Anti-Money Laundering (AML) Program

Firm Policy

It is the policy of Compass Securities Corporation to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities.

Notice to Customers

Compass Securities Corporation will provide notice to customers that it is requesting information from them to verify their identities, as required by Federal law under the USA PATRIOT Act Section 314. The firm will use the following method to provide notice to customers:

- Web site posting at www.compassfinancialservicesgroup.com
- A Disclosure notice to be used as part of the New Account opening process
- A notice in our “welcome letter” which is sent to all new accounts.

Compass Capital will identify customers and verify their identity by requesting that the customer provide us with an unexpired picture ID suitable for copying for our files and will delegate further identification procedures to our clearing firms who will check the names against the appropriate databases.

In addition to the information we must collect under FINRA Rules, we will, at a minimum:

- Verify, to the extent reasonable and practicable, the identity of any customer seeking to open an account.
- Maintain records of information used to verify a customer's identity.
- Check that a customer does not appear on government terrorist lists, such as the list on Treasury's Office of Foreign Assets Control (OFAC) Web Site. The kinds of information that we will collect before opening different types of accounts are listed below.
- We will make any necessary modifications to these procedures when the final Treasury/SEC regulations on verification of customer identification are issued.

Risk-Based Information On Various Account Types

Compass Securities will collect the following information for all accounts, if applicable, for any person, entity or organization who is opening a new account (or is being granted trading authority over a new or existing account) and whose name is on the account or has authority over the account:

- The name and mailing and residential (or principal place of business) street address of the customer;
- The customer's date of birth;
- For U.S. persons, the customer's Social Security number or taxpayer identification number (including U.S. tax forms), or, for non-U.S. persons without a taxpayer identification number, an 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 biometric safeguard.

Recognizing that different types of accounts pose different risks and trigger different requirements under the rules, we will gather the additional information specified below for each of the following categories of accounts we provide:

(1) Individual Accounts –We will make reasonable efforts to obtain the customer's net worth, annual income, occupation and employment data, such as the employer's address, and the customer's investment experience and objectives.

(2) Non-U.S. Person Accounts – We may inquire more fully depending on a number of factors, such as the country of origin of the account holder or persons authorized to trade. *Note that under the Bank Secrecy Act (BSA), firms must record a current passport number or other valid government identification number for non-U.S. person account transfers or transmittals of $3,000 or more.*

(3) Domestic Operating or Commercial Entities – We will collect information sufficient to determine the corporate or business entity's identity, and the authority of its business representative to act on its behalf.

(4) Domestic Trusts – We will identify the trustee, the activity the trust authorizes, and the authority of the trust's representative to act on its behalf.

(5) Foreign and Offshore Entities – We will identify the account holder and other persons or entities authorized to trade for the account and we will consider the entity's country of incorporation, location and other factors to determine what additional identifying information is necessary and available. (See Sections 5 and 6 below for special procedures governing correspondent accounts for foreign shell banks and other foreign financial institutions and foreign private banking accounts.)

(6) Institutional Accounts, Hedge Funds, Investment Funds and Other Intermediary Relationships – While our AML procedures cover institutional clients, we recognize that certain types of institutional accounts are different from retail accounts. Institutional accounts often are opened for financially sophisticated customers who trade frequently, in volume, and usually through an intermediary, some of whose AML policies and procedures are sufficient and verifiable. When dealing with an institutional client, we will consider whether it has an AML program and the quality of that program, the length and nature of our experience with the institution, and the history of the institution. In addition, in determining whether it is necessary to identify the investors of non-U.S. institutions, we will consider the regulation of the institution by its home country and whether the institution is located in a bank secrecy haven or a non-cooperative country. (See Sections 5 and 6 below for special procedures governing correspondent accounts for foreign shell banks and other foreign financial institutions and foreign private banking accounts.)

(7) High Risk and Non-Cooperative Jurisdictions – It is highly unlikely that Compass will open accounts for persons or entities from these types of areas. However if such an account were to present itself, we will especially scrutinize accounts that are located in problematic countries. We will check the lists and accompanying narrative information of the Financial Action Task Force (FATF) [http://www.fatf-gafi.org], FinCEN [http://www.fincen.gov], and the "Major Money Laundering Countries" section of the "Money Laundering and Financial Crimes" part of the U.S. Department of State's annual International Narcotics Control Strategy Report [http://www.state.gov/j/inl/rls/nrcrpt/2016/vol2/253367.htm] to determine problematic countries and will factor this information into our decisions on whether to open or maintain accounts that are based in these jurisdictions.

(8) Senior Foreign Government/Public Officials – It is highly unlikely that Compass will open accounts for persons or entities from these types of individuals. Firms must conduct enhanced scrutiny of accounts requested or maintained by or on behalf of senior foreign political figures (including their family members and close associates). We will conduct enhanced due diligence of accounts of "senior foreign political figures," as well as their families and business associates, to detect and report transactions that involve the proceeds of foreign corruption.

(9) Transferred Accounts – Although we are not required to verify the identity of a customer whose account is transferred to our firm if the customer does not initiate the transfer, we will still consider the scenarios above in deciding if the risks of a particular transferred account require our obtaining and verifying information from the transferred customer. In general Compass will treat a transferred account as a new account and process it accordingly.

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 Officer will be notified so that we can determine whether we should report the situation to FinCEN.

Verifying Information

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

We will verify customer identity through documentary evidence, non-documentary evidence, or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever possible. We may also use such non-documentary means, after using documentary evidence, if we are still uncertain about whether we know the true identity of the customer.

Appropriate documents for verifying the identity of natural persons include the following:

- An unexpired driver's license, passport, or other government identification showing nationality, residence, and photograph or other biometric safeguard, or, for non-U.S. persons, an unexpired alien registration card or other government issued identification showing nationality, residence and photograph or other biometric safeguard.

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

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

Verification of customer identity through the use of non-documentary evidence is mandatory in the following situations: (1) when the customer is unable to present an unexpired identification card with a photograph or other biometric safeguard; (2) when the documents the customer presents for identification verification are unfamiliar to the firm; (3) when the customer and firm do not have face-to-face contact; and (4) when 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. Under these circumstances, we will use the following non-documentary methods of verifying identity:

- Contact the customer after the account has been opened (although we cannot rely solely on customer contact as a means for verification);
- Obtain financial statements from the customer;
- Compare information obtained from the customer against databases, such as Equifax, Experion, Lexis/Nexis, or other in-house or custom databases;
- Compare information obtained from customer with information available from a trusted third-party source (such as a credit report);
- Check references with other financial institutions; and
- Any other non-documentary means deemed appropriate.

We will verify the information at the time new accounts are opened, if possible, but in most situations no later than five business days after opening. However, we recognize that there may be situations where even a five-day delay will be too long. 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 restrict the types of transactions or dollar amount of transactions pending verification. We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. We will maintain those records for five years after the account has been closed or the customer's trading authority over the account has ended.

As required under the BSA, we will record a current passport number or other valid government identification number for transfers or transmittals of $3,000 or more by or for non-resident alien accounts.

Using Government Provided Lists of Terrorists and Other Criminals.

Before opening an account, and on an ongoing basis, we will delegate to our clearing firm, the process of checking to ensure that a customer does not appear on a list provided to us by the government, like Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) (See the OFAC Web Site at *www.treas.gov/ofac*, which is also available through an automated search tool on http://www.finra.org/ofac), and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. Because the OFAC Web Site is updated frequently, we will consult the list on a regular basis and subscribe to be sent updates when they occur. We will also review existing accounts against these lists when they are updated and we will document our review.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions

with a person or entity located in an embargoed country or region, we or our clearing firm will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. We will also call the OFAC Hotline at 1-800-540-6322.

Thank you for your patience understanding and support as we conduct our business in a compliant manner and do our part to deny terrorist groups and criminals access to America’s financial system.