounts for unregulated foreign shell banks. However, we will detect correspondent accounts (any account that permits the foreign financial institution to engage in securities or futures transactions, funds transfers, or other types of financial transactions) for unregulated foreign shell banks by monitoring accounts and making client inquiries. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Officer, who will terminate any verified correspondent account in the United States for an unregulated foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by an unregulated foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will terminate any correspondent account for which we have not obtained the information described in Appendix A of the proposed regulations regarding shell banks not later than 10 days after notification by the Secretary of the Treasury or the Attorney General.

**b. Certifications**

We will require our foreign bank account holders to complete model certifications issued by the Treasury. We will send the certification forms to our foreign bank account holders for completion, which requires them to certify that they are not shell banks and to provide ownership and agent information. We will re-certify when we believe that the information is no longer accurate and at least once every three years.

**1.1.2 c. Recordkeeping for Foreign Correspondent Accounts**

We will keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

**1.1.3 d. Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships.**

**1.1.4** If we receive a written request from a federal law enforcement officer for information concerning correspondent accounts, we will provide that information to the requesting officer not later than 7 days after receipt of the request. We will close, within 10 days, any account for a bank that we learn from Treasury or the Department of Justice has failed to comply with a summons or has contested a summons. We will scrutinize any account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these accounts.

**10. Private Banking Accounts/Foreign Officials:**

The Firm does not offer private banking accounts. However, should these accounts be offered in the future, this section is included for future reference.

However, the following describes the due diligence requirements for such activity: Firms must have a due diligence program that is reasonably designed to detect and report any known or suspected money laundering conducted through or involving any private banking account maintained by or on behalf of a non-U.S. person, as well as the existence of the proceeds of foreign corruption in any such account. This requirement applies to all private banking accounts for non-U.S. persons, regardless of when they were opened. Accounts requested or maintained by or on behalf of "senior foreign political figures" (including their family members and close associates) require enhanced scrutiny. At the outset, decisions to open accounts for senior foreign political figures should be approved by senior management.

A "private banking" account is an account (or any combination of accounts) that requires a minimum aggregate deposit of \$1,000,000, is established for one or more individuals, and is assigned to or administered or managed by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

A "senior foreign political figure" includes a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise; a corporation, business, or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual publicly known (or actually known by the firm) to be a close personal or professional associate of such an individual.

We will review our accounts to determine whether we offer any "private banking" accounts. If we offer such accounts we will conduct due diligence on such accounts. This due diligence will include, at least, (1) ascertaining the identity of all nominal holders and holders of any beneficial ownership interest in the account (including information on those holders' lines of business and sources of wealth); (2) ascertaining the source of funds deposited into the account; (3) ascertaining whether any such holder may be a senior foreign political figure; and (4) reporting, in accordance with applicable law and regulation, any known or suspected violation of law conducted through or involving the account.

We will review public information, including information available in Internet databases, to determine whether any "private banking" account holders are "senior foreign political figures." If we do not find information indicating that a "private banking" account holder is a "senior foreign political figure," and the account holder states that he or she is not a "senior foreign political figure," then additional enhanced due diligence is not required.

If, however, we discover information indicating that a particular "private banking" account holder may be a "senior foreign political figure," and upon taking additional reasonable steps to confirm this information, we determine that the individual is, in fact, a "senior foreign political figure," we will conduct additional enhanced due diligence to detect and report transactions that may involve the proceeds of foreign corruption.

In so doing, we will consider the risks that the funds in the account may be the proceeds of foreign corruption, including the purpose and use of the private banking account, location of the account holder(s), source of funds in the account, type of transactions engaged in through the account, and jurisdictions involved in such transactions. The degree of scrutiny we will apply will depend on various risk factors, including, but not limited to, whether the jurisdiction the "senior foreign political figure" is from is one in which current or former political figures have been implicated in corruption and the length of time that a former political figure has been in office. Our enhanced due diligence might include, depending on the risk factors, probing the account holder's employment history, scrutinizing the account holder's sources of funds, and monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption, and reviewing monies coming from government, government controlled, or government enterprise accounts (beyond salary amounts).

If due diligence cannot be performed adequately, we will, after consultation with the firm's AML compliance officer and as appropriate, not open the account, suspend the transaction activity, file a SAR, or close the account.

## **1.2 11. FBAR**

We will file with FinCEN an FBAR for any financial accounts of more than \$10,000 that we hold, or for which we have signature or other authority over, in a foreign country. We will use the FBAR Form at <http://www.fincen.gov/f9022-1.pdf>

## **1.3 12. Monitoring Accounts For Suspicious Activity**

We will manually monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as “non-cooperative” are involved, or any of the “red flags” identified in Section 8. b. below. We will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. The AML Compliance Officer or designee in consultation with the Sales Supervisor will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious activities to the appropriate authorities. Among the information we will use to determine whether to file a Form SAR-SF are exception reports that include transaction size, location, type, number, and nature of the activity. We will create employee guidelines with examples of suspicious money laundering activity and lists of high-risk clients whose accounts may warrant further scrutiny. Our AML Compliance Officer will conduct an appropriate investigation before a SAR is filed. Our monitoring of specific transactions by the Sales Supervisor includes review of order tickets and blotter.

### **a. Emergency Notification to the Government by Telephone**

When conducting due diligence or opening an account, we will immediately call Federal law enforcement when necessary, and especially in these emergencies: a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region listed on the OFAC list, an account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list, a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity, we have reason to believe the customer is trying to move illicit cash out of the government’s reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism. We will first call the OFAC Hotline at 1-800-540-6322. The other contact numbers we will use are: Financial Institutions Hotline (1-866-556-3974), local U.S.

Attorney's Office (415-436-7200), local FBI Office (415-553-7400), and local SEC Office (415-705-2500).

### **b. Red Flags**

Red flags that signal possible money laundering or terrorist financing include, but are not limited to (note: the first 8 bullet points are most applicable to the Firm's business):

- The customer exhibits unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the firm's policies relating to the deposit of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the \$10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.

- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
  - The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.
  - The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
  - The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.
- 
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
  - The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
  - The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
  - The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
  - The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
  - The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
  - The customer requests that a transaction be processed to avoid the firm's normal documentation requirements.
  - The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
  - The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
  - The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.

- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

**c. Responding to Red Flags and Suspicious Activity:**

When a member of the firm detects any red flag he or she will investigate further under the direction of the AML Compliance Officer. This may include gathering additional information internally or from third party sources, contacting the government, prohibiting transactions, freezing the account, and filing a SAR-SF.

**13. Suspicious Transactions and BSA Reporting:**

***Name Here* has been designated as the Firm's AML Officer charged with administering the AML program including reporting decisions, recording keeping, supervision and training.**

**a. Filing a SAR-SF:**

We will file SAR-SFs for any account activity (including deposits and transfers) conducted or attempted through our firm involving \$5,000 or more where we know, suspect, or have reason to suspect: 1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation, 2) the transaction is designed to evade the any requirements of the BSA regulations, 3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or 4) the transaction involves the use of the firm to facilitate criminal activity.

We will not base our decision on whether to file a SAR-SF solely on whether the transaction falls above a set threshold. We will file a SAR-SF and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. [See: [NiM 02-21](#), page 9.] In high-risk situations, we will notify the government immediately (See Section 8 for contact numbers) and will file a SAR-SF with FinCEN. Securities law violations that are reported to the SEC or an SRO may also be reported promptly to the local U.S. Attorney if appropriate.

We will not file SAR-SFs to report violations of Federal securities laws or Self Regulatory Organization rules by our employees or registered representatives that do not involve money laundering or terrorism, but we will report them to the SEC or SRO. [See: [NtM 02-21](#), page 10, n.35.]

All SAR-SFs will be periodically reported to the Board of Directors and senior management, with a clear reminder of the need to maintain the confidentiality of the SAR-SF.

We will report suspicious transactions by completing a SAR-SF and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection.

We will retain copies of any SAR-SF filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state securities regulators, upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR-SF or the information contained in the SAR-SF, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency or an SRO registered with the SEC, will decline to produce to the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

*SAR-SF Form (fill-in version) -- [http://www.fincen.gov/fin101\\_formandinstructions.pdf](http://www.fincen.gov/fin101_formandinstructions.pdf)*

*[http://www.fincen.gov/fin101\\_form\\_only.pdf](http://www.fincen.gov/fin101_form_only.pdf)*

*SAR Activity Reviews -- [http://www.fincen.gov/pub\\_main.html](http://www.fincen.gov/pub_main.html)*

*SAR Bulletins -- [http://www.fincen.gov/pub\\_main.html](http://www.fincen.gov/pub_main.html)*

**b. Currency Transaction Reports (CTR):**

CTRs are filed only for certain transactions involving "currency." "Currency" is defined as "coin and paper money of the United States or of any other country" that is "customarily used and accepted as a medium of exchange in the country of issuance." Currency includes U.S. silver certificates, U.S. notes, Federal Reserve notes, and official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country.

Our firm prohibits the receipt of currency. If we receive currency from a client, it will be returned immediately to a client after senior management and the AML Compliance Officer have been notified. If we discover currency has been received, we will file with FinCEN CTRs for transactions involving currency that exceed \$10,000. Multiple transactions will be treated as a single transaction if they total more than \$10,000 during any one business day. We will use the CTR form at [http://www.fincen.gov/reg\\_bsaforms.html#4789](http://www.fincen.gov/reg_bsaforms.html#4789)

**c. Currency and Monetary Instrument Transportation Reports (CMIR):**

CMIRs are filed for certain transactions involving "monetary instruments." "Monetary instruments" include the following: currency (defined above); traveler's checks in any form; all negotiable instruments (including personal and business checks, official bank checks, cashier's checks, third-party checks, promissory notes, and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title passes upon delivery; incomplete negotiable instruments that are signed but omit the payee's name; and securities or stock in bearer form or otherwise in such form that title passes upon delivery.

Our firm prohibits the receipt of currency and has the procedures described in the previous subsection to prevent its receipt. If we discover currency has been received, we will file with the Commissioner of Customs a CMIR whenever the firm transports, mails, ships or receives or causes or attempts to transport, mail, ship or receive monetary instruments of more than \$10,000 at one time (on one calendar day or, if for the purposed of evading the reporting

requirements, on one or more days) in or out of the U.S. We will file a CMIR for all such shipments or receipts of monetary instruments, except for currency or monetary instruments shipped or mailed through the postal service or by common carrier. We will, however, file a CMIR for such receipts of currency and monetary instruments and for shipments and deliveries made by the firm by means other than the postal service or common carrier, even when such shipment or transport is made by the firm to an office of the firm located outside the U.S. We will use the CMIR Form at [http://www.fincen.gov/reg\\_bsaforms.html#4790](http://www.fincen.gov/reg_bsaforms.html#4790)

**d. Foreign Bank and Financial Accounts Reports (FBAR):**

We will file with FinCEN an FBAR for any financial accounts that we hold, or for which we have signature or other authority over, in a foreign country of more than \$10,000. We will use the FBAR Form at <http://www.fincen.gov/f9022-1.pdf>

**e. Transfers of \$3,000 or more Under the Joint and Travel Rule:**

When we transfer funds of \$3,000 or more, we will record on the transmittal order at least the following information: the name and address of the transmitter and recipient, the amount of the transmittal order, the identity of the recipient's financial institution, and the account number of the recipient. We will also verify the identity of transmitters and recipients who are not established customers of the firm (i.e., customers of the firm who have not previously maintained an account with us or for whom we have not obtained and maintained a file with the customer's name, address, taxpayer identification number, or, if none, alien identification number or passport number and country of issuance).

**14. AML Record Keeping:**

**a. SAR-SF Maintenance and Confidentiality**

We will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or SAR-SF information and immediately tell FinCEN of any such subpoena we receive. We will segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Officer will handle all subpoenas or other requests for SAR-SFs. We will share information with our clearing broker about suspicious

transactions for determining when a SAR-SF should be filed. As mentioned earlier, we may share with the clearing broker a copy of the filed SAR-SF – unless it would be inappropriate to do so under the circumstances, such as where we file a SAR-SF concerning the clearing broker or its employees.

**b. Responsibility for AML Records and SAR Filing:**

Our AML Compliance Officer or designee will be responsible to ensure that AML records are maintained properly and that SAR-SFs are filed as required. [See: [NtM 02-21](#), page 14.]

**c. Records Required:**

As part of our AML program, our firm will create and maintain all relevant documentation on customer identity and verification (See relevant sections above), and funds transfers and transmittals as well as any records related to customers listed on the OFAC list. We will maintain SAR-SFs and their accompanying documentation for at least five years. Other documents will be kept according to existing BSA and other record keeping requirements, including certain SEC rules that require six-year retention.

**15. Clearing/Introducing Firm Relationships:**

We will work closely with our clearing firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with AML laws. We will provide our clearing firm with proper customer identification information as required to successfully monitor customer transactions. We have set out these responsibilities in our clearing agreement under FINRA Rule 3230. We understand that the agreement will not relieve either of us from our independent obligation to comply with AML laws.

**16. Training Programs:**

The Firm will develop ongoing employee training under the leadership of the AML Compliance Officer and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the firm's compliance efforts and how to perform them; the firm's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, Intranet systems, in-person lectures, and explanatory memos. As part of the Firm's annual compliance meeting, RR's will be provided an educational segment discussing AML. Additionally, new RRs will receive an independent session with the AML officer. Future educational programs may include such tools such as power point presentation that can be used for new RRs as well as for on-going training requirements. We will maintain records to show the names of the persons trained, the dates, and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

**17. Program to Test AML Program:**

**a. Staffing:**

The testing of our AML program will be performed by an independent third party. This individual will be qualified by extensive experience in the securities industry, registrations and working knowledge of applicable requirements under the Bank Secrecy Act and its implementing regulations.

**b. Evaluation and Reporting:**

AML testing will be completed at least annually and may consist of reviewing a sampling of client accounts. After we have completed the testing, staff will report its findings to senior management. We will address each of the resulting recommendations.

**18. Monitoring Employee Conduct and Accounts:**

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Officer. We will also review the AML performance of supervisors, as part of their annual performance review. Another designated Principal will review the AML Compliance Officer's accounts.

**19. Confidential Reporting of AML Non-Compliance:**

Employees will report any violations of the firm's AML compliance program to the AML Compliance Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to the CEO. Such reports will be confidential, and the employee will suffer no retaliation for making them.

**20. Additional Areas of Risk:**

The firm has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above. There does not appear to be any additional areas besides our customer accounts.

**21. Senior Manager Approval :**

I have approved this AML (Anti Money Laundering) program as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA (Bank Secrecy Act) and the implementing regulations under it.

Rules: *FINRA Rule 3011.*

Signed: \_\_\_\_\_

Name of President/CEO or senior officer

Date:

## **ADDENDA to AML PROCEDURES**

### **1. Guide to FINRA AML Publications**

General guidance and background are provided by FINRA Notices to Members (NtM) 02-21, [<http://www.finra.org/pdf-text/0221ntm.pdf>], 02-47 [<http://www.finra.org/pdf-text/0247ntm.pdf>], 02-50 [<http://www.finra.org/pdf-text/0250ntm.pdf>], 02-78 [<http://www.finra.org/pdf-text/0278ntm.pdf>], and 02-80 [<http://www.finra.org/pdf-text/0280ntm.pdf>], which provide extensive guidance on setting up Anti-Money Laundering programs and related relevant information about firms' Anti-Money Laundering obligations. The Securities Industry Association's Preliminary Guidance for Deterring Money Laundering Activity may also be consulted. [<http://www.sia.com/moneyLaundering/pdf/AMLguidance.pdf>].

### **2. Special Measures for Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern (Section 311 of the PATRIOT Act)**

Special measures have been imposed by FinCEN in response to findings that the Latvian bank VEF Banka and its subsidiaries, including Veiksmes lizing (effective August 14, 2006) and the Comerical Bank of Syria and its subsidiaries, including Syrian Lebanese Commercial Bank (effective April 14, 2006) are of primary money laundering concern. Broker dealers are prohibited from opening or maintaining a correspondent account on behalf of these banks, and others as designated by FinCEN. Additionally, broker dealers are required to apply due diligence to correspondent accounts to prevent indirect use by these banks. On a monthly basis, the AML Compliance Officer will access the following website for information on all special measures issued by FINCEN: [www.fincen.gov/reg\\_section311.html](http://www.fincen.gov/reg_section311.html)

**3. AML Policy Attestation Form and Sample SAR Report**

ACKNOWLEDGEMENT OF RECEIPT & CERTIFICATION FORM

**2.0 I acknowledge that I have read and understand the Firm Anti-Money Laundering Policy and Procedures and received anti-money laundering (“AML”) training as part of the Firm’s regular Compliance program. I also acknowledge that I have been advised to consult the Anti-Money Laundering Compliance Officer and/or my immediate supervisor regarding any questions or concerns about the Anti-Money Laundering Compliance Program heretofore set forth in the Firm’s AML Program. I hereby agree to adhere to the provisions set forth in the Program at all times during my association with the Firm. I also understand that I am responsible for reading, understanding and adhering to any and all supplements and amendments thereto.**

*I understand that the Anti-Money Laundering Program and the information I received at the Firm’s ongoing AML training program is the property of the Firm. I agree not to divulge, copy, or disclose the information I received at the training (whether oral or written) to any outside source, nor to copy or disclose the information contained in the Firm’s AML Program to anyone outside of the Firm without the express written consent of the AML Compliance Officer. I understand that these AML Procedures have been assigned for use during my employment with the Firm and that I will return my copy of the AML Procedures upon termination of employment.*

**3.0**

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

**Signature:** \_\_\_\_\_

**Printed Name:** \_\_\_\_\_

5. SAMPLE MLR FORM

6.

Money Laundering Reporting Form

**Date(s) of Activity:** \_\_\_\_\_

**Account Number and Type of Account:** \_\_\_\_\_

4.0 *Suspect Identification Information*

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Phone: \_\_\_\_\_

Social Security Number or Tax ID: \_\_\_\_\_

5.0 *Third Party Information*

Third Party Name: \_\_\_\_\_

Address: \_\_\_\_\_

Phone: \_\_\_\_\_

Other Contact Information: \_\_\_\_\_

**Type of Activity (provide details below)**

Money Laundering       Structuring Transactions       Unusual Trading Activity

Identification Issue       Unusual Wire Transfer Activity       Unusual Request

Other \_\_\_\_\_

Description of the Activity

---

---

---

***Signature of Reporting Person:*** \_\_\_\_\_

***Printed Name:*** \_\_\_\_\_

***Title:*** \_\_\_\_\_

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

(SUBMIT COMPLETED FORM TO THE MONEY LAUNDERING REPORTING OFFICER)



### **The USA Patriot Act and Anti-Money Laundering**

The USA Patriot Act was signed into law in October 2001 in response to the September 11, 2001 attack. The purpose of this act is to detect and deter terrorism. Because terrorists and other criminals use laundered money to fund their operation, part of the Act concentrates on strengthening the anti-money laundering (AML) laws. It imposes a number of regulatory obligations on broker-dealers including the Firm.



### **Penalties**

Penalties for violating the AML laws are potentially severe and include both criminal and civil sanctions. If a broker dealer or one of its employees is found guilty of facilitating money laundering, penalties include up to 20 years in prison in addition to fines of \$500,000 per transaction or twice the amount of the funds involved, whichever is greater. Violators may also face civil fines. Please note that a broker-dealer or its employee need not actually know about a money laundering scheme or to participate in it to be prosecuted.



### **Red Flags**

Because Firm customers are primarily broker-dealers or entities that have accounts with broker-dealers, the Firm trading desk personnel typically do not know the identity of the customer originating the trade executed via the Firm. However, please be mindful of the following red flags that may indicate possible AML issues:

- Opportunistic trading prior to a significant event (such excessive activity in airline issues prior to the events of 9/11/01 in USA)
- Client engages in transactions that lack business sense or apparent investment strategy
- Accepting an order from an unfamiliar source or individual.

Additional red flags are listed on the attachment to this memo. Should an employee suspect suspicious activity, the employee should elevate those concerns to a supervisor or the

Compliance Officer. There is significant reliance on the trading desk personnel to note or detect potential money laundering.

#### The Firm's AML Program and Record Retention

Although the Firm's AML program is not described in detail here, the complete policy and procedures, including the customer identification program and filing of suspicious activity reports is available in the administrative offices for your review. The Firm is required to maintain records associated with its program for a period of 5 years.

If you have any questions regarding the AML program or would like to see review a complete copy of the AML procedures, please call the Firm's administrative office.

## Attachment to AML Training



### Additional Red flags



Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- The trading desk is unfamiliar with the client representative who with they have contact with.
- The customer exhibits unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the firm's policies relating to the deposit of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the \$10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.

Additional Red flags (con't)

- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.

- The customer requests that a transaction be processed to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.



## **5.1 Insider Trading and Prevention of the Misuse of Material, Nonpublic Information (JSC/ASE rules here)**

According to the Insider Trading and Securities Fraud Enforcement Act of 1988 and NYSE Arca Rule 11.3 (*replace with JSC/ASE laws, articles, directives. Please note, the US acronym for our Insider Trading Act is “ITSFEA”*), every firm is required to establish, maintain, and enforce supervisory procedures that are reasonably designed to prevent the misuse of non-public information. All registered and/or Associated Persons are strictly prohibited from trading on any information that could be considered material, non-public (insider) information, as well as, disclosing such information to others. Such trading may not occur in any account that is directly or indirectly controlled by the registered person. All registered persons, associated persons and/or employees of the firm will annually review and sign the Firm’s ITSFEA procedures and submit it to the Exchange. In addition, as per NYSE Arca Regulatory Bulletin RBO-02-06, Associated Persons will review and acknowledge these ITSFEA procedures within 10 days of hire. The Firm will submit its Annual ITSFEA Compliance Acknowledgement Form annually to the Exchange (*these last three sentences do not apply to JSC but could be considered for future rules.*)

### **Definitions:**

**“Material” Information:** Information that a reasonable investor would consider important in making an investment decision. Generally, a corporate insider having material, non-public information about the issuer, and anyone to whom such information is disclosed, may not trade while in possession of that information unless it is first disclosed to the investing public. Whenever any employee receives such information, he or she must immediately contact the Compliance Department to discuss the appropriate action to be taken. Material information is generally regarded as “material” if there is a substantial likelihood that a reasonable investor would consider the information important in deciding whether to purchase, sell or hold a security. Information may be material even if it relates to speculative or contingent events. Information that is material to a decision to trade a security is also likely to be material to a decision to trade related derivatives.

**“Confidential Information”:** Includes “Inside Information” and “Proprietary Information”. “Inside Information” is generally defined as material non-public information provided by an external source (such as a client, prospective client, or other third party) with the expectation that the information will be kept confidential and used solely for the business purposes of that third party. Firm employees may receive inside information from corporate officers, employees or directors of a client or prospective client. Inside Information relating to a particular security also can come from a person who is not an official of the issuer, such as an investment banker, accountant or attorney with a relationship to the issuer or a bidder or potential bidder for the issuing company’s securities. It may also include “tips” received directly or indirectly from corporate insiders, whether inside or outside of a client relationship,

particularly where the recipient knows, or should know, that the corporate insider is disclosing the information improperly, in breach of the insider's duty to his or her own company.

“Material Insider Information”: Such information may include, but is not limited to, significant developments in the following areas: changes in projected earnings, write-offs or upward adjustments in previously reported earnings, proposed or contemplated dividend changes, proposed or contemplated stock splits or stock dividends, changes to key managerial personnel, significant acquisitions, material litigation, labor disputes, a significant expansion or curtailment of operations, extraordinary borrowing, a change in major product or product lines or a change of major customers or suppliers, significant new products or discoveries or the entering into of significant contractual arrangements, or significant unreported changes of stock ownership, plans regarding tender offers, joint ventures, other acquisitions, the control of an issuer's securities, or other purchasing or selling plans which could affect supply of and demand for a security and in particular regarding fixed income securities, decisions to “call” certain bonds, refundings or a default regarding interest payments.

“Proprietary Information”: Non-public information, analyses, and plans that are created or obtained by the Firm for the Firm's business purposes. Examples include unpublished research information, opinions and recommendations; information about the Firm's securities trading positions or trading intentions; the Firm's investment, trading or financial strategies or decisions; pending or contemplated customer orders; unpublished analyses of companies; industries or economic forecasts; advice to investment banking clients; and analyses done by the Firm of companies that are potential acquirers of other companies or their assets or companies that are possible candidates for acquisition, merger or sale of assets.

Non-public Information’: Information that is “non-public” unless and until it has been broadly disseminated or made widely available to the public, such as by means of a press release carried over a major news service, a major news publication, a research report or publication, a public filing made with a regulatory agency, materials sent to shareholders or potential investors or customers such as proxy statement or prospectus, or materials available from public disclosure services. It is important to note that even following a public announcement relating to a matter, many aspects of the matter may remain non-public.

*If an associated person or employee of the Firm has any questions about whether information in their possession is non-public, material, inside or proprietary, that person should not act upon such information.*

## **Handling of Confidential Information**

### Disclosure of Inside or Proprietary Information:

Firm associated persons and employees should disclose inside information or proprietary information only to employees and third parties (such as the Firm's outside counsel or the client's lawyers or accountants) who have a valid business reason for receiving the information, i.e., persons who need to know the information in order to serve the Firm or its clients. In no event may an employee communicate inside or proprietary information to any person under circumstances in which it appears likely that such person will misuse the information.

### Use of Inside or Proprietary Information:

Material inside information obtained directly or indirectly from any source may be used only for the specific purpose for which it was given; any other use without the permission of the source, which originally entrusted the Firm with the information, is a misuse. Except with the prior approval of the Compliance Officer, material proprietary information may be used only for the business purposes for which the information was created or obtained. Firm employees may not use inside or proprietary information for their personal benefit or for the benefit of any related person. Any Firm broker or employee who becomes aware of the possible misuse of material, non-public information must promptly notify (*the JSC and ASE*). In accordance with *Regulatory Agency name here* directives, conduct constituting the misuse of material, non-public information includes, but is not limited to the following:

1. Trading in any securities issued by a corporation, or in any related securities of related options or other derivative securities, while in possession of material, non-public information concerning that issuer;
2. Trading in a security or related options or other derivative securities, while in possession of material non-public information concerning imminent transactions in the security or related securities; or
3. Disclosing to another person or entity any material, non-public information involving a corporation whose shares are publicly traded or an imminent transaction in an underlying security or related securities for the purpose of facilitating the possible misuse of such material, non-public information.

### **Trading While in Possession of Material Inside Information:**

Firm associated persons and employees are prohibited from buying or selling or recommending the purchase or sale of a security (or a derivative of such security) for any account (i.e. any proprietary account, client account, employee-related account) while the employee is in possession of material inside information relating that security or its issuer.

**Evidencing Procedure (may not be a JSC requirement):**

Copies of trade confirmations and monthly brokerage account statements must be received and retained for each associated person. The activity in such brokerage accounts will be reviewed at least quarterly by The Compliance officer for the possible misuse of confidential information obtained as a result of an association with the broker or an organization.

**Frontrunning (this definition may be specific to US markets only):**

Firm associated persons and employees may not buy or sell or recommend the purchase or sale of any security or a derivative thereof for any account in anticipation of a price change resulting from a contemplated or pending block transaction in the security or a derivative thereof for another account unless the transaction is an offsetting hedge transaction in connection with the execution of a client order and the client is informed of the transaction. For example, if a Registered Representative has accepted an order from a customer of the Firm to buy or sell a large block of securities and/or options, the employee must not trade on such information ahead of the execution of such order or communicate such information to any person (including another customer) who does not “need to know” such information for a legitimate business purpose.

**Handling of Inside or Proprietary Information:**

Firm associated persons and employees should not discuss the Firm’s or its clients’ business with, or in the presence of, persons who are not authorized to receive, or do not “need to know” such information (an “unauthorized” person). Firm employees should avoid such discussions in hallways, elevators, trains, subways, airplanes, restaurants, and other public places generally. Use of speaker or mobile phones should be avoided in circumstances where unauthorized persons may overhear material inside or proprietary information. Documents and files that are confidential and, in particular, contain inside information, must be secure in order to minimize the possibility that such information will be transmitted to an unauthorized person. Confidential documents should be stored in locked file cabinets or other secure locations. Confidential databases and other confidential information accessible by computer should be maintained in computer files that are password protected or otherwise secure against access by unauthorized persons. Documents relating to investment banking projects and other proprietary material such as the Restricted List or customer lists or records, must not be circulated or discussed outside the Firm or within the Firm except on a “need to know” basis.

### **Personal Benefit:**

Firm associated persons are reminded that any material inside or proprietary information created or obtained by the Firm for its business purposes is the exclusive property of the Firm. Firm associated persons are prohibited from misappropriating such information for personal use or benefit, or for any other purpose.

### **Rumors:**

Firm associated persons should promptly report to the Compliance Officer any rumor, which, if true, might be considered material, non-public information concerning any publicly traded company. No action should be taken on the basis of such a rumor, nor should it be communicated further, without the prior approval of the Compliance Officer. This does not apply to discussions of unsubstantiated information widely circulated in the public media, so long as the source and unsubstantiated nature of the information are disclosed during the discussions. Spreading rumors, trading or making recommendations on the basis of rumors in violation of this policy may result in disciplinary action by the Firm and, in certain circumstances, may violate the rules of the JSC and the various self-regulatory organizations.

If an associated person or employee believes that he or someone else may have obtained or disclosed inside or proprietary information in a manner not permitted by the policies and procedures set forth herein, he should contact the Compliance officer immediately and should not use or further disclose the information.

### **Insider Trading and Securities Fraud “Declaration of Understanding by an Associated Person”:**

All persons will be obligated to document their outside account activity and other interest in public corporations monthly and sign a “Declaration of Understanding by an Associated Person” document that details specifics of their compliance with Insider Trading provisions. ITSFEA Attestations will be signed annually by all Firm personnel and submitted to the Exchange within 17 business days after the calendar year end. The attestations will be maintained for three years, the first two in an easily accessible place. The attestation will be in a form substantially similar to the following:

#### **ITSFEA ATTESTATION**

#### **THE UNDERSIGNED STATES AND ATTESTS AS FOLLOWS:**

“I understand that should I acquire material non-public information concerning a corporation whose shares are listed on a national securities exchange, it would be a violation of exchange rules and federal securities laws for me or my employer to trade in any securities issued by the corporation, or options or other derivative securities

thereon while such information remains material and non-public.

“I further understand that should I obtain material non-public information concerning the market in an underlying security, neither I nor my employer may take advantage of such knowledge by trading in the underlying security or options thereon, while such information remains material and non-public. I understand that such information includes, but is not limited to, information obtained in the course of receiving execution reports and information obtained in the course of negotiating to participate in transactions of block size.

“I further understand that should I obtain material non-public market or corporate information concerning a publicly traded security, it would be a violation of exchange rules and federal securities laws for me to disclose such information to another person while such information remains material and non-public.”

Print Name: \_\_\_\_\_ Date: \_\_\_\_\_

Signature: \_\_\_\_\_

**Attestation Regarding Employee Trading Accounts** (may not apply to JSE directives)

**THE UNDERSIGNED STATES AND ATTESTS AS FOLLOWS:**

“I have either a direct or indirect interest in the following personal securities accounts:

Account Number(s): \_\_\_\_\_

Brokerage Firm/Type of Account: \_\_\_\_\_

Branch Address/Contact Person: \_\_\_\_\_

“I agree to provide monthly statements for the above listed accounts to the Firm for review. I agree to provide duplicate confirmations and monthly statements for all accounts over which I exercise discretionary control with respect to the purchase or sale of individual securities. Additionally, I agree to notify the Compliance officer regarding any changes to my accounts during my employment with the Firm or one of its Affiliates.

I agree to notify the Firm of any changes made to outside brokerage accounts within 10 business days of occurrence.

Print Name: \_\_\_\_\_ Date: \_\_\_\_\_

Signature: \_\_\_\_\_

*Insert Firm Name Here*  
Business Continuity Plan (BCP)

---

**I. Emergency Contact Persons**

The following persons (each a “Disaster Recovery Coordinator”) have been designated as emergency contact personnel for the Firm:

**Primary Contact:**

*Insert Name Here,*

President

Office phone: xxx-x-xxx-xxxx

Cell phone: xxxxxxxxxxxx

Fax: xxx-x-xxxxxxx

Email:

**Secondary Contact:**

*Insert Name Here,*

Chief Information Officer

Office: xxx-x-xxx-xxxx

Cell phone: xxxxxxxxxxxx

fax: xxx-x-xxxxxxx

Email:

These names will be updated in the event of a material change, and our Executive Representative, or designee, will review them within 17 business days of the end of each quarter.

The Disaster Recovery Coordinators must be members of senior management and registered principals of the Firm

Rule: *FINRA Rule 3520.*

**II. Firm Policy**

The 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 call in order to transact business.

## **5.2 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 bombing, 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.

## **5.3 Approval and Execution Authority**

*Name Here*, the Firm's President, a registered principal, is responsible for approving the plan and for conducting the required annual review. The President and the CIO have the authority to execute this BCP.

## **5.4 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. An electronic copy of our plan is located in a shared directory with the following folder (**L:\xxxxxx**). Furthermore, this plan is available both in hard copy and CD at our alternative location, in Novato, CA.

## **III. Business Description**

The Firm conducts business in equity and derivative securities. Our firm is an agency business that does not perform any type of clearing function for itself or others. Currently, our affiliate *Firm Affiliate I* executes approximately 60% of the Firm's trades. The remaining 40% of the Firm's trades are executed with a number of different brokers at the domestic option exchanges. Furthermore, we do not hold customer funds or securities. The Firm is engaged in the business of brokering orders for institutional businesses such as RIAs. We do not engage in any private placements, market making or proprietary trading. All Firm customers have a prime broker or have their own clearing arrangement established. The Firm utilizes Electronic Brokerage Services ("EBS")/Belzberg, Goldman or Man Securities to facilitate the allocation of trades to the customer's clearing firm. (i.e. EBS or Man will clear the trade to the client's clearing organization.) The client's clearing firms maintain the

customers' accounts, grant customers access to them, and delivers funds and securities. We maintain the Firm error account at Goldman Sachs Execution & Clearing, LP ("Goldman").

Our error account clears Goldman. Our contact person at Goldman is *Name Here*, xx-xxx-xxxx. Electronic Brokerage Services provides a platform for execution, allocation and settlement. Our contact person at EBS is *Name Here*, xxx-xxx-xxxx or Belzberg Technologies (USA), Inc., 212-943-1400, or at [www.belzberg.com](http://www.belzberg.com). Man Financial provides allocation and settlement of our customer's trades; our contact person is *Name Here* at xxx-xxx-xxxx

#### **IV. Office Locations**

##### **Office Location #1**

The Firm has a single office located at San Francisco, CA 94104. This location serves as the Home Office and Office of Supervisory Jurisdiction. Its main telephone number is xxx-xxx-xxxx. The Firm employees may travel to this office by means of foot, car, subway, train, bus or boat. The Firm engages in order taking and entry at this location.

#### **V. Alternative Physical Location(s) of Employees**

In the event of an SBD, the Firm staff will move from affected offices to its alternative location at Novato, CA. Its main telephone number is xxx-xxx-xxxx. At this location, employees will have the ability to conduct business via cell phone and have access to the internet, although in a limited capacity depending on the severity and type of SBD. If internet access is available, our staff will have access to certain critical systems; Track Data and Bloomberg

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

#### **VI. Electricity**

In the event that the power fails at the Firm's main office location in San Francisco, the firm will continue its normal operating at the alternative site. The site is serviced by an entirely different power grid from the primary San Francisco location.

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

The Firm does not maintain custody of customers' funds or securities, which are maintained at the customers' clearing firms. .

Rules: *FINRA Rule 3510(a)*; Securities Exchange Act Rule 15c3-1; 15 U.S.C. 7 (2003).

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

The Firm maintains its primary hard copy books and records and its electronic records at San Francisco, CA. *Name Here*, Chief Information Officer (xxx-xxx-xxxx, cell xxx-xxx-xxxx) is responsible for the maintenance and back-up of these electronic books and records. These books and records include any document created electronically such as email/instant messaging, billing info, outrade and certain trade data, etc. Some information is maintained only in hardcopy such as order memoranda (tickets), client files-new account information, certain financial records (G/L and trial balances) and clearing sheets. These records are kept in our primary location and not by our clearing firms. Some of the data, such as certain trade data or clearing information is available at the exchanges where we execute orders. Order tickets, are stored in our offices or in the building where our offices are located. The Firm's third party vendors also maintain copies of critical data as follows: *Controller's name here* (phone xxx-xxx-xxxx) maintains copies of our financial data including FOCUS filings; *Attorney's name here*, the Firm's attorney (phone xxx-xxx-xxxx) maintain copies of the Firm's operating agreement and meeting minutes and; the Firm's auditor, *CPA's name here* (phone xxx-xxx-xxxx) maintains copies of the Firm's financial statements and audits.

The Firm backs up its electronic records daily by copying the data to tape and keeping this copy at the alternative location.

If the Firm's our primary location is inoperable, we will continue operations from our alternate location. For the loss of electronic records, we will either physically recover the storage media or electronically recover data from our back-up.

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

## IX. Financial and Operational Assessments

Because of the size and limited business activities of the Firm, the ability to identify changes in its operational, financial and credit risk exposures is immediate. For example, the CIO, arrives at the Firm's on-site location approximately 30 minutes prior to the opening of the stock/options markets and immediately begins the process of confirming if all computer systems and vendor systems critical to the Firm's operation are functional. In the event that the CIO is unable to perform these evaluations, the Firm has retained *Personal Computer Support*, in San Francisco, CA to provide back-up operational assistance.

Similarly, the Firm's President arrives on-site approximately 30 minutes prior to the opening to assess all financial and credit issues and to ensure that outstanding issues are resolved satisfactorily. Also, both the CIO and the President are accessible by cell phone.

### Operational Risk

In the event of an SBD, the Firm 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 cellular phone, telephone voice mail, and secure e-mail. In addition, we will retrieve our key activity records as described in the section above, Data Back-Up and Recovery (Hard Copy and Electronic).

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

### 5.5 Financial and Credit Risk

In the event of an SBD, we will 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 or otherwise continue to fund our operations, we will request additional financing from our bank or other credit sources to fulfill our obligations. 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).*

## X. Mission Critical Systems

Our firm's "mission critical systems" are those that ensure prompt and accurate processing of securities transactions, including stock/option market information and pricing, order taking, entry, execution, comparison, allocation, clearance and settlement of securities transactions. (The Firm does not perform the functions of maintenance of customer accounts, access to customer accounts, and the delivery of funds and securities.) More specifically, The Firm's mission critical systems include: **Bloomberg**, market information service provider; **EBS**, executing/clearing firm; **Goldman**, executing/clearing firm; **Track Data**, information service provider; **Casey Securities, LLC**, option execution services; the **International Securities**

*Exchange (“ISE”), options execution services (and other alternative order execution firms operating at other exchanges); Cheevers & Co, stock execution services.*

We have primary responsibility for establishing and maintaining our business relationships with our customers and have sole responsibility for our mission critical functions of order taking, entry and forwarding the trade for execution and clearance. Man, Goldman and EBS, as clearing agent assists in the comparison, allocation, clearance and settlement of securities transactions.

EBS and Goldman provide us or access to their business continuity plans. They have represented that they will advise us of any material changes to its plan that might affect our ability to maintain our business.

The clearing firm of our error account, Goldman, represents that it maintains a back-up facility and has also confirmed the effectiveness of its back-up arrangements to recover from a wide scale disruption by testing these arrangements once a quarter.

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, EBS, has the following SBD recovery time and resumption objectives: recovery time period within 2 hours; and resumption time of up to 24 hours while Fortis’ recovery and resumption time is immediate for most systems.

## **Our Firm’s Mission Critical Systems**

### **5.5.1 Order Taking**

Currently, the Firm receives orders from customers via telephone (typically land-line), Bloomberg messaging or AOL instant message. 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. Customers will be informed of alternatives by whatever means available.

### **5.5.2 Order Entry**

Currently, the Firm enters orders by recording them on paper and electronically transmitting them electronically or telephonically. Alternatively, we route customer orders through *telephone, instant messaging, Bloomberg, Goldman REDI system and the EBS platform.*

Some of these orders are routed to the *Firm Affiliate I* which resides on the NYSE Arca Exchange (“the Exchange”) located in San Francisco, CA. Orders may also be routed to the International Securities Exchange (“ISE”) located in NY, NY, or other domestic options exchanges. Stock trades done for our customers are entered and executed at the Chicago Stock Exchange (CHX) located in Chicago, IL or EBS also located in Chicago, IL.

In the event of an internal SBD, we will enter and send records to clearing firms by the fastest alternative means available. In the event of an external SBD, we will maintain the order in electronic or paper format, and deliver the order by the fastest means available.

### **5.5.3 Order Execution**

The Firm does not execute orders, instead it brokers orders. The *Firm Affiliate I* is solely engaged in the order execution function for the Firm and other broker - dealers. The *Firm Affiliate I* accepts orders both telephonically and electronically on the trading floor of the Exchange. Currently, at the Exchange and alternative option exchanges, such as the CBOE and PHLX, most orders are executed via open outcry by a floor broker. At the ISE most orders are executed electronically without human intervention. In the event of an internal SBD at either the *Firm Affiliate I* or the Exchange, the Firm would route orders to the ISE or another exchange for execution. In the event of an external SBD, if we do have the ability to route orders electronically to the ISE, orders would be transmitted telephonically to the ISE, CHX, ARCA or other alternative exchange for execution.

### **5.6 Mission Critical Systems Provided by the Clearing Agent**

The Firm relies, by contract, on clearing agents including EBS to provide order comparison and order allocation for our customer’s orders.

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

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

### **A. Customers**

The Firm communicates with its customers primarily using the telephone, e-mail and instant message and secondarily using, fax and U.S. mail. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. For example, if we have communicated with a party by e-mail but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the U.S. mail.

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

### B. Employees

The Firm communicates with its employees using the telephone, 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 or oral) 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.

The person to invoke use of the call tree is: *Nick*

<b>Caller</b>	<b>Call Recipients</b>
<i>Nick (cell xxx-xxx-xxxx)</i>	<i>Harry (home xxx-xxx-xxxx)</i>
	<i>Steven (cell xxx-xxx-xxxx)</i>
	<i>Joseph (cell xxx-xxx-xxxx)</i>
	<i>Kevin (cell xxx-xxx-xxxx)</i>
<i>Kevin</i>	<i>Richard (cell xxx-xxx-xxxx)</i>
<i>(cell xxx-xxx-xxxx)</i>	<i>George (cell xxx-xxx-xxxx)</i>
	<i>Christina (cell xxx-xxx-xxxx)</i>
	<i>Greg (work xxx-xxx-xxxx ext.301)</i>

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

### C. Regulators

We are currently members of the following SROs: FINRA and are Electronic Access Member (EAM) of the ISE and an Option Trade Permit (OTP) Firm of NYSE Arca, Inc. As noted earlier, our order execution affiliate, is an OTP and an EAM of the NYSE Arca, Inc. and ISE, respectively. 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.

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

## **XII. Critical Business Constituents, Banks, and Counter-Parties**

As described in the paragraphs above, the nature of the Firm's business activity is limited in scope. Thus, there is an immediate impact with an SBD yet little change in how the Firm will operate given the SBD. The Firm will continue to contact its business constituents in whatever methods are available including telephone, instant messaging, email and U.S. mail.

### **5.7 Business constituents**

**We have 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. Our suppliers are: Bloomberg - market information service provider, 499 Park Avenue, New York, NY 10022, 212-318-2000; EBS - clearing firm, 141 West Jackson Blvd., Suite 3510, Chicago, IL 60604, 312-986-6280; Goldman - clearing firm, 555 California, 44<sup>th</sup> fl, San Francisco, CA 94104, 415-834-7830 ; Track Data - market information service provider, 95 Rockwell Place, Brooklyn, NY 11217-718-522-7373.**

**Cheevers & Co – stock execution services, 440 S. LaSalle Street, Chicago, IL 6060, 312-663-2794; American Stock Exchange, LLC – quote information, PO Box 11181A, New York, NY 10286, 212 306-1340; Bigdough – marketing data (Hedge Fund customers), 12189 Collections Center Drive, Chicago, IL 60693, 800-254-1005; BizAtomic – website & email server, 23 Sanchez Avenue, Saint Augustine, FL 32084, 904 794-9463; IPC Information Systems Inc. - 142 Sansome Street-3rd Floor, San Francisco, CA 94104, 415 544-1800; IPC Network Services Inc. – telecom services, 1 State Street, 12th Floor, New York, NY 10004-1417, 888 286-2343 (Help Desk); International Securities Exchange – member exchange, 60 Broad Street, 26th Floor, New York, NY 10004, 212 897-8152; KGM Circuit Solutions, LLC (Gerard Martell) – telecom services, 45 John Street, Suite 410, New York, NY 10038-3746, 212 791-1555; New York Stock Exchange Inc. – quote information, Grand Central Station, PO Box 4695, New York, NY 10163; OPRA – quote information, PO Box 95718, Chicago, IL 60694-5718, 312 786-7195; SBC – telecom services, Payment Center, Sacramento, CA 95887-0001, 800 649-7570; Sprint - telecom services, PO Box 79255, City of Industry, CA 91716-9255, 800 436-2070; and Professional Computer Support (Dan Hernandez) – systems support, 515 Alabama Street, San Francisco, CA, 415-252-5575, 415-616-2008**

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

### **5.8 Banks**

We have 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: *Westamerica Bank, 7333 Redwood Boulevard, Novato, CA 94948, 415- 382-5568 and the contact person is Vicky Tappero.* The bank maintaining our

Proprietary Account of Introducing Brokers/Dealers (PAIB account) is Fortis., 175 West Jackson, Suite 400, Chicago, IL 60605, 312-604-8047 and the contact person is Dave. If our banks and other lenders are unable to provide the financing, we will seek alternative financing immediately.

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

### **5.9 Counter-Parties**

The Firm's counter parties, including its affiliate, clearing firm and third party vendors have been discussed previously in this plan. 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).

### **VIII. Regulatory Reporting**

Our firm is subject to regulation by: *FINRA, NYSE Arca, Inc. and the ISE*. 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, 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. *Christian Zrull, One Montgomery Street, Suite 2100, San Francisco, CA 94104, 415-217-1101*. Our regulatory contact at the NYSE Arca is *James Draddy, 100 S. Wacker Dr., Chicago IL 60606, 3125-442-7930* and at the ISE our regulatory contact is *Michael J. Simon, 60 Broad Street, NY, NY 10004, 212-943-2400*.

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

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

The Firm will provide, in writing and upon request, an abbreviated copy of this BCP to its customers. Rule: FINRA Rule 3510(e).

### **XV. 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 BCP annually to modify it for any changes in our operations, structure, business, or location or those of our clearing firm.

Rule: *FINRA Rule 3510(b).*

#### **XVI. 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 an SBD.

*Rule: FINRA Rule 3510(d).*

Signed: \_\_\_\_\_

Title: President

Date: 03/10/08

**(Firm name here) Books & Records Retention Schedule**

\* “Branch” not currently/currently applicable to (Firm name here)

Books & Records	File	Main Office	OSJ	Branch*	Retention Period
List of Supervisory Personnel including designation of Supervisory Personnel as in Supervisory Procedures Manual	Chronologically	X	X (copy)		6 years after change in designated personnel
Documentation of Annual Compliance Meeting	Chronologically	X			3 years
Document of payment/receipt of gratuities or compensation	Alphabetically by Employee	X			3 years
Customer Complaints (General)	Chronologically Alphabetically	X	X (copy)	X (copy)	3 years
Correspondence Outgoing and Incoming	Chronologically	X	X (copy)	X (copy)	3 years
Advertising and Sales Literature	Chronologically	X	X (copy)		6 years
Articles of Incorporation, Minute Books, all corporate records	Chronologically	X			Life of Corporation
Records concerning delivery of official statements	Chronologically	X			3 years
Copy of annual compliance review and report to senior management including all audit documentation and work papers for main and branch office audits	Chronologically	X	X (copy)		3 years

Books & Records	File	Main Office	OSJ	Branch*	Retention Period
Proof of money balances including checkbooks, bank statements, canceled checks, cash reconciliations	Monthly	X			3 years
Calculations of Aggregate Indebtedness, net capital	Monthly	X			3 years
Customer Account Agreement/New Account Form or Information	Alphabetically or by Account Number	X	X (copy)	X (copy)	6 years after account is closed
Trade Memos	Trade date	X	X		6 years
Confirmations	Trade date	X	X		6 years
Purchase and Sales Blotter	Trade date	X	X		6 years
Securities Received/Delivery Blotter (Receipts)	Chronologically	X or	X	X	6 years
Cash Received/Disbursed Blotter (Receipts)	Chronologically	X or	X	X	6 years
U-4, U-5. Fingerprints, Employment Agreements	Alphabetically	X	X (copy)		3 years after termination
Form BD and all BD registration forms, files	Chronologically	X			Life of the firm
Original BD registration documents	Chronologically	X			Life of the firm
Audited financials and records supporting calculations	Annually	X			6 years
FOCUS reports and work papers	Monthly and Quarterly	X			3 years
Bills receivable/payable	Monthly	X			3 years
Record of Rule 17f-2 (fingerprint) exemptions	Chronologically	X	X		Life of corporation
Books & Records	File	Main Office	OSJ	Branch	Retention Period

Annual SIPC and NASD assessment reports and documentation	Annually	X			6 years
Ledger (Asset - Liability)	Daily, Monthly	X			6 years
Ledger (Income Expense)	Daily, Monthly	X			6 years
Capital Accounts	Daily, Monthly	X			6 years
Files containing exam results for NASD, SEC, state, etc.	Chronologically	X			6 years
17a-8 reports – Currency Reports	Chronologically	X			6 years
Continuing Education Program	Annually	X			Life of corporation
CEO Certification	Annually	X			Life of corporation

### Action Plan for Books and Records Retention Schedule

6.0 Requirements	7.0 Broker/Dealer Actions
<b>8.0 Supervisory Responsibility</b>	CCO
<b>Frequency of Review</b>	Retention log is reviewed annually.
<b>Review Sample</b>	Above Log
<b>Review Process</b>	CCO will ensure that the above log is current.
<b>Evidencing Procedures</b>	Changes to retention log will be maintained. Documentation of sample review of actual files will be maintained by reviewer as well as a listing

### 7) Errors

The Firm does not conduct proprietary trading and does not hold, carry, or assume any positions other than those placed in the error account as a result of a *bona fide* error *i.e.*, a miscommunication, mis-entry or because a system issue has occurred. It is the policy of the Firm that all errors will be liquidated immediately, but not later than 24 hours after the error is discovered. The exception to this policy is when an option is “no bid,” or market conditions in general make it impossible to access a market (e.g. those which occurred in 1987). In this instance, the Sales Supervisor will enter a “Good-‘Til-Cancelled” (“GTC”) sell order in that series to ensure the error is liquidated should the option become eligible for execution. Additionally, the CCO will review time and sales daily to ensure that the option remained “no bid.”

Should an error occur as the result of a miscommunication or system outage, the Sales Supervisor will determine if any Customer should be made whole as a result. Each error that requires the Firm to take an offsetting position must be documented, and records will be kept according to the record keeping requirements outlined in the WSPs.

The Firm registered representatives may never place a trade in the error account or liquidate a trade in the error account without approval of the Sales Supervisor

The CCO, or designee, will review the error accounts on a daily basis to confirm that all positions are liquidated within 24 hours. If for any reason (besides a “no bid” option), the CCO discovers an error was not liquidated within 24 hours, a trade may be entered to liquidate the position.

**Customer Liability and Out Trades.**

Generally, it is inconsistent with just and equitable principles of trade for any Customer, or person associated with a Customer, to accept a transaction in which he was not involved. Further, a Customer who has an out-trade is prohibited from giving the out-trade to or clearing the trade with a Customer who was not involved in the transaction which resulted in the out-trade.

Name of Supervisor:	Sales Supervisor and Chief Compliance Officer
Frequency of Review:	As needed when errors occur.
How Conducted:	Liquidating order entered by Sales Supervisor immediately and no later than 24 hours after initial error occurs. CCO or designee reviews account statements to ensure liquidation occurred w/i 24 hours.
How Documented:	<i>Source ticket, account statements, cover sheet describing error &amp; liquidation</i>
3010 Checklist:	<i>2110 and SEC Rule 15c3-1(a)(2)(vi)</i>
Corrective action:	Error liquidation by CCO.

**Sustainable Achievement of Business Expansion and Quality (SABEQ)**

**BearingPoint, Inc.**

**Salem Center, Sequleyah Street, Al-Rabiyeh**

**Amman, 11194 Jordan**

**Phone: + 962-6 550-3050**

**Web address: <http://www.SABEQ-Jordan.org>**