Inland Securities Corporation
Anti-Money Laundering (AML) Program:
Compliance and Supervisory Procedures

---

1. Firm Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities 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 Suzanne L. Bond as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program. Suzanne L. Bond has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training, including the Financial Industry Regulatory Authorities' course on AML. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, and hold the position as Chief Compliance Officer. The AML Compliance Officer 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 Suzanne L. Bond 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, Suzanne L. Bond 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. 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, a compliance officer 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), a compliance officer will structure our search accordingly.

If a compliance officer searches our records and does not find a matching account or transaction, then they will not reply to the 314(a) Request. We will maintain documentation that we have performed the required search by maintaining a log showing the date of the request, the number of accounts searched, the name of the individual conducting the search and a notation of whether or not a match was found.

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. The ISC compliance department 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 broker-dealers. NSLs are highly confidential. No broker-dealer, officer, employee or agent of the broker-dealer can disclose to any person that a government authority or the FBI has sought or obtained access to records. Firms that receive 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

We understand 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 obtaining information from the required areas of business and not disclose the nature of the request. Only the compliance staff will be aware that the subpoena was received. 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 will 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. Our AML Compliance Person 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 in a locked file. Only authorized compliance staff will have access to these files.

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 will file joint SARs in the following circumstances; both entities are involved in the same suspicious transaction. We will also share 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.

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 Inland Real Estate Investment Corporation. Before we share SAR-SFs with Inland Real Estate Investment Corporation, we will have in place written confidentiality agreements or written arrangements that Inland Real Estate Investment Corporation 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, we 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. 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. We will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and we 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

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.

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).

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.

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, we 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 require a copy of the application and proof that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

Our firm does not generally do business with a foreign business or enterprise that does not have an identification number. Should we do business in the future 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. A compliance prinicipal 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.

We will verify customer identity through documentary means, non-documentary means or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever 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.

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 Lexis Nexis.

- Checking references with other financial institutions; or

- Obtaining a financial statement.

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: We will obtain information about beneficial ownership, individuals with authority or control over such account.

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. Prior to opening any new accounta a written explanation of the CIP will be provided to each accountholder. The language ised is as follows:

> **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) 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). (The letters provide staff guidance regarding the extent to which a broker-dealer may rely on an investment adviser to conduct the required elements of the CIP rule, prior to such adviser being subject to an AML rule.)

6. General Customer Due Diligence

We 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;

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 that is an entity other than a revocable trust, we will take steps to obtain sufficient customer information to comply with our suspicious activity reporting requirements. Such information should include:

- 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);
- explanations for any changes in account activity.

We will also ensure that the customer information remains accurate by obtain an updated new account form every twelve months or for each additional investment, whichever is longer.

7. Correspondent Accounts for Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Foreign Shell Banks

It is our firm's policy to not establish, maintain administer or manage correspondent accounts for unregulated foreign shell banks. To ensure that this does not occur our registered reps are instructed not to file new account paperwork for foreign shell banks. Our compliance department will not approve the opening of new accounts for foreign shell banks.

Rules: 31 C.F.R. §§103.175, 103.177.

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

We have reviewed our accounts and we do not have, nor do we intend to open or maintain, correspondent accounts for foreign financial institutions. To ensure that this does not occur our registered reps are instructed not to file new account paperwork for foreign financial institutions. Our compliance department will not approve the opening of new accounts for foreign financial institutions.

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).

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

We do not open or maintain private banking accounts. To ensure that this does not occur our registered reps are instructed not to file new account paperwork for private banking accounts. Our compliance department will not approve the opening of new accounts for private banking accounts.

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

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. Monitoring will be conducted through the following methods: we will review all the information at the time we open the account; we will review each new investment as it is made. Each account is reviewed annually.

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), Chicago branch of the U.S. Attorney's office 312-353-5300, the Chicago FBI office 312-431-1333 and local SEC office 31-353-7390 (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 the AML Compliance Officer. 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.

"Any instances of cyber-attacks including account hijacking, identity theft, and computer intrusion may be considered suspicious activity for AML purposes. As such, the firm will consider filing an SAR for any of these reasons. The "Other" SAR Reporting Category would be used if an SAR is ultimately filed."

12. Suspicious Transactions and BSA Reporting

a. Filing a SAR-SF

Our firm does not accept cash or cash equivalent to be deposited in an account. We 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.

"The Firm will use the BSA's E-Filing System to make SAR filings. All individuals responsible for filing a SAR are required to review the FinCEN guidance package for the filing of SARs. The package consists of three parts:

- "Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative";
- The Suspicious Activity Report (SAR); and
- Keys to Writing a Complete & Sufficient SAR Narrative".

A description of the guidance package is maintained with the training materials and is issued by the AMLCO to each person responsible for filing a SAR. Additionally, instructions regarding the use of the BSA E-Filing System for filing SARs are available on FinCEN's website."

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

Our firm prohibits transactions involving currency and has the following procedures to prevent such transactions: every employee has been instructed not to accept currency. If someone insisted upon delivering currency, a principal of the firm must be immediately notified so that she can speak with the individual to explain the policy and ensure that currency is not accepted. 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. All required CTRs will be filed by the 15th calendar day after the day of the transaction as directed on FinCEN's website.

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

c. Currency and Monetary Instrument Transportation Reports

Our firm 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. If the firm is required to complete a CMIR, it will be filed by the 15th clalndar day after the day of receipt, as directed on FinCEN's website.

Rules: 31 C.F.R. §§103.11, 103.23.

d. Foreign Bank and Financial Accounts Reports

Our firm does not hold any financial account regardless of the amount for which we have signature or other authority over, in a foreign country.

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

e. Monetary Instrument Purchases

We do not issue bank checks or drafts, cashier's checks, money orders or traveler's checks.

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

Our firm does not hold fund regardless of the amount for any individual.

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 Person 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 officer will handle all subpoenas or other requests 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

We shall retain either the original or other copy or reproduction of each of the following:

- 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

Our firm does not use a clearing firm. Our principal business is Real Estate Investment Trusts (REIT), Direct Participation Programs and TIC/1031 Exchange programs sponsored by affiliates of the Inland Real Estate Group of Companies, Inc. However, if we do use a clearing firm, we will establish procedures and work closely with our clearing firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with AML laws.

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 leadership of the AML Compliance Person 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 will 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. Currently our training program is: FINRA E-Learning course:

[FINRA Anti-Money Laundering (retail)]. 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, operations, 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

a. Staffing

The testing of our AML program will be performed at least annually (on a calendar year basis) by an independent AML/Regulatory consultant.
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. 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 the firm's president.

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 president of the firm.

Such reports will be confidential, and the employee will suffer no retaliation for making them.

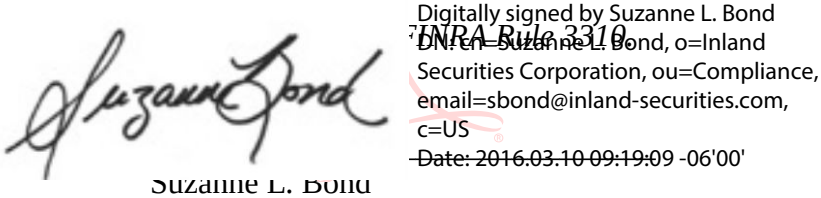
Rules: 31 C.F.R. § 103.120; FINRA Rule 3310.

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. It has not identified any other major areas of risk not included.

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 signatures below.



Suzanne L. Bond

Title: Senior Vice President, Chief Compliance Officer

Date: March 10, 2016