反洗錢政策 (AML)

政策聲明和原則
在遵守金融情報和反洗錢法2002（FIAMLA2002），2002年防止腐敗法（POCA2002）和2002年防止恐怖主義法（POTA2002），本公司已通過了反洗錢的政策所規定的董事會會議紀錄。

政策範圍
本政策適用於所有本公司職員，僱員，任命製造者和本公司提供的產品和服務。所有本公司的業務單位和場所內將合作努力在打擊清洗黑錢活動。各業務單位和地點已經實施合理預期風險為本的程序預防，檢測和交易報告皆須根據反洗錢法。產生的一切結果將遵照反洗錢法被記錄和保留。反洗錢委員會負責發起可疑活動報告（"SARs）或其他需要報告給相關執法或監管機構。

政策
這是本公司於禁止並積極開展預防洗錢和任何活動的政策及有利於洗錢或資助恐怖或犯罪活動。本公司致力於遵守反洗錢適用的法律，並要求其職員，僱員及委任生產者遵守這些標準，防止使用其產品和服務進行洗錢的目的。洗錢通常被定義為從事設計行為隱瞞或掩飾真實的犯罪所得收益的來源，使違法所得似乎已被來自合法來源，構成合法資產。一般來說，洗錢發生在三個階段。現金首次進入金融系統在"放置"的階段，那裡的犯罪活動產生的現金轉換成貨幣工具，如匯票或旅行支票，或存入帳戶的金融機構。在"分層"的階段，資金轉移或移動到其他帳戶或其他金融機構進一步分離其犯罪來源的金錢。在"整合"階段，資金重新進入金融市場用於購買基金的合法資產或其他犯罪活動或合法的業務。恐怖分子籌資活動的收益可能不涉及犯罪行為，而是企圖隱瞞來源或用途的資金，而稍後將用於犯罪目的。

反洗錢委員會
反洗錢委員會，全權負責與我國的政策應包括總法律顧問，首席合規官，本公司，副監察主任，本公司,助理副總裁，內部審計和公司律師。首席合規官還應當持有行政反洗錢官的稱號，並須有權簽署。反洗錢委員會的反洗錢方面的政策應包括但不限於設計和實施，以及更新的政策要求職責;傳播信息的人員，本公司僱員和任命的培訓職員，僱員及委任生產者，監測合格的本公司經營單位和指定生產商，都需保持必要的和適當的記錄，需要時提交股票增值;及獨立測試的運作的政策。每個本公司業務單位應指定一名聯絡人，以直接面對反壟斷法規條委員會，以協助委員會進行調查，監測和其他要求。

客戶識別計劃
本公司通過了客戶識別項目（CIP）。本公司將尋求識別信息，收集一些最起碼每一位客戶的身份資料的，記錄這些信息和核查方法和結果，並比較客戶身份信息與外國資產管理處。

客戶須知
本公司向客戶提供通知要求提供資料，這是由所適用的法律來驗證他們的身份。

驗證信息
根據風險，並合理和可行的範圍內，本公司將確保有一個合理理由去相信其客戶的真實身份。在核實客戶身份，委任生產者應當審查附照片的身份證明。本公司不得試圖確定該文件是否是客戶已有效發出提供用於識別。為了核實目的，本公司應當依靠政府頒發的身份證，建立客戶的身份。但是本公司會將所提供的資料進行分析，以確定是否有任何邏輯不一致所獲得的信息。本公司將文件進行核查，包括所有由客戶提供的身份信息，使用的方法和結果的核查，包括但不限於簽署過的，由指定的生產商配對照片的身份證明。

客戶拒絕提供信息
如果客戶拒絕提供上述信息時的要求，或似乎有故意提供誤導性資料，委任代理人應當通知其業務團隊。業務團隊將拒絕申請，並通知反洗錢委員會。

外國資產控制檢驗辦公室（"外國資產管理處"）列表
所有新收到的申請，並持續進行，付款，新的生產者任命或新員工，本公司將檢查，以確保個人或實體沒有出現在財政部外國資產管理處"特別指定國民和阻止者"名單（供需列表），並且不是從禁運的國家和地區上市的外國資產管理處網站中從事交易的人或實體。本公司將以世界合同檢查，以確保速度和準確性檢查。本公司亦會檢討現有保單持有人，對這些生產商和員工定期列出。審查的頻率將被記錄和保留。在事件的供需匹配列表或其他外國資產管理處名單，業務部門將確定進行審查的情況。如果企業單位是無法確認審查情況真實性，反洗錢委員會應得到通知。

監測和報告
交易的監測將出現在本公司適當的業務單位。監測具體的交易將包括但不限於交易總額為5000美元或更多，本公司有理由懷疑有哪些可疑的活動。所有報告都將根據反洗錢法要求被記錄並保留。

當有跡象出現可疑的洗錢活動。這些通常被稱為紅色的標誌。如果檢測到一個紅色的標誌，將執行程序與交易之前，進行額外的調查。如果可疑的活動沒有一個確定的合理解釋，應當通報反洗錢委員會。紅色的標誌的例子有：

-客戶提供合法來源的資金訊息是虛假，誤導或絕大部分是不正確的。
-客戶拒絕或未能確定，表示任何他或她的資金和其他資產的合法來源。
-客戶（客戶相關人士）有一個可疑的背景或為新聞報導顯示可能的刑事，民事，或監管的行為。
-客戶表現出缺乏關注風險，佣金或其它交易成本。
-客戶作為未公開的主體之代理人，沒有正當的商業理由，拒絕或不願意提供信息或以其他方式迴避有關該人士或實體。
-客戶試圖經常或大額存款貨幣，堅持只處理現金等值物，或要求豁免從公司的政策有關的存款，現金及現金等值項目。
-客戶沒有明顯的原因而有單一名稱多個帳戶或多個名稱，用大量的同名賬戶或第三方轉讓。
-客戶來自或是持有賬戶來自金融行動特別工作組認定為不合作的國家或地區。
-客戶的帳戶顯示了眾多的貨幣或出納員支票交易到大量的資金。
-客戶的帳戶有大量電匯給不符合客戶的合法商業目的之無關的第三方。
-客戶的帳戶電匯已經沒有明顯的經營宗旨，或確定為一個國家洗錢風險或銀行保密的庇護所。
-客戶的帳戶設置大型或頻繁電匯，立即撤回支票或借記卡，沒有任何明顯的經營宗旨。
-客戶資金存款隨後立即要求將錢電匯出去給第三者，或另一家公司，沒有任何明顯的經營宗旨。
-客戶資金存款為購買長期投資為目的請求後，由清算中的地位和轉讓的收益超過了該帳戶。
-客戶請求避免該公司的正常文件要求的處理的方式交易。

調查
經通知反洗錢委員會對外國資產管理處供需名單或可能可疑的活動展開調查。調查將包括但不一定限於審查所有可用的訊息，如付款記錄，出生日期和地址。如果反洗錢委員會或行政區適當的執法或監管機構調查的結果建議提交一份凍結資產聲明。則反洗錢委員會負責任何通知或備案至執法部門或監管機構。調查結果將不會與任何人或是合法需要知道的人透露或討論。在任何情況下，任何管理人員，僱員或委任代理人披露或討論任何反洗錢的關注，調查，通知或特區提交與該人或人員問題等，或任何其他人，包括成員有關人員，僱員或指定代理人的家人。

記錄保管
反洗錢委員會將負責反洗錢的記錄，以確保維持正確的實施，特別行政區和阻止財產報告的規定提交。本公司會將反洗錢記錄維持至少五年。

訓練
本公司將遵照反洗錢法提供一般反洗錢培訓，其職員，僱員及委任生產者意識的要求。培訓將包括在最低限度：

如何識別標誌的紅色的標誌和洗錢;本公司高級職員，僱員及委任生產者介紹，以及如何履行這些職責和責任;什麼做一次紅色的標誌或發現可疑活動;本公司於記錄保留不遵守法案政策和紀律的後果。此外，每個受影響的地區將提供增強培訓，按照程序開發的各個領域的人員和僱員合理預期的處理錢，請求，或加工，可能使他們接觸到上述指定的信息。培訓將每年進行。本公司的反洗錢委員會將決定正在進行的培訓要求，並確保書面程序更新，以反映任何變化需要這種訓練。本公司將以文件保存培訓記錄。

每年將會由一個外部的第三方測試政策。任何調查結果將上報反洗錢委員會，審計委員會和高級管理人員採取適當行動。

反洗錢委員會負責管理，修訂，解釋和應用本政策。該政策將每年檢討並做必須的修改。

ANTI-MONEY LAUNDERING POLICY (AML)

POLICY STATEMENT AND PRINCIPLES
In compliance with the Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA 2002), the Prevention of Corruption Act 2002 (POCA 2002) and the Prevention of Terrorism Act 2002 (POTA 2002), we have adopted an Anti-Money Laundering (AML) compliance policy ("Policy") as set forth in the Board minutes.

SCOPE OF POLICY
This policy applies to all we officer, employees, appointed producers and products and services offered by us. All business units and locations within us will cooperate to create a cohesive effort in the fight against money laundering. Each business unit and location have implemented risk-based procedures reasonably expected to prevent, detect and cause the reporting of transactions required under the FIAMLA. All efforts exerted will be documented and retained in accordance with the FIAMLA. The AML Compliance Committee is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Committee.

POLICY
It is the policy of us 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. We are 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.

AML COMPLIANCE COMMITTEE
The AML Compliance Committee, with full responsibility for the Policy shall be comprised of the General Counsel; Chief Compliance Officer, we; Deputy Compliance Officer, we; Assistant Vice President-Internal Audit, and Corporate Attorney. The Chief Compliance Officer shall also hold the title Chief AML Officer, and shall have authority to sign as such. The duties of the AML Compliance Committee with respect to the Policy shall include, but are not limited to, the design and implementation of as well as updating the Policy as required; dissemination of information to officers, employees and appointed producers of us, training of officers, employees and appointed producers; monitoring the compliance of us operating units and appointed producers, maintaining necessary and appropriate records, filing of SARs when warranted; and independent testing of the operation of the Policy. Each our business unit shall appoint a contact person to interact directly with the AML Compliance Committee to assist the Committee with investigations, monitoring and as otherwise requested.

CUSTOMER IDENTIFICATION PROGRAM
We have adopted a Customer Identification Program (CIP). We 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 with OFAC.

NOTICE TO CUSTOMERS
We 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, we 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. We shall not attempt to determine whether the document that the customer has provided for identification has been validly issued. For verification purposes, we shall rely on a government-issued identification to establish a customer's identity. We, however, will analyze the information provided to determine if there are any logical inconsistencies in the information obtained. We 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. Our New Business team will decline the application and notify the AML Compliance Committee.

CHECKING THE OFFICE OF FOREIGN ASSETS CONTROL ("OFAC") LIST
For all (1) new applications received and on an ongoing basis, (2) disbursements (3) new producers appointed or (4) new employees, we will check to ensure that a person or entity does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. We shall contract with World-Check to ensure speed and accuracy in the checks. We will also review existing policyholders, producers and employees against these lists on a periodic basis. The frequency of the reviews will be documented and retained. In the event of a match to the SDN List or other OFAC List, the business unit will conduct a review of the circumstances where such match has been identified. If the business unit is unable to confirm that the match is a false positive, the AML Committee shall be notified.

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

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 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 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.