L.M. KOHN & COMPANY
Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

---

Last Updated January 29, 2019

Resources: The FINRA AML Web page , Financial Crimes Enforcement Network (FinCEN) and the Securities and Exchange Commission (SEC), including the SEC's AML Source Tool and Spotlight on AML Rulemaking. NASD Notices to Members (NTM) 02-21, 02-47, 02-50, 02-78, 02-80, 03-34 and 06-07, and BSA reporting requirements (BSA E-Filing System).

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 Carl R. Hollister as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program. Carl R. Hollister has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees, reviewing the adequacy of the AML training provided by our current vendor NRS Inc with an online training module. The AML officer is also the Chief Compliance Officer for the firm and along with the firm compliance manager, Drew Kohn, will endeavor to remain compliant with all applicable rules, laws and regulations. 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. Our AML Compliance Officer will work closely with our clearing firm RBC Correspondent Services to satisfy their AML compliance with our client base. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

Our firm has provided 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 Carl Hollister 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, Carl Hollister or Angela Boehm 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, Taylor Dennis or Carl Hollister 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), Taylor Dennis will structure our search accordingly.

If Taylor Dennis, or Trease Thomson searches our records and does not find a matching account or transaction, then Taylor Dennis, Trease Thomson or Carl Hollister will not reply to the 314(a) Request. We will maintain documentation that we have performed the required search by electronic spreadsheet. Upon receipt of a FINCEN request, Trease downloads the FINCEN files as Excel spreadsheets and save in the User (U:) drive under "Compliance FINCEN", A copy of each list is printed off as well as a resorted copy alias last name. The names are cross checked vs. the names in our DbCAMs database, we cross check for last name, first name, if a match is found then by middle name, address and social security number. Any matches found are reported to the AML Officer, our COO/CCO Carl Hollister. The printed worksheets are retained in a 3-ring binder on the document shelf in the reception area. Upon completion Taylor saves the Self Verification report electronically and in print, they are saved in same physical and computer locations as the FINCEN lists.

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. Carl Hollister 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). FinCEN also provides financial institutions with General Instructions and Frequently Asked Questions relating to 314(a) requests through the 314(a) Secured Information Sharing System or by contacting FinCEN at (800) 949-2732.

b. National Security Letters

Our AML Officer is responsible for appropriate handling of all national security letters received from our local FBI offices or other federal government authority conducting counterintelligence and counterterrorism investigations to obtain among other things, financial records. Our AML Officer will ensure that AML training covers NSLs and the dissemination of any NSLs received on a strict need to know basis. Any individual(s) found to have treated NSLs in a less than fully confidential nature will be terminated and a determination will be made if we would be required to file a SAR-SF. In addition, our AML Officer will ensure that any SAR-SFs field after receipt of a NSL contain no reference any 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 using three personnel in the firm to review, process, investigate and respond to the subpoena accordingly. The designated persons will be the Carl Hollister, Larry Kohn and Drew Kohn. No other firm personnel will be included in any activities involving the subpoena. 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. Carl Hollister 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.

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, according to our partnership with RBC Correspondent Services; any SARs reports made in connection with any customer from activity involving a brokerage account carried by RBC Correspondent Services on behalf of L.M. Kohn & Company will be filed jointly as RBC and LMK; or on any

activity where an Investment Company suspects the need for a SARs report, on activity we are made aware of we will then file a joint SARs report with the notifying Investment Company. 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.

We will share information about particular suspicious transactions with our clearing broker, RBC Correspondent Services, 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 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

We have no parent company.

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, Rhonda Hogan, Trease Thomson, Diane Eastman or Taylor Dennis (for direct application business) or Cara Kimmerly, Brad Dirheimer or Tom Berry (for RBC platform business) and Kristin Hobbs (for TD Ameritrade RIA platform) 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. Rhonda, Trease, Diane or Taylor will also review

existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated, and she 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 asset 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). For direct application business whether it is from a new or existing (three-year update) LMK Customer Acknowledgement form Trease, Rhonda, Diane or Taylor will go to the OFAC website and run an OFAC check. Once that is completed there is a section at the bottom of the LMK CA form to mark and initial that the OFAC check was completed, additionally this is annotated on the appl log. If a query were to come up positive, they would immediately notify the AML Officer. For RBC CS platform business each new account is checked by Brad Dirheimer, Tom Berry or Cara Kimmerly (Kristin Hobbs for TD Ameritrade RIA platform) against the OFAC website, the results are memorialized on the LMK system Compliance/RBC-TDA-Fund Direct/ Excel Spreadsheets. TD: Compliance / Advisory Files / Fee client list, RBC: compliance / RBC TDA Fund Direct / excel spreadsheets / required files and on the app the log. Any positive match would be reported immediately to our AML Officer.

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

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).

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.

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, for direct application business Trease Thompson, Rhonda Hogan, Diane Eastman and or Taylor Dennis will review, process and submit the LMK Acknowledgement form to the designated approving supervisor (Carl Hollister, Larry Kohn, Kristin Hobbs or Drew Kohn) prior to opening any new account for all required information If any of the required information is missing the order processing is put on hold until the required information is provided by the client and the RR; for RBC Correspondent Services based platforms Brad Dirheimer, Cara Kimmerly and Tom Berry (Kristin Hobbs for TD Ameritrade RIA platform) receives new account paperwork and it is date stamped, the paperwork is then processed for review of completeness of information, is then processed and submitted to the approving supervisor (Carl Hollister, Larry Kohn, Kristin Hobbs or Drew Kohn) prior to account opening to insure we have collected 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).

Welcome letters are sent to clients opening new accounts with a copy of the new account to make sure the information collected is re-verified by the client.

We do not open accounts without a valid TIN or social security number. In the event that we would receive an application or new account form without a TIN or social security number we would hold the paperwork, not enter any orders or process any orders until we had the required information.

In the event that a customer has applied for, but has not received, a taxpayer identification number, we will if by direct application have Trease Thomson, Rhonda Hogan, Diane Eastman or Taylor Dennis or if for RBC based platforms have Brad Dirheimer, Cara Kimmerly, or Tom Berry (Kristin Hobbs for TD Ameritrade RIA Platform) log the date application was made to the appropriate US agency by the customer, circumstances surrounding the filing with the US agency for a valid TIN, to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

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

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. Carl Hollister, Larry Kohn, or Drew Kohn 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 and or 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 (*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 military or dependent identification cards

- For a person other than 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 by utilizing RBC Correspondent Services credit checks that are performed prior to the opening of margin accounts by RBC Correspondent Services or other practical searches that may be available.

- Checking references with other financial institutions; or

- Obtaining a financial statement.

- Contacting the customer through email, telephone number, address provided or by visiting place of employment, or other practical means.

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 require the same information and verification for any person(s) with authority or control over any 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

There currently are no government-provided lists of suspected terrorists that firms are required to use as part of their CIP. 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 methods to provide notice to customers: oral or written notice, for walk-ins, or by email.

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, RBC Correspondent Services (including any of their parent or affiliate entities) 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

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 following criteria; new account / new relationship with an entity or household, incomplete primary new account form information without clear objectives. 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 any, many or all of 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 conducting a three year customer update for all direct and RBC Correspondent Services platform account, at times this will be cumulative and redundant with clients (households) having both direct application business and RBC based platforms.

7. Correspondent Accounts for Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Foreign Shell Banks

We will do business with foreign bank accounts on a very limited basis with a very narrow scope of business on a DVP basis for fixed income trading only. Our trading with any such foreign bank will be on a purely risk-less principal based transaction basis. We may be asked to get bids on foreign fixed income instruments from time to time from such foreign banks; we may have foreign banks who bid on USD or other denominated

fixed income securities. All of these trades will be executed on an RBC platform with the added set of eyes for irregularities coming from the RBC compliance systems in addition to our own reviews. At a minimum we require that any potential foreign bank wishing to do business with LMK submit a "Certification Regarding Correspondent Accounts for Foreign Banks" (OMB Control Number 1505-0184) be completed and signed and submitted to our AML Officer for review and approval. We will research the internet, or other information agencies if available to us, to develop a comfort level that the proposed foreign bank is an actual entity with a history of the limited investment activity we would be willing to engage in. If we find that the entity may be a foreign shell, we will not conduct business with that entity. If we find thru the course of business, public notices, reports fro SROs, Agencies of the USG we will immediately stop any activity with any such foreign bank we had previously transacted business with and instruct RBC Correspondent Services to place a BLOCK on the account to restrict any activity. 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 our 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. We will have on file the Foreign Account Section 312 form as well as the Certification Regarding Correspondent Accounts for Foreign Banks (OMB Control Number 1505-0184),

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. We will have on file the Foreign Account Section 312 form as well as the Certification Regarding Correspondent Accounts for Foreign Banks (OMB Control Number 1505-0184),

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

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).

We will conduct an 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, 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 will apply our risk-based due diligence procedures and controls to each financial foreign institution correspondent account on an ongoing basis. This includes periodically reviewing the activity of each foreign financial institution correspondent sufficient to ensure whether the nature and volume of account activity is generally consistent with the information regarding the purpose and expected account activity and to ensure that the firm can adequately identify suspicious transactions. Ordinarily, we will not conduct this periodic review by scrutinizing every transaction taking place within the account. One procedure we may use instead is to use any account profiles for our correspondent accounts (to the extent we maintain these) that we ordinarily use to anticipate how the account might be used and the expected volume of activity to help establish baselines for detecting unusual activity. Of the limited number of foreign accounts with which LMK conducts securities transactions the majority is riskless principal transactions in fixed income. The AML Officer is the supervisor in charge for reviewing the activity in the foreign accounts; trades are reviewed by either Pro Surv (electronic memorialization,

UMG Wires for electronic memorialization, statements for accounts for non-dollar denominated securities.

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

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

We do not open or maintain private banking accounts nor do we open or maintain accounts for senior foreign political figures.

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

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. For example, if the final rule deems a certain bank and its subsidiaries (Specified Bank) to be of primary money laundering concerns, a special measure may be a prohibition from opening or maintaining a correspondent account in the United States for, or on behalf of, the Specified Banks. In that case, we will take the following steps:

(1) We will review our account records, including correspondent account records, to ensure that our accountholders and correspondent accountholders maintain no accounts directly for, or on behalf of, the Specified Banks; and

(2) We will apply due diligence procedures to our correspondent accounts that are reasonably designed to guard against indirect use of those accounts by the Specified Banks. Such due diligence may include:

- Notification to Correspondent Accountholders

  We will notify our correspondent accountholders that the account may not be used to provide the Specified Banks with access to us; the notice will include language stating the accounts may frozen / blocked, we may cease doing businesses with the entity and inform RBC Correspondent Services of same recommending they cease business with entity as well,

  We will transmit the notice to our correspondent accounts using the following method; email, telegram, or certified mail and or, and we shall retain documentation of such notice.

- Identification of Indirect Use

  We will take reasonable steps in order to identify any indirect use of our correspondent accounts by the Specified Banks. We will determine if such indirect use is occurring from transactional records that we maintain in the normal course of business. We will take a risk-based approach when deciding what, if any, additional

due diligence measures we should adopt to guard against the indirect use of correspondent accounts by the Specified Banks, based on risk factors such as the type of services offered by, and geographic locations of, their correspondents.

We understand that we have an ongoing obligation to take reasonable steps to identify all correspondent account services our correspondent accountholders may directly or indirectly provide to the Specified Banks.

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. All trades are reviewed on a T+1 basis thru the Pro Surv, Protegent System for our RBC platform accounts, each new trade for investment company business is reviewed and approved by a supervisor in the home office prior to execution. All transactions on the TD Ameritrade RIA platform are reviewed daily. Wire requests that are frequent out of any single account generate an AML inquiry form RBC CS. For outgoing wires to persons or entities other than the same registration as the sender require a supervisor review and approval prior to executing the wire. Monitoring will be conducted through the following methods: Trade reviews, new account opening reviews and approvals, wire request reviews and approvals, exception reports generated by our clearing form for missing documents, missing CIP information The AML Compliance Person, the firm compliance manager , the firm CEO are responsible for this monitoring, will review any activity that our monitoring system detects, 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.

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 OFACs 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) (specially to report transactions relating to terrorist activity), local U.S. Attorney's office (513-684-3711), local FBI office (513-421-4310*)* and local SEC office (Chicago office 312-353-7390). 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, which 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 Carl Hollister via email or in person (small office all

support and back office staff of the firm is located in same location with AML 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.

12. Suspicious Transactions and BSA Reporting

Rule: 31 C.F.R. §103.19.

a. Filing a SAR-SF

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 the 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

Our firm prohibits transactions involving currency and has the following procedures to prevent such transactions: We do not accept cash or credit card payment for deposits or purchases, period. 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

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.

Rules: 31 C.F.R. §§103.11, 103.23.

d. Foreign Bank and Financial Accounts Reports

We 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

We do not issue bank checks or drafts, cashier's checks, money orders or traveler's checks in the amount of $3,000 or more.

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

We do not transmit funds, our clearing firm does on our behalf, all transmittal requests are reviewed by appropriate firm personnel based on procedures outlined above. We retain a wire request log, as well as copies of the wire requests. Our log contains 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 transmittor's 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 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, and 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. 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, hard copy or pdf version of said copy or other copy or reproduction of each of the following when applicable:

- 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 following exception reports and tools for supervisory reviews offered by our clearing firm in order to monitor customer activity: Daily money line reports thru Betalink or exception report, trade reviews thru Pro Surv, Protegent System, or thru the Daily Audit Report of Trades, Missing CIP information reports, our internal change of address verification or the Name & Address change verification report, and the exception reports requiring attention. 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 Recertification's 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 is ongoing, and our firm element training will include that all licensed and identified associated personnel must complete the on line AML training module at least annually. 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 made available on-line as part of our overall compliance toll package thru NRS Inc. our compliance tool kit vendor. And through Financial Tracking our workflow application system which offers Kaplan based CE as well. There is annual AML module that all licensed and identified associated personnel must complete. We will maintain records to show the persons trained as well as 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

a. Staffing

The testing of our AML program will be performed at least annually (on a calendar year basis), by an independent entity. Currently for continuity purposes we utilize the AML testing services of Kessler Business Services, Bob Kessler, who is not an employee of LMK nor is he a contractor with LMK for AML supervision, AML development or other AML activities. Personnel of our firm, including our AML Compliance Person, our compliance manager, or our CEO will work with Kessler Business Services for the annual audit. We are dependent on an outside AML audit due to our small size and scope of business; many personnel wear many hats in the firm. 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, the AML Officer will report the findings of the auditor to senior management or our three directors. 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 Larry M. Kohn the firm CEO and in his absence should he be out of the country by Drew Kohn the firm Compliance Manager.

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 Officer, unless the violations implicate the AML

Compliance Person, in which case the employee shall report to Larry M. Kohn the CEO 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. We are comfortable that our current practices under current rules, regulations and laws reduce the risk significantly that we would be any party to any potential violation of any part of eh Patriot Act.

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.

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

Signed:

Title:

Date: