U.S. Sterling Capital, Corp.

Due Diligence Packet

2013

Contents

Introduction 1
Private Policy Statement 2
Consolidated Financial Statements 4
Business Continuity Planning 6
AML – CIP – BSA Procedures 11

U.S. STERLING
Capital Corp.

1393 Veterans Memorial Highway · Suite 412N · Hauppauge, NY 11788
631-360-2829 800-935-9300 Fax 631-360-2841

Fiscal Year 2013

Dear U.S. Sterling Customer:

I have received your request for information to complete your due diligence. I think a brief discussion of U.S. Sterling Capital and U.S. Sterling Securities and their roles that each play for our investing customers is appropriate at this time.

Regulated Securities Transactions for non-exempt securities are completed by U.S. Sterling Securities Inc. CRD#35912, for institutional customers only. For FDIC insured exempt CD issues which U.S. Sterling Capital sells on an agency, basis the firm is a FDIC exempt second tier broker subject to SEC regulation, with customer funds being held by a FDIC registered bank or equivalent licensed banking institution pursuant to state/federal banking regulations. The firm does not sell or offer any non-FDIC insured CD products.

Please find additional information herein to clarify regulatory and compliance procedures for U.S. Sterling Companies and its Designated Examination Authorities (DEA).

As a private firm, U.S. Sterling Capital, the parent company, does not require an independent audit of its financial data. Instead, we can provide you financials that represent management's needs provided by our accounting firm, nor does the firm prepare an Annual Report for public distribution.

Our companies stand ready to provide any other additional documents you may require. Please be advised the firm operates at a very high level of integrity and internal controls. If you have any legal and or financial operational questions please contact the firm directly. I hope this information is satisfactory to your staff.

Sincerely,

Herbert A. Orr, Jr.
President & CEO

2013 Privacy Policy

Notice of Privacy Policy and Practices

Please read this Privacy Policy carefully. It has information about our policies for the collection, use, disclosure, and protection of information we collect and maintain. It is important for you to know we do not sell or share Customer Information with marketers outside the U.S. Sterling Securities and their service providers.

U.S. Sterling Capital, Corp. recognizes and respects the privacy concerns and expectations of our customers, including individuals who provide their nonpublic personal information to U.S. Sterling Capital, Corp.

U.S. Sterling Capital has an information security program, which incorporates the following policies:

1. Ensure the security and confidentiality of personal information;
2. Protect against any anticipated threats or hazards to the security or integrity of personal information; and
3. Protect against any unauthorized access to or use of personal information that could result in substantial harm or inconvenience to our valued customers.

This notice is provided so that you will know what kinds of information we collect about our customers and the circumstances in which that information may be disclosed to third parties who are not affiliated with the U.S. Sterling.

Collection of Customer Information

We collect nonpublic personal information about our customers from the following sources:

- Account Applications and other forms, which may include a customer's name, address and social security number;
- Account History, including information about the transactions and balances in customers' accounts; and
- Correspondence, written, or telephonic between a customer and U.S. Sterling Securities.

Disclosure of Customer Information

We may disclose any or all of the information described above to third parties who are not affiliated with the U.S. Sterling only under one or more of these circumstances:

- As authorized – if you request or authorize the disclosure of the information
- As permitted by law – for example, limited sharing of information with companies that work for us such as the investment adviser, the custodian, the transfer agent, the distributor and the administrator.

- In other situations – we may also disclose this information to non-affiliated third parties when permitted or required by law. This may include disclosure in connection with a subpoena or similar legal process, an investigation or an audit or examination.

This notice and disclosure applies to the following affiliated companies and/or subsidiaries. When applicable, the companies do not share personal or private information with third party concerns. Information required to process customer account information is kept confidential and secured and is utilized by the associated companies to engage customer specified requirements:

U.S. Sterling Capital, Corp.
U.S. Sterling Securities, Inc.
First Southwest Clearing

First Southwest Securities, our clearing agent, certifies that it will keep personal information that U.S. Sterling provides to First Southwest confidential, and will use the information only to provide the services we've asked them to perform.

Security, Safeguarding and Destruction of Customer Information and Reports

We restrict access to nonpublic personal information about you to those employees who need to know that information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.

Opt In Opt Out

U.S. Sterling does not share, sell, or forward any personal or business data with any third party entity not involved with engaging the business activities within your account. Information is kept private. If this changes in the future, we will sent you a notification with instructions on how to opt out.

For additional information or for any questions please call the
U.S. Sterling Privacy Coordinator at: 800-935-9300
or
Contact us in writing at:

U.S. Sterling Capital, Corp.
Privacy Security Coordinator
1393 Veterans Memorial Highway, Suite 412N
New York, NY 11788

You may also FAX your request or communications to:
631-360-2840

March 1, 2013

Board of Directors
U.S. Sterling Capital, Corp.

I have compiled the accompanying consolidated statement of financial position of U.S. Sterling Capital, Corp. and U.S. Sterling Securities, Inc. as of December 31, 2012.

The accompanying financial statement has not been audited or reviewed, and accordingly, does not include or express an independent opinion, other than the representation of management.

The attached financial statement presents the financial position of the U.S. Sterling companies (U.S. Sterling Capital, Corp. and its subsidiary U.S. Sterling Securities, Inc.) as of December 31, 2012. As a private corporation, we do not offer or publish other financial information including comparative analysis, cash flows, notes or other disclosures.

U.S. Sterling Capital, Corp.

Herbert A. Orr, Jr.
President & CEO

U.S. Sterling Capital Corp.

Consolidated

Balance Sheet

As of December 31, 2012

ASSETS

CURRENT ASSETS		
Cash	$ 363,945	
Accounts Receivable	257,779	
Total Current Assets		$ 621,724
FIXED ASSETS (Net Accumulated Depreciation)		6,609
OTHER ASSETS		
Prepaid Expenses	13,613	
Security Deposit	43,355	
Clearing Account	132,404	
Loan to other companies	80,000	
Total Other Assets		269,372
TOTAL ASSETS		$ 897,705

LIABILITIES & STOCKHOLDERS' EQUITY

CURRENT LIABILITIES		
Accounts Payable	$ 56,362	
Total Other Current Liabilities	$ 43,951	
Total Current Liabilities		$ 100,313
LONG TERM LIABILITIES		
Notes Payable		341,539
Total Long Term Liabilities		
STOCKHOLDERS' EQUITY		
Common Stock (10,000 no par)	20	
Additional Paid in Capital	275,114	
Retained Earnings	180,719	
Total Stockholders' Equity		455,853
TOTAL LIABILITIES & STOCKHOLDERS' EQUITY		$ 897,705

For Executive Information Purposes - Internal Use Only - Company Confidential

US Sterling Companies Consolidated Financials

US Sterling Securities, Inc., 100% wholly owned subsidiary
of US Sterling Capital Corp.

US Sterling Companies do not hold Customer investment assets, nor it's cusrodian accounts.
All Securities are held by the bank, credit union or our Clearing firm, First Southwest Co.

US Sterling Companies do not hold Customer investment assets, nor it's cusrodian accounts.
All Securities are held by the bank, credit union or our Clearing firm, First Southwest Co.

2013 U.S. Sterling Securities, Inc.'s Business Continuity Planning

Smart Planning for Disruptions – Important Information

U.S. Sterling has developed a Business Continuity Plan on how we will respond to events that significantly disrupt our business. Since the timing and impact of disasters and disruptions is unpredictable, we will have to be flexible in responding to actual events as they occur. With that in mind, we are providing you with this information on our business continuity plan. We care about your business and the ability to serve you without disruption.

Contacting Us – If after a significant business disruption you cannot contact us as you usually do at 631-360-2829, you should call our alternative number 800-935-9300. If you cannot access us through either of those means, you should contact our clearing firm, First Southwest Company at 800-678-3792 or online at www.firstsw.com for instructions on how it may provide prompt access to funds and securities, enter certain orders and process other trade-related, cash and security transfer transactions for our important customers.

Our Business Continuity Plan – We plan to quickly recover and resume business operations after a significant business disruption and respond by safeguarding our employees and important property. By making a financial and operational assessment as panned, we can protect the firm's books and records and allowing our customers to transact business. In short, our business continuity plan is designed to permit our firm to resume operations as quickly as possible, given the scope and severity of any significant business disruption.

Our business continuity plan addresses: data backup and recovery; all mission critical systems; financial and operational assessments; alternative communications with customers, employees, and regulators; alternate physical location of employees; critical supplier, contractor, bank and counter-party impact; regulatory reporting; and assuring our customers prompt access to their funds and securities if we are unable to continue our business operations under a protracted communication interruption situation.

Our clearing firm, First Southwest Company, backs up some of our important records in several geographically separate areas. While every emergency situation poses unique problems based on external factors, such as time of day and the severity of the disruption, we have been advised by our clearing firm that its objective is to restore its own operations and be able to complete existing transactions and accept new transactions and payments within 24 hours or less. Your orders and requests for funds and securities could be delayed during this period.

Varying Disruptions – Significant business disruptions can vary in their scope, such as only our firm, a single building housing our firm, the business district where our firm is located, the city where we are located, or the whole region. Within each of these areas, the severity of the disruption can also vary from minimal to severe. In a disruption to only our firm or a building housing our firm, we will transfer our operations to a local site when needed and expect to recover and resume business within 24 hours. In a disruption affecting our business district, city, or region, we will transfer our operations to a site outside of the affected area, and recover and resume business within 24 hours. In either situation, we plan to continue in business, transfer operations to our clearing firm if necessary, and notify you through by email, by phone or provide information our customer emergency number detailing how to contact us. If

the significant business disruption is so severe that it prevents us from remaining in business, we will assure our customer's prompt access to their funds and securities, by providing continuity through our clearing firm First Southwest Company.

For more information – If you have questions about our business continuity planning, you can contact us at info@ussterlingsec.com or by calling our compliance department at 631-360-2829

Fiscal Year 2013

Dear Customer:

Your institution has asked that U.S. Sterling perform on your behalf the customer identification and/or identity verification procedures on customers referred to you by U.S. Sterling as required by Section 326 of the USA Patriot Act. We hereby agree to do so or to have our agent(s) do so. The procedures to be performed for your institution are the following:

- CIP – Customer Identification Procedures – documentary and non-documentary, Section 326 Patriot Act.
- OFAC Checks – FINRA, Requirements office of assets control reviews
- FinCEN and Treasury recording & reporting procedures.

We hereby certify to you that we are a financial institution that is subject to a rule implementing 31 USC 5318(h) and that we are regulated by a federal designated examination authority (DEA). We hereby agree to certify to you annually that we have implemented our anti-money laundering program and that we (or our agents) will perform the above procedures for you. All terms used in this letter agreement have the meanings assigned to them in 31 CFR 103.121.

In addition, be advised that U.S. Sterling Securities, Inc., and its parent company, U.S. Sterling Capital Corp. fully complies with and subscribes to all provisions of the Gramm-Leach-Bliley Financial Modernization Act which requires U.S. Sterling to provide protection for all our customer accounts. As a provider or processor of financial services we do not share customer information except wherein authorized or required for clearing or mandatory service demands. Please find enclosed or attached a disclosure document for your execution and special notification on your rights to Privacy and our company's policy to protect important customers of the U.S. Sterling Companies.

Sincerely,

Herbert A. Orr, Jr.
President & CEO

Edward Gregory and Associates, LLC

East Brunswick, N.J. 08816

Fiscal Year 2011-2012 Independent AML Inspection Certification

To Whom it May Concern:

The U.S. Sterling companies serve primarily Federal and State registered and licensed institutions throughout the United States; the firm, currently has no international locations, or customers located outside of the U.S.A. The firm engages a complete and thorough Anti-Money Laundering (AML) program using conventional and proprietary methods & systems. The firm has a current in-house program that verifies the integrity of the capital process at several stages in transactional business, while simultaneously verifying the integrity of the participant companies that the firm conducts its business. Confidential non material findings of fact was provided to the company for the current year under review.

For the fiscal year 2011-2012 U.S. Sterling has implemented a program reasonably designed to assure enterprise wide compliance referenced in FFIEC Examination Manual dated April29, 2010 which expanded bank AML requirements to all financial institutions and businesses engaging in banking related financial transactions. Pursuant to the authority contained in 31 U.S.C. 5318A Section 311 of the Uniting and Strengthening America Act which provided Appropriate Tools Required to Intercept and Obstruct, The Terrorism Act of2001 (USA PATRIOT Act) which added Section 5318A to the Bank Secrecy Act which may conclude that a certain jurisdiction and/or institutions (or an International class of transactions or a type of

account is a primary money laundering target location) the firm tested satisfactorily in its compliance operations to interdict potential violators and/or capturing of unlawful activities of various entities. This act requires domestic financial institutions and domestic financial agencies to take certain "special measures" against the much money laundering concern. U.S. Sterling had a program in place to interdict and identify these entities and assets, and take the appropriate action.

Therefore, in our opinion, U.S. Sterling, for the time period reviewed, was in material compliance with the provisions of the US Patriot Act Section(s) 352 & 356 and the Bank Secrecy Act and US Treasury Regulations specially 31 CFR Part I 03 Customer Identification Programs for Broker-Dealers. In addition the firm was in compliance with the US Office of Foreign Asset Control (OFAC) requirements for screening SDN entities and targeted countries, individuals & companies.

In our opinion U.S. Sterling was found to be in compliance with currently in force regulation FINRA Rule 3310 which require member firms and organizations to establish risk-based AML compliance programs. Our findings indicate that U.S. Sterling completed its AML mission satisfactorily for the audit year from July 15, 2011 to July 15, 2012, the timeframe under independent audit by our inspection personnel.

Sincerely,

Edward G. Samson, C.P.A.

Edward G. Samson, CPA

2010 US Sterling Securities, Inc. (USSI) Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

UPDATED AS OF FEBRUARY 1, 2010 AML- CIP- BSA REGULATIONS

1. Firm Policy

It is the policy of USSI to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the 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 either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable BSA regulations and FINRA rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

Rules: 31 C.F.R. § 103.120(c); FINRA Rule 3310.

2. AML Compliance Person Designation and Duties

The firm has designated Herbert A. Orr as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program. Herbert A. Orr has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training, including over twenty years in managing a securities business. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, and. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SAR-SFs) are filed with the Financial Crimes Enforcement Network (FinCEN) when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

The firm will provide FINRA with contact information for the AML Compliance Person, including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile number through the FINRA Contact System (FCS). The firm will promptly notify FINRA of any change in this information through FCS and will review, and if necessary update, this information within 17 business days after the end of each calendar year. The annual review of FCS information will be conducted by George Goldman Co-CCO or Herbert Orr, CCO and will be completed with all necessary updates being provided no later than 17 business days following the end of each calendar year. In addition, if there is any change to the information, George Goldman will update the information promptly, but in any event not later than 30 days following the change.

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310, NASD Rule 1160.
Resources: NTM 06-07; NTM 02-78. Firms can submit their AML Compliance Person information through FINRA's FCS Web page.

3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

a. FinCEN Requests Under USA PATRIOT Act Section 314(a)

We will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (a 314(a) Request) by immediately searching our records 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 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure Web site. We understand that we have 14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request. We will designate through the FINRA Contact System (FCS) one or more persons to be the point of contact (POC) for 314(a) Requests and will promptly update the POC information following any change in such information. (*See also* Section 2 above regarding updating of contact information for the AML Compliance Person.) Unless otherwise stated in the 314(a) Request or specified by FinCEN, we are required to search those documents outlined in FinCEN's FAQ. If we find a match, Brian Orr, will report it to FinCEN via FinCEN's Web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (for example, if FinCEN limits the search to a geographic location), we will structure our search accordingly.

If Brian Orr searches our records and does not find a matching account or transaction, then B. Orr will not reply to the 314(a) Request. We will maintain documentation that we have performed the required search physically reviewing the files due to the relatively low number of Institutional Customer accounts

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. Herbert Orr and George Goldman will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

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

Unless otherwise stated in the 314(a) Request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

Rule: 31 C.F.R. § 103.100.
Resources: FinCEN press release (2/6/03); FinCEN press release (2/12/03); NASD Member Alert (2/14/03); FinCEN's 314(a) Fact Sheet (11/18/08).

b. National Security Letters

National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records of our firm. NSLs are highly confidential. No broker-dealer, officer, employee or agent of our broker-dealer can disclose to any person that a

government authority or the FBI has sought or obtained access to records. If the Firm receives an NSLs must have policies and procedures in place for processing and maintaining the confidentiality of NSLs. If you file a Suspicious Activity Report (SAR-SF) after receiving a NSL, the SAR-SF should not contain any reference to the receipt or existence of the NSL.

Resource: *FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 8 (National Security Letters and Suspicious Activity Reporting) (4/2005)*.

c. Grand Jury Subpoenas

The Firm understands that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a Suspicious Activity Report (SAR-SF). When we receive a grand jury subpoena, we will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and file a SAR-SF in accordance with the SAR-SF filing requirements. We understand that none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, we will process and maintain the subpoena by sequestering all documents with the Executive Rep/CEO and not communicate nor share this information as in a Chinese wall. If we file a SAR-SF after receiving a grand jury subpoena, the SAR-SF will not contain any reference to the receipt or existence of the subpoena. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Resources: *FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 10 (Grand Jury Subpoenas and Suspicious Activity Reporting) (5/2006)*.

d. Voluntary Information Sharing With Other Financial Institutions Under USA PATRIOT Act Section 314(b)

We do not share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. H. Orr, G Goldman and B. Orr will ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. We will use the notice form found at FinCEN's Web site. 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 to financial institutions *with which we are affiliated* and that 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, for example, by segregating it from the firm's other books and records when and if sharing occurs.

We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.

Rule: 31 C.F.R. § 103.110.
Resources: FinCEN Financial Institution Notification Form; FIN-2009-G002: Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act (06/16/2009).

e. Joint Filing of SARs by Broker-Dealers and Other Financial Institutions

We may not file joint SARs. We will share only permissible information about a particular suspicious transaction with any broker-dealer, as appropriate, involved in that particular transaction for purposes of determining whether we will file jointly a SAR-SF.

We will share information about particular suspicious transactions with our clearing broker for purposes of determining whether we and our clearing broker will file jointly a SAR-SF. In cases in which we file a joint SAR-SF for a transaction that has been handled both by us and by the clearing broker, we may share with the clearing broker, if lawful, a copy of the filed SAR-SF.

If we determine it is appropriate to jointly file a SAR-SF, we understand that we cannot disclose that we have filed a SAR-SF to any financial institution except the financial institution that is filing jointly. If we determine it is not appropriate to file jointly (*e.g.*, because the SAR-SF concerns the other broker-dealer or one of its employees), we understand that we cannot disclose that we have filed a SAR-SF to any other financial institution or insurance company.

Rules: 31 C.F.R. §103.19; 31 C.F.R. § 103.38; 31 C.F.R. § 103.110.

f. Sharing SAR-SFs With Parent Companies

Because we are a subsidiary, we may share SAR-SFs with US Sterling Capital Corp USSC. Before we share SAR-SFs with USSC, we will have in place written confidentiality agreements or written arrangements that USSC protect the confidentiality of the SAR-SFs through appropriate internal controls.

Resources: FinCEN Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities (1/20/06).

4. Checking the Office of Foreign Assets Control Listings

Before opening an account, and on an ongoing basis, Shawn Orr and Brian Orr will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. (*See* the OFAC Web site for the SDN list and listings of current sanctions and embargoes). Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. *See also* FINRA's OFAC Search Tool that screens names against the SDN list. B Orr will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and he will document the review.

If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. We will also call the OFAC Hotline at (800) 540-6322 immediately.

Our review will include customer accounts, transactions involving customers (including activity that passes through the firm such as wires) and the review of customer transactions that involve physical security certificates or application-based investments (*e.g.*, mutual funds).

Resources: SEC AML Source Tool, Item 12; OFAC Lists Web page (including links to the SDN List and lists of sanctioned countries); FINRA's OFAC Search Tool. You can also subscribe to receive updates on the OFAC Subscription Web page. See also the following OFAC forms: Blocked Properties Reporting Form; Voluntary Form for Reporting Blocked Transactions; Voluntary Form for Reporting Rejected Transactions; OFAC Guidance Regarding Foreign Assets Control Regulations for the Securities Industry.

5. Customer Identification Program

USSI is required to have and follow reasonable procedures to document and verify the identity of their customers who open new accounts. These procedures must address the types of information the firm will collect from the customer and how it will verify the customer's identity. These procedures must enable the firm to form a reasonable belief that it knows the true identity of its customers. The final rule, which FinCEN and the SEC jointly issued on April 30, 2003, applies to all new accounts opened on or after October 1, 2003.

USSI's customer identification program (CIP) is evidenced here in writing and is a part of the firm's AML compliance program.

Note that the CIP rule applies only to "customers" who open new "accounts" with a broker-dealer. Specifically, the CIP rule defines a "customer" 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. "Customer" does not refer to persons who fill out account opening paperwork or who provide information necessary to establish an account, if such persons are not the accountholder as well.

Also, for purposes of the CIP rule's definition of customer, the following entities are excluded from the definition of "customer":

- a financial institution regulated by a federal functional regulator (that is, an institution regulated by the Board of Governors of the Federal Reserve;
- Federal Deposit Insurance Corporation;
- National Credit Union Administration;
- Office of the Comptroller of the Currency;
- Office of Thrift Supervision; Securities and Exchange Commission; or
- Commodity Futures Trading Commission) 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 (now designated as either a NASDAQ Global Market Security or a NASDAQ Global Select Market Security) listed on the NASDAQ Stock Market, with the exception of stock or interests listed under the separate "NASDAQ Small-Cap Issues" (now known as NASDAQ Capital Markets) heading (but only to the extent of domestic operations for any such persons that are financial institutions, other than banks); or

- a person that has an existing account with the broker-dealer, provided the broker-dealer has a reasonable belief that it knows the true identity of the person.

Accordingly, our broker-dealer is not 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 the CIP 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 borrowing 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).

Rule: 31 C.F.R. §103.122(a)(1)(i)(ii) and 103.122(a)(4)(i)(ii).
Resources: SEC Staff Q&A Regarding the Broker-Dealer Customer Identification Program Rule (October 1, 2003); NTM 03-34; FIN-2006-G007: Frequently Asked Question: Customer Identification Program Responsibilities under the Agency Lending Disclosure Initiative (April 25, 2006).

Note that while our clearing firm does not have an obligation to perform CIP for our introduced customer our the clearing firm and as USSI is the introducing firm we have entered into a clearing agreement under which the functions of opening and approving customer accounts and directly receiving and accepting orders from the introduced customer are allocated exclusively to USSI, the introducing firm and the functions of extending credit, safeguarding funds and securities, and issuing confirmations and statements are allocated to the clearing firm. The clearing firm has a failsafe mechanism wherein all accounts are vetted through their checking systems. This position also extends to piggybacking arrangements[1] where, pursuant to a piggybacking arrangement when applicable, with any introducing firm, the piggybacking firm retains the functions of opening and approving customer accounts and directly receiving and accepting orders from introduced customers. Thus, under a piggybacking arrangement, the clearing firm and the introducing firm are not obligated to perform CIP for the customers introduced by the piggybacking firm.

Please note that any clearing firm's and introducing firm's AML programs should contain risk-based policies, procedures, and controls for assessing the money laundering risk

[1] In a "piggybacking" arrangement, an introducing firm (the piggybacking firm) does not enter into a clearing agreement with a clearing firm, but rather establishes a relationship with an introducing firm that has established a clearing arrangement with a clearing firm, thus piggybacking off the introducing firm's clearing agreement. FIN-2008-G002 at p.2.

posed by its fully disclosed clearing arrangements, for monitoring and mitigating that risk, and for detecting and reporting suspicious activity.

Resources: FIN-2008-G002: Customer Identification Program Rule No-Action Position Respecting Broker-Dealers Operating Under Fully Disclosed Clearing Agreements According to Certain Functional Allocations (March 4, 2008) and FIN-2008-R008 (Bank Secrecy Act Obligations of a U.S. Clearing Broker-Dealer Establishing a Fully Disclosed Clearing Relationship with a Foreign Financial Institution) (June 3, 2008)

In addition to the information we must collect under FINRA Rule 2010 (Standards of Commercial Honor and Principles of Trade), NASD Rules 2310 (Recommendations to Customers - Suitability) and 3110 (Books and Records) and Securities Exchange Act of 1934 (Exchange Act) Rules 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 (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 the required adequate CIP notice to customers that we will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government. *See* Section 5.g. (Notice to Customers) for additional information.

We will collect information to determine whether any entity opening an account would be excluded as a "customer," pursuant to the exceptions outlined in 31 CFR 103.122(a)(4)(ii) (*e.g.*, documentation of a company's listing information, licensing or registration of a financial institution in the U.S, and status or verification of the authenticity of a government agency or department).

Rule: 31 C.F.R. §103.122.
Resources: SEC Staff Q&A Regarding the Broker-Dealer Customer Identification Program Rule (October 1, 2003); NTM 03-34.

a. Required Customer Information

Prior to opening an account, S Orr and administrative staff will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account:

(1) the name;
(2) date of birth (for an individual);
(3) an address, which will be a residential or business street address (for an individual), an Army Post Office (APO) or Fleet Post Office (FPO) box 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); and

(4) 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 notify the customer, we will confirm to new applicant filed before the customer opens the account and the firm must 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.

Rule: 31 C.F.R. §103.122(b)(2)(i)(A) & § 103.122(b)(2)(i)(B).

b. Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Person will be notified so that we can determine whether we should report the situation to FinCEN on a 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. S Orr as a designee and B Orr will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both which includes several levels of industry cross check using government and private sources. 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 necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying

the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or 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.

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:

- 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 indirectly, which is MIS the top industry resource;

- Checking references with other financial institutions; or

- Obtaining a financial statements and other proprietary publications and government database(s).

We will use non-documentary methods of verification when:

(1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
(2) the firm is unfamiliar with the documents the customer presents for identification verification;
(3) the customer and firm do not have face-to-face contact; and
(4) there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

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, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a SAR-SF in accordance with applicable laws and regulations.

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 jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified. We will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient: All required documentation under federal regulation for institutional activities under enterprise wide compliance for banks and credit unions. For individuals third party information may be required – credit related or bank related or professional related data verifications.

Rule: 31 C.F.R. §103.122(b).

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: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close an account after attempts to verify customer's identity fail; and (4) determine whether it is necessary to file a SAR-SF in accordance with applicable laws and regulations.

Rule: 31 C.F.R. §103.122(b)(2)(iii).

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 discrepancies identified in the verification process. 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 also keep records containing a description of the resolution of each substantive discrepancy

discovered when verifying the identifying information obtained. We will retain 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.

Rule: 31 C.F.R. §103.122(b)(3).

f. Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, 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), 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 separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

Rule: 31 C.F.R. §103.122(b)(4).
Resources: NTM 02-21, page 6, n.24; 31 C.F.R. § 103.122.

g. Notice to Customers

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by federal law. We will use the following method to provide notice to customers which is not limited to telephone, online or walk in as is appropriate.

> **Important Information About Procedures for Opening a New Account**
> To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.
>
> **What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.**

Rule: 31 C.F.R. §103.122(b)(5).

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 or our clearing firm) of some or all of the elements of our CIP 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.

Rule: 31 C.F.R. § 103.122(b)(6).
Resources: No-Action Letters to the Securities Industry and Financial Markets Association (SIFMA) (formerly known as the Securities Industry Association (SIA)) (February 12, 2004; February 10, 2005; July 11, 2006; and January 10, 2008).

6. General Customer Due Diligence

The firm may deem some accounts to be of higher risk based on:

- customer's actual or anticipated business activity;
- customer's ownership structure;
- anticipated or actual volume and types of transactions;
- transactions involving high-risk jurisdictions.

Higher risk accounts should be subject to greater due diligence.

It is important to our AML and SAR-SF reporting program that we obtain sufficient information about each customer to allow us to evaluate the risk presented by that customer and to detect and report suspicious activity. When we open an account for a customer, the due diligence we perform may be in addition to customer information obtained for purposes of our CIP.

For each account meeting the criteria that falls outside of normal ranges as defined by the operations office(essential a unlicensed or unregulated banking operation), we will take steps to obtain sufficient customer information to comply with our suspicious activity reporting requirements. Such information should include information to file a SAR gleaning information for law enforcement on case by case basis.

- the customer's business;
- the customer's anticipated account activity (both volume and type);
- the source of the customer's funds.

For accounts that we have deemed to be higher risk, we will obtain the following information:

- the purpose of the account;
- the source of funds and wealth;
- the beneficial owners of the accounts;
- the customer's (or beneficial owner's) occupation or type of business;
- financial statements;
- banking references;
- domicile (where the customer's business is organized);
- description of customer's primary trade area and whether international transactions are expected to be routine;
- description of the business operations and anticipated volume of trading;
- explanations for any changes in account activity.

We will also ensure that the customer information remains accurate by regular updating of the account and reviewing the account each year.

7. Correspondent Accounts for Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Foreign Shell Banks

Our firm does not establish, maintain, administer or manage correspondent accounts for foreign banks, as this is our firm's policy and our firm has internal controls such as 2 principal review of any new account, to detect any attempt to open a correspondent account.

We will identify foreign bank accounts and any such account that is a correspondent account (any account that is established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank) for foreign shell banks by independent administration verification with the local government regulator. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Person, who will terminate any verified correspondent account in the United States for a foreign shell

bank. We will also terminate any correspondent account that we have determined is not maintained by a 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 regulations regarding shell banks within the time periods specified in those regulations.

Rules: 31 C.F.R. §§103.175, 103.177.

b. Certifications

We will require any foreign bank account holders to identify the owners of the foreign bank if it is not publicly traded, the name and street address of a person who resides in the United States and is authorized and has agreed to act as agent for acceptance of legal process, and an assurance that the foreign bank is not a shell bank nor is it facilitating activity of a shell bank. In lieu of this information the foreign bank may submit the Certification Regarding Correspondent Accounts For Foreign Banks provided in the BSA regulations. We will re-certify when we believe that the information is no longer accurate or at least once every three years.

Rules: 31 C.F.R. §§ 103.175, 103.177.
Resources: 31 C.F.R., Pt. 103, Subpt. I, App. A (Certification Regarding Correspondent Accounts for Foreign Banks); FIN-2006-G003: Frequently Asked Questions: Foreign Bank Recertifications under 31 C.F.R. § 103.77 (February 3, 2006).

c. Recordkeeping for Correspondent Accounts for Foreign Banks

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 when and if applicable.

Rules: 31 C.F.R. §§ 103.175, 103.177.

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

When we receive a written request from a federal law enforcement officer for information identifying the non-publicly traded owners of any foreign bank for which we maintain a correspondent account in the United States and/or the name and address of a person residing in the United States who is an agent to accept service of legal process for a foreign bank's correspondent account, we will provide that information to the requesting officer not later than seven days after receipt of the request. We will close, within 10 days, any correspondent account for a foreign bank that we learn from FinCEN

or the Department of Justice has failed to comply with a summons or subpoena issued by the Secretary of the Treasury or the Attorney General of the United States or has failed to contest such a summons or subpoena. We will scrutinize any correspondent 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 correspondent accounts.

Rule: *31 C.F.R. § 103.185.*

8. Due Diligence and Enhanced Due Diligence Requirements for Correspondent Accounts of Foreign Financial Institutions

a. Due Diligence for Correspondent Accounts of Foreign Financial Institutions

A foreign financial institution is:

(1) a foreign bank;
(2) any branch or office located outside the United States of a broker-dealer; futures commission merchant or introducing broker; or open-end mutual fund company;
(3) any other person organized under foreign law (other than a branch or office of such person in the United States) that, if it were located in the United States, would be a broker-dealer; futures commission merchant or introducing broker; or open-end mutual fund company; and
(4) any person organized under foreign law (other than a branch or office of such person in the United States) that is engaged in the business of, and is readily identifiable as: (a) a currency dealer or exchanger; or (b) a money transmitter.

A person, however, is not "engaged in the business" of a currency dealer, a currency exchanger or a money transmitter if such transactions are merely incidental to the person's business.

A "correspondent account" is defined in this context as any account established for a foreign financial institution to receive deposits from, or to make payments or other disbursement on behalf of, the foreign financial institution, or to handle other financial transactions for the foreign financial institution. "Account" is defined as any formal relationship established with a broker or dealer in securities to provide regular services to effect transactions in securities, including but not limited to, the purchase or sale of securities and securities loaned and borrowed activity, and to hold securities or other assets for safekeeping or as collateral.

For broker-dealers, correspondent accounts established on behalf of foreign financial institutions include, but are not limited to: (1) accounts to purchase, sell, lend, or otherwise hold securities, including securities repurchase programs; (2) prime brokerage accounts that clear and settle securities transactions for clients; (3) accounts for trading

foreign currency; (4) custody accounts for holding securities or other assets in connection with securities transactions as collateral; and (5) over-the-counter derivative contracts.

On January 30, 2008, FinCEN issued guidance clarifying that covered financial institutions (which includes U.S. broker-dealers) presenting a negotiable instrument for payment to a foreign financial institution on which the instrument is drawn would not, by itself, be establishing a correspondent account between the covered financial institution and the paying institution. See FinCEN Guidance on Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment (1/30/08).

USSI will conduct an account inquiry to determine whether a foreign financial institution has a correspondent account established, maintained, administered or managed by the firm.

If we have correspondent accounts for foreign financial institutions, which is unlikely, we will assess the money laundering risk posed, based on a consideration of relevant risk factors. We can apply all or a subset of these risk factors depending on the nature of the foreign financial institutions and the relative money laundering risk posed by such institutions.

The relevant risk factors can include:

- the nature of the foreign financial institution's business and the markets it serves;
- the type, purpose and anticipated activity of such correspondent account;
- the nature and duration of the firm's relationship with the foreign financial institution and its affiliates;
- the anti-money laundering and supervisory regime of the jurisdiction that issued the foreign financial institution's charter or license and, to the extent reasonably available, the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered; and
- information known or reasonably available to the covered financial institution about the foreign financial institution's anti-money laundering record.

In addition, our due diligence program will consider additional factors that have not been enumerated above when assessing foreign financial institutions that pose a higher risk of money laundering.

We have reviewed our accounts and we do not have, nor do we intend to open or maintain, correspondent accounts for foreign financial we do monitor for these accounts and will not permit opening of so designated accounts.

Rules: 31 C.F.R. §§ 103.175, 103.176.
Resources: FIN-2006-G009 Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries (May 10, 2006).

b. Enhanced Due Diligence

The BSA, as amended by Section 312 of the USA PATRIOT Act, and the rules promulgated thereunder require, in part, that a firm's due diligence program for correspondent accounts of foreign financial institutions include the performance of enhanced due diligence on correspondent accounts for any foreign bank that operates under:

(1) an offshore banking license;
(2) a banking license issued by a foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the U.S. representative to the group or organization concurs; or
(3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

We will assess any correspondent accounts for foreign financial institutions to determine whether they are correspondent accounts that have been established, maintained, administered or managed for any foreign bank that operates under:

(1) an offshore banking license;
(2) a banking license issued by a foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the U.S. representative to the group or organization concurs; or
(3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

If we determine that we have any correspondent accounts for these specified foreign banks, we will perform enhanced due diligence on these correspondent accounts. The enhanced due diligence that we will perform for each correspondent account will include, at a minimum, procedures to take reasonable steps to:

(1) conduct enhanced scrutiny of the correspondent account to guard against money laundering and to identify and report any suspicious transactions. Such scrutiny will not only reflect the risk assessment that is described in Section 8.a. above, but will also include procedures to, as appropriate:

(i) obtain (*e.g.*, using a questionnaire) and consider information related to the foreign bank's AML program to assess the extent to which the foreign bank's correspondent account may expose us to any risk of money laundering;

(ii) monitor transactions to, from or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity (this monitoring may be conducted manually or electronically and may be done on an individual account basis or by product activity); and

(iii) obtain information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account (a correspondent account maintained for a foreign bank through which the foreign bank permits its customer to engage, either directly or through a subaccount, in banking activities) and the sources and beneficial owners of funds or other assets in the payable-through account.

(2) determine whether the foreign bank maintains correspondent accounts for other foreign banks that enable those other foreign banks to gain access to the correspondent account under review and, if so, to take reasonable steps to obtain information to assess and mitigate the money laundering risks associated with such accounts, including, as appropriate, the identity of those other foreign banks; and

(3) if the foreign bank's shares are not publicly traded, determine the identity of each owner and the nature and extent of each owner's ownership interest. We understand that for purposes of determining a private foreign bank's ownership, an "owner" is any person who directly or indirectly owns, controls or has the power to vote 10 percent or more of any class of securities of a foreign bank. We also understand that members of the same family shall be considered to be one person.

Rules: 31 C.F.R. §§ 103.175, 103.176.

c. Special Procedures When Due Diligence or Enhanced Due Diligence Cannot Be Performed

In the event there are circumstances in which we cannot perform appropriate due diligence with respect to a correspondent account, we will determine, at a minimum, whether to refuse to open the account, suspend transaction activity, file a SAR-SF, close the correspondent account and/or take other appropriate action.

Rules: 31 C.F.R. §§ 103.175, 103.176.

9. Due Diligence and Enhanced Due Diligence Requirements for Private Banking Accounts/Senior Foreign Political Figures

Described is USSI's due diligence program for "private banking" accounts for non-U.S. persons. 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," which is defined below and includes their immediate family members and close known associates, require enhanced scrutiny. Senior foreign political figures are often referred to as "politically exposed persons" or "PEPs."

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 widely and publicly known (or actually known by the firm) to be a close personal or professional associate of such an individual.

USSI does not open or maintain private banking accounts as defined. While the firm does not anticipate these accounts, this section may be updated to reflect additional requirements that may apply or procedures we may implement.

Rules: 31 C.F.R. §§ 103.175, 103.178.
Resource: Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption.

10. Compliance with FinCEN's Issuance of Special Measures Against Foreign Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern

We do not maintain any accounts (including correspondent accounts) with any foreign jurisdiction or financial institution. However, if FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, we understand that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule.

Rules: 31 C.F.R. §§ 103.186, 103.187, 103.188, 103.192, 103.193.
Resources: Section 311 – Special Measures (for information on all special measures issued by FinCEN); NTM 07-17; NTM 06-41.

11. Monitoring Accounts for Suspicious Activity

USSI has established a risk-based procedures reasonably designed to detect and report suspicious transactions in order to comply with the BSA and FINRA Rule 3310. The risk of suspicious activity will vary for each firm depending on its size and location and based on its business model and the products and services it offers. Your firm can identify that risk by looking at the type of customers it serves, where the customers is located, and the types of products and services it offers.. Higher risk accounts and transactions generally need to be subjected to greater scrutiny.

Our procedures describe how USSI monitors or otherwise identify "red flags." Our firm monitors transactions manually and also uses through automated systems a combination of the two, as the system is reasonably designed to identify and report suspicious activity. The firm notes that the types of suspicious activity that are reportable on SAR-SF are very broad and include, among other things, securities fraud.

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified in Section 11.b. below.) Monitoring will be conducted through the following methods: AML exception reports provided by the clearing firm queries to registered sales persons, risk reports are provided by MIS among other reviews of incidents of trade (unusual institutional activity). The AML Compliance Person or his or her designee namely H. Orr has assigned B. Orr, GSP and he will be responsible for this monitoring, and he will review any activity that our monitoring system detects, as he will determine whether any additional steps are required, will document when and how this

monitoring is carried out, and will report suspicious activities to the appropriate authorities. G Goldman will provide system review and compliance implementation reviews and reports, to verify integrity of the program and provide notices of regulation updates.

We will conduct the following reviews of activity that our monitoring system detects: excessive transfers, MIS list hits, unusual behavior, rep concerns, and periodic listen in of phone communications. We will document our monitoring and reviews as follows: annually or more often as required (account opening, inspection reports, and monthly trade reviews of EOM activity). The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR-SF is filed. Relevant information can include, but not be limited to, the following: all matters that apply to the issue at hand not limited in scope or information or data proximate to an event sequence.

Rules: 31 C.F.R. §103.19; FINRA Rule 3310(a).
Resource: Final Rule Release: 67 Fed. Reg. 44048 (July 1, 2002) ("it is intended that broker-dealers, and indeed every type of financial institution to which the suspicious transaction reporting rules of 31 CFR part 103 apply, will evaluate customer activity and relationships for money laundering risks, and design a suspicious transaction monitoring program that is appropriate for the particular broker-dealer in light of such risks").

a. Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. If a customer or company appears on OFAC's SDN list, we will call the OFAC Hotline at (800) 540-6322. Other contact numbers we will use are: FinCEN's Financial Institutions Hotline ((866) 556-3974) (especially to report transactions relating to terrorist activity), local U.S. Attorney's office (*insert contact number)*, local FBI office (*insert contact number)* and local SEC office (*insert contact number)* (to voluntarily report such violations to the SEC in addition to contacting the appropriate law enforcement authority). If we notify the appropriate law enforcement authority of any such activity, we must still file a timely SAR-SF.

Although we are not required to, in cases where we have filed a SAR-SF that may require immediate attention by the SEC, we may contact the SEC via the SEC SAR Alert Message Line at (202) 551-SARS (7277) to alert the SEC about the filing. We understand that calling the SEC SAR Alert Message Line does not alleviate our obligations to file a SAR-SF or notify an appropriate law enforcement authority.

Rule: 31 C.F.R. § 103.19.
Resources: *FinCEN's Web site*; *OFAC Web page*; *NTM 02-21*; *NTM 02-47*.

b. Red Flags

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

Customers – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.
- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.
- Background is questionable or differs from expectations based on business activities.
- Customer with no discernable reason for using the firm's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an employee not to file required reports or not to maintain required records.
- "Structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.
- Unusual concern with the firm's compliance with government reporting requirements and firm's AML policies.

Certain Funds Transfer Activities

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.
- Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer's business or history. May indicate a Ponzi scheme.
- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

Certain Deposits or Dispositions of Physical Certificates

- Physical certificate is titled differently than the account.
- Physical certificate does not bear a restrictive legend, but based on history of the stock and/or volume of shares trading, it should have such a legend.
- Customer's explanation of how he or she acquired the certificate does not make sense or changes.
- Customer deposits the certificate with a request to journal the shares to multiple accounts, or to sell or otherwise transfer ownership of the shares.

Certain Securities Transactions

- Customer engages in prearranged or other non-competitive trading, including wash or cross trades of illiquid securities.
- Two or more accounts trade an illiquid stock suddenly and simultaneously.
- Customer journals securities between unrelated accounts for no apparent business reason.
- Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.
- Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position and wiring out proceeds.
- Customer's trading patterns suggest that he or she may have inside information.

Transactions Involving Penny Stock Companies

- Company has no business, no revenues and no product.
- Company has experienced frequent or continuous changes in its business structure.
- Officers or insiders of the issuer are associated with multiple penny stock issuers.
- Company undergoes frequent material changes in business strategy or its line of business.
- Officers or insiders of the issuer have a history of securities violations.
- Company has not made disclosures in SEC or other regulatory filings.

- Company has been the subject of a prior trading suspension.

Transactions Involving Insurance Products

- Cancels an insurance contract and directs funds to a third party.
- Structures withdrawals of funds following deposits of insurance annuity checks signaling an effort to avoid BSA reporting requirements.
- Rapidly withdraws funds shortly after a deposit of a large insurance check when the purpose of the fund withdrawal cannot be determined.
- Cancels annuity products within the free look period which, although could be legitimate, may signal a method of laundering funds if accompanied with other suspicious indicia.
- Opens and closes accounts with one insurance company then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.
- Purchases an insurance product with no concern for investment objective or performance.
- Purchases an insurance product with unknown or unverifiable sources of funds, such as cash, official checks or sequentially numbered money orders.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.
- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Other Suspicious Customer Activity

- Unexplained high level of account activity with very low levels of securities transactions.

- Funds deposits for purchase of a long-term investment followed shortly by a request to liquidate the position and transfer the proceeds out of the account.

- Law enforcement subpoenas.

- Large numbers of securities transactions across a number of jurisdictions.

- Buying and selling securities with no purpose or in unusual circumstances (*e.g.*, churning at customer's request).

- Payment by third-party check or money transfer without an apparent connection to the customer.

- Payments to third-party without apparent connection to customer.

- No concern regarding the cost of transactions or fees (*i.e.*, surrender fees, higher than necessary commissions, etc.).

c. Responding to Red Flags and Suspicious Activity

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify Hebert Orr or Brian Orr or George Goldman. Under the direction of the AML Compliance Person, the firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a SAR-SF.

12. Suspicious Transactions and BSA Reporting

USSI is exempt from reporting on a SAR-SF the following violations: (1) a robbery or burglary that is committed or attempted and already reported to appropriate law enforcement authorities; (2) lost, missing, counterfeit or stolen securities that the firm has reported pursuant to Exchange Act Rule 17f-1; and (3) violations of the Federal securities laws or self-regulatory organization (SRO) rules by the firm, its officers, directors, employees or registered representatives, that are reported appropriately to the SEC or SRO, except for a violation of Exchange Act Rule 17a-8, which must be reported on a SAR-SF. However, if USSI relies on one of these exemptions, it may be required to demonstrate that it relied on one of these exemptions and must maintain records, for at least five years, of its determination not to file a SAR-SF based on the exemption.

Rule: 31 C.F.R. §103.19.

a. Filing a SAR-SF

USSI AML Compliance Officer will file SAR-SFs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving $5,000 or more of funds or assets (either individually or in the aggregate) 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 or to avoid any transaction reporting requirement under federal law or regulation;
(2) the transaction is designed, whether through structuring or otherwise, to evade 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 after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
(4) the transaction involves the use of the firm to facilitate criminal activity.

We will also file a SAR-SF and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. In addition, although we are not required to, we may contact that SEC in cases where a SAR-SF we have filed may require immediate attention by the SEC. *See* Section 11 for contact numbers. We also understand that, even if we notify a regulator of a violation, unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR-SF reporting the violation.

We may file a voluntary SAR-SF for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the SAR rule. It is our policy that all SAR-SFs will be reported regularly to the Board of Directors and appropriate 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. The phrase “initial detection” does not mean the moment a transaction is highlighted for review. The 30-day (or 60-day) period begins when an appropriate review is conducted and a determination is made that the transaction under review is “suspicious” within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

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, federal or state securities regulators or SROs 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 will, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency, or an SRO registered with the SEC, decline to produce 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.

Rules: 31 C.F.R. §103.19, FINRA Rule 3310(a).
Resources: FinCEN's Web site contains additional information, including information on the BSA E-Filing System, the SAR-SF Form (fill-in version), and the biannual SAR Activity Reviews and SAR Bulletins, which discuss trends in suspicious reporting and give helpful tips. SAR Activity Review, Issue 10 (May 2006) (documentation of decision not to file a SAR; grand jury subpoenas and suspicious activity reporting, and commencement of 30-day time period to file a SAR); FinCEN SAR Narrative Guidance Package (11/2003), FinCEN Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (10/10/2007);NTM 02-21; NTM 02-47.

b. Currency Transaction Reports

USSI prohibits transactions involving currency and has the following procedures to prevent such transactions: The firm will reject any attempt to delivery currency or unverified bank drafts when applicable since we do not accept cash securities or other tender from consumers. If we discover such transactions have occurred, we will file with FinCEN CTRs for currency transactions that exceed $10,000. Also, we will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a CTR if they total more than $10,000 and are made by or on behalf of the same person during any one business day. We will use the CTR Form provided on FinCEN's Web site.

Rules: 31 C.F.R.§§103.11, 103.22.
Resource: BSA E-Filing System.

c. Currency and Monetary Instrument Transportation Reports

A currency and monetary instrument transportation report (CMIR) must be filed whenever more than $10,000 in currency or other monetary instruments is physically transported, mailed or shipped into or from the United States. A CMIR also must be filed whenever a person receives more than $10,000 in currency or other monetary instruments that has been physically transported, mailed or shipped from outside the United States and a CMIR has not already been filed with respect to the currency or other monetary instruments received. A CMIR is not required to be filed by a securities broker-dealer

mailing or shipping currency or other monetary instruments through the postal service or by common carrier. “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.

USSI prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to us from outside of the United States, and the physical transportation, mailing or shipment of currency or other monetary instruments by any means other than through the postal service or by common carrier. We will file a CMIR with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the U.S. currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time (on one calendar day or, if for the purposes of evading reporting requirements, on one or more days). We will also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal service or by common carrier currency or other monetary instruments of more than $10,000 at one time (on one calendar day or, if for the purpose of evading the reporting requirements, on one or more days). We will use the CMIR Form provided on FinCEN’s Web site.

Rules: 31 C.F.R. §§103.11, 103.23.

d. Foreign Bank and Financial Accounts Reports

The regulations under the BSA require that USSI as a registered broker-dealer, to report and keep records related to any financial interest in, or signature authority over, a bank account, securities account or other financial account that the firm has in a foreign country in which the aggregate value of any accounts exceed $10,000. Foreign bank and financial accounts reports (FBARs) must be filed with the Commissioner of the IRS on or before June 30th of each calendar year for the previous year in which such accounts exist.

USSI compliance will file a FBAR with the IRS 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 provided on the IRS’s Web site.

Rule: 31 C.F.R. §103.24.
Resource: FBAR Form.

e. Monetary Instrument Purchases

Note from USSI compliance: No financial institution may issue or sell a bank check or draft, cashier’s check, money order or traveler’s check for $3,000 to $10,000 inclusive in

currency unless it obtains and records certain information when issuing or selling one or more of these instruments to any individual purchaser. A financial institution issuing or selling one or more of these instruments to any individual purchaser in excess of $10,000 will also need to file a CTR. See Section 12.b.

As USSI does not issue bank checks or drafts, cashier's checks, money orders or traveler's checks in the amount of $3,000 or more, this should not apply. If this changes this section should be updated to included retention or required records.

(a) (1) If the purchaser has a deposit account with us:

(i) (A) the name of the purchaser;

(B) the date of purchase;

(C) the type(s) of instrument(s) purchased;

(D) the serial number(s) of each of the instrument(s) purchased; and

(E) the amount in dollars of each of the instrument(s) purchased.

(ii) In addition, we must verify that the individual is a deposit accountholder or must verify the individual's identity. Verification may be either through a signature card or other file or record provided the deposit accountholder's name and address were verified previously and that information was recorded on the signature card or other file or record; or by examination of a document which is normally acceptable as a means of identification when cashing checks for non-depositors and which contains the name and address of the purchaser. If the deposit accountholder's identity has not been verified previously, we shall verify the deposit accountholder's identity by examination of a document which is normally acceptable within the community as a means of identification when cashing checks for non-depositors and which contains the name and address of the purchaser, and shall record the specific identifying information (*e.g.*, driver's license number and state of issuance).

(2) If the purchaser does not have a deposit account with us:

(i) (A) the name and address of the purchaser;

(B) the Social Security number of the purchaser, or if the purchaser is an alien and does not have a Social Security number, the alien identification number;

(C) the date of birth of the purchaser;

(D) the date of purchase;

(E) the type(s) of instrument(s) purchased;

(F) the serial number(s) of the instrument(s) purchased; and

(G) the amount in dollars of each of the instrument(s) purchased.

(ii) In addition, we shall verify the purchaser's name and address by examination of a document which is normally acceptable within the community as a means of identification when cashing checks for non-depositors and which contains the name and address of the purchaser, and shall record the specific identifying information (*e.g.*, driver's license number and state of issuance).

(b) Contemporaneous purchases of the same or different types of instruments totaling $3,000 or more shall be treated as one purchase. Multiple purchases during one business day totaling $3,000 or more shall be treated as one purchase if an individual employee, director, officer or partner of USSI has knowledge that these purchases have occurred.

(c) We shall keep records required to be kept for a period of five years, and such records shall be made available to the federal and state authorities or SROs upon request at any time.

Rule: 31 C.F.R. § 103.29. See also 31 C.F.R. 103.22(b).
Resources: 52 Fed. Reg. 52250 (October 17, 1994) (Final Rule Amendments to BSA Regulations Relating to Identification Required to Purchase Bank Checks and Drafts, Cashier's Checks, Money Orders, and Traveler's Checks).

f. Funds Transmittals of $3,000 or More Under the Travel Rule

When USSI is the transmittor's financial institution in funds of $3,000 or more (USSI does not engage this position since it does not funds or securities), we will retain either the original or a copy (*e.g.*, microfilm, electronic record) of the transmittal order. We will also record on the transmittal order the following information: (1) the name and address of the transmittor; (2) if the payment is ordered from an account, the account number; (3) the amount of the transmittal order; (4) the execution date of the transmittal order; and (5)

the identity of the recipient's financial institution. In addition, we will include on the transmittal order as many of the following items of information as are received with the transmittal order: (1) the name and address of the recipient; (2) the account number of the recipient; (3) any other specific identifier of the recipient; and (4) any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

We will also verify the identity of the person placing the transmittal order (if we are the transmitting firm), provided the transmittal order is placed in person and the transmittor is not an established customer of the firm (*i.e.*, a customer of the firm who has 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). If a transmittor or recipient is conducting business in person, we will obtain: (1) the person's name and address; (2) the type of identification reviewed and the number of the identification document (*e.g.*, driver's license); and (3) the person's taxpayer identification number (*e.g.*, Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record the lack thereof. If a transmittor or recipient is not conducting business in person, we shall obtain the person's name, address, and a copy or record of the method of payment (*e.g.*, check or credit card transaction). In the case of transmittors only, we shall also obtain the transmittor's taxpayer identification number (*e.g.*, Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. In the case of recipients only, we shall obtain the name and address of the person to which the transmittal was sent.

Rule: 31 C.F.R. §103.33(f) and (g).

13. AML Recordkeeping

a. Responsibility for Required AML Records and SAR-SF Filing

Our AML Compliance Officer, and his or her designee will be responsible for ensuring that AML records are maintained properly and that SAR-SFs are filed as required.

In addition, as part of our AML program, our firm will create and maintain SAR-SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification (*See* Section 5 above) and funds transmittals. We will maintain SAR-SFs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other recordkeeping requirements, including certain SEC rules that require six-year retention periods (*e.g.*, Exchange Act Rule 17a-4(a) requiring firms to preserve for a period of not less than six years, all records required to be retained by Exchange Act Rule 17a-3(a)(1)-(3), (a)(5), and (a)(21)-(22) and Exchange Act Rule

17a-4(e)(5) requiring firms to retain for six years account record information required pursuant to Exchange Act Rule 17a-3(a)(17)).

Rules: 31 C.F.R. § 103.38, Exchange Act Rule 17a-8 (requiring registered broker-dealers subject to the Currency and Foreign Transactions Reporting Act of 1970 to comply with the BSA regulations regarding reporting, recordkeeping and record retention requirements), FINRA Rule 3310.

b. SAR-SF Maintenance and Confidentiality

We will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, an SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or for information that would disclose that a SAR-SF has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive. *See* Section 11 for contact numbers. 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 Person will handle all subpoenas or other requests for SAR-SFs. [*Describe any other retention or confidentiality procedures of your firm for SAR-SFs.*] We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a SAR according to the provisions of Section 3.d. In cases in which we file a joint SAR for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed SAR.

Rules: 31 C.F.R. §103.19(e); 67 Fed. Reg. 44048, 44054 (July 1, 2002).
Resources: NTM 02-47.

c. Additional Records

BSA regulations require USSI to retain either an original or a microfilm copy or some other form of copy of certain records. 31 C.F.R. §§ 103.33 and 103.35(b).

We shall retain either the original or a microfilm or other copy or reproduction of each of the following when and if applicable (the clearing firm holds all customer accounts):

- A record of each extension of credit in an amount in excess of $10,000, except an extension of credit secured by an interest in real property. The record shall contain the name and address of the person to whom the extension of credit is made, the amount thereof, the nature or purpose thereof and the date thereof;

- A record of each advice, request or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds, checks, investment securities or credit, of more than $10,000 to or from any person, account or place outside the U.S.;

- A record of each advice, request or instruction given to another financial institution (which includes broker-dealers) or other person located within or without the U.S., regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, checks, investment securities or credit, of more than $10,000 to a person, account or place outside the U.S.;

- Each document granting signature or trading authority over each customer's account;

- Each record described in Exchange Act Rule 17a-3(a): (1) (blotters), (2) (ledgers for assets and liabilities, income, and expense and capital accounts), (3) (ledgers for cash and margin accounts), (4) (securities log), (5) (ledgers for securities in transfer, dividends and interest received, and securities borrowed and loaned), (6) (order tickets), (7) (purchase and sale tickets), (8) (confirms), and (9) (identity of owners of cash and margin accounts);

- A record of each remittance or transfer of funds, or of currency, checks, other monetary instruments, investment securities or credit, of more than $10,000 to a person, account or place, outside the U.S.; and

- A record of each receipt of currency, other monetary instruments, checks or investment securities and of each transfer of funds or credit, of more than $10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside the U.S.

Rules: 31 C.F.R. §§ 103.33, 103.35(b).

14. 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 our contractual obligations and] with AML laws. Both our firm and our clearing firm have filed (and kept updated) the necessary annual certifications for such information sharing, which can be found on FinCEN's Web site. As a general matter, we will obtain and use the exception reports offered by our clearing firm in order to monitor customer activity and we will provide our clearing firm with proper customer identification and due diligence information as required to successfully monitor customer transactions. We have discussed how each firm will apportion customer and transaction functions and how we will share information and set forth our understanding in a written document. We understand that the apportionment of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the BSA and its implementing regulations.

Rules: 31 CFR 103.110; FINRA Rule 3310, NASD Rule 3230.

Resources: *FIN-2006-G003: Frequently Asked Questions: Foreign Bank Recertifications under 31 C.F.R. § 103.77 (February 3, 2006)*.

15. Training Programs

We will develop ongoing employee training under the directive of the AML Compliance Officer(s) 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 and be updated as necessary to reflect any new developments in the law.

Our training may include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SAR-SFs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

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 or other publications. Currently our training program is: Using the FINRA web based tutorials however certain person may receive alternate training as in target publications We will maintain records to show the persons trained, the dates of training 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.

Rule: *FINRA Rule 3310.*
Resources: *See NTM 02-21*, *FinCEN SAR Narrative Guidance Package (11/2003)*, *FinCEN Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (10/10/2007)*.

16. Program to Independently Test AML Program

As a general matter, independent testing of USSI's AML compliance program includes: (1) evaluating the overall integrity and effectiveness of our AML compliance program; (2) evaluating our procedures for BSA reporting and recordkeeping requirements; (3) evaluating the implementation and maintenance of our CIP; (4) evaluating our customer due diligence requirements; (5) evaluating our transactions, with an emphasis on high-

risk areas; (6) evaluating the adequacy of our staff training program; (7) evaluating USSI's systems, whether automated or manual, for identifying suspicious activity; (8) evaluating our system for reporting suspicious activity; (9) evaluating our policy for reviewing accounts that generate multiple SAR-SF filings; and (10) evaluating our response to previously identified deficiencies.

a. Staffing

The testing of our AML program will be performed a annually generally, on a calendar year basis. We will evaluate the qualifications of the independent third party to ensure they have a working knowledge of applicable requirements under the BSA and its implementing regulations. Independent testing will be performed more frequently if circumstances warrant.

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310.
Resource: NTM 06-07.

b. Evaluation and Reporting

After we have completed the independent testing, staff will report its findings to senior management [*or to an internal audit committee*]. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310.

17. 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 Person. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Person's accounts will be reviewed by Shawn Orr designee and reported to H. Orr and G. Goldman

Rules: 31 C.F.R. §§ 103.19, 103.120; FINRA Rule 3310.

18. Confidential Reporting of AML Non-Compliance

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

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310.

19. Additional Risk Areas

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. The major additional areas of risk include any addition of non-institutional consumers. Additional procedures to address these major risks will require additional procedures and safeguards if USSI adds this consumer or customer account sector.

20. Senior Manager Approval

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by digital signature below.

Rules: 31 C.F.R. § 103.120; FINRA Rule 3310.

/s/ Herbert A. Orr
Chief Executive Officer

Date: February 1, 2010