



AML Policy

OTM CAPITAL ANTI-MONEY LAUNDERING ("AML") POLICY STATEMENT AND PRINCIPLES

SCOPE OF POLICY

This policy applies to all OTM CAPITAL officers, employees, appointed producers and products and services offered by OTM CAPITAL. All business units and locations within OTM CAPITAL will cooperate to create a cohesive effort in the fight against money laundering.

POLICY

It is the policy of OTM CAPITAL to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. OTM CAPITAL is committed to AML compliance in accordance with applicable law and requires its officers, employees and appointed producers to adhere to these standards in preventing the use of its products and services for money laundering purposes. For the purposes of the Policy, money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

CUSTOMER IDENTIFICATION PROGRAM

OTM CAPITAL has adopted a Customer Identification Program (CIP). OTM CAPITAL will provide notice that they will seek identification information; collect certain minimum customer identification information from each customer, record such information and the verification methods and results; and compare customer identification information.

NOTICE TO CUSTOMERS

OTM CAPITAL will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law.

VERIFYING INFORMATION

Based on the risk, and to the extent reasonable and practicable, OTM CAPITAL will ensure that it has a reasonable belief of the true identity of its customers. In verifying customer identity, appointed producers shall review photo identification. OTM CAPITAL shall not attempt to determine whether the document that the customer has provided for identification has been validly issued. For verification purposes, OTM CAPITAL shall rely on a government-issued identification to establish a customer's identity. OTM CAPITAL, however, will analyze the information provided to determine if there are any logical inconsistencies in the information obtained. OTM CAPITAL will document its verification, including all identifying information provided by the customer, the methods used and results of the verification, including but not limited to sign-off by the appointed producer of matching photo identification.

CUSTOMERS WHO REFUSE TO PROVIDE INFORMATION

If a customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the appointed agent shall notify their New Business team. The OTM CAPITAL New Business team will decline the application and notify the AML Compliance Committee.

MONITORING AND REPORTING

Transaction based monitoring will occur within the appropriate business units of OTM CAPITAL. Monitoring of specific transactions will include but is not limited to transactions aggregating \$5,000 or more and those with respect to which OTM CAPITAL has a reason to suspect suspicious activity. All reports will be documented and retained in accordance with the FIAMLA requirements.

SUSPICIOUS ACTIVITY

There are signs of suspicious activity that suggest money laundering. These are commonly referred to as "red flags." If a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AML Compliance Committee. Examples of red flags are:

The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.

The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.

The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry. The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.

The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the \$10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.

For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force.

The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

The customer's account shows numerous currency or cashier's check transactions aggregating to significant sums. The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.

The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.

The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.

The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose. The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.

The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)

The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.

Attempt to borrow maximum cash value of a single premium policy soon after purchase. If the appointed producer: Exhibits a dramatic or unexpected increase in sales (particularly of single premium contracts)

Has consistently high activity in single premium contracts in excess of company averages Exhibits a sudden change in lifestyle

INVESTIGATION

The AML Compliance Committee is responsible for any notice or filing with law enforcement or regulatory agency. Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know

RECORDKEEPING

The AML Compliance Committee will be responsible to ensure that AML records are maintained properly and that SARs and Blocked Property Reports are filed as required. OTM CAPITAL will maintain AML records for at least five years.

TRAINING

OTM CAPITAL shall provide general AML training to its officers, employees and appointed producers to ensure awareness. The training will include, at a minimum: how to identify red flags and signs of money laundering; what roles the officers, employees and appointed producers have in the OTM CAPITAL compliance efforts and how to perform such duties and responsibilities; what to do once a red flag or suspicious activity is detected; OTM CAPITAL record retention policy; and the disciplinary consequences for non-compliance with the Act and this Policy. In addition, each affected area will provide enhanced training in accordance with the procedures developed in each area for officers and employees reasonably expected to handle money, requests, or processing that may bring them into contact with information designated above. Training will be conducted on an annual basis. The OTM CAPITAL AML Compliance Committee will determine the ongoing training requirements and ensure written procedures are updated to reflect any changes required in such training. OTM CAPITAL will maintain records to document that training has occurred.

TESTING OF THE POLICY

The testing of the Policy will be conducted by an outside independent third party annually. Any findings will be reported to the AML Compliance Committee, SFG Audit Committee and Senior Management for appropriate action.

ADMINISTRATION

The AML Compliance Committee is responsible for the administration, revision, interpretation, and application of this Policy. The Policy will be reviewed annually and revised as needed.