# AML (Anti-Money Laundering) Policy

This policy applies to the director of DAM FOREX, all officers and employees, and the products and services offered by DAM FOREX. All business units and locations within DAM FOREX will work together to create a cohesive effort in the fight against money laundering. Each business unit and location will implement risk-based procedures that can reasonably be expected to prevent, detect and report transactions. All efforts are documented and maintained.

The AML Compliance Committee is responsible for initiating suspicious activity reports or other required reports to appropriate law enforcement or regulatory authorities. All communications from law enforcement or regulatory authorities relating to this Policy shall be directed to the AML Compliance Committee.

The Committee shall:
Receive internal reports of (suspected) money laundering.
Investigate reports of suspicious activity.
Report any related suspicious activity to the appropriate authorities.
Ensure that arrangements for employee and adviser awareness and training are appropriate.
Report at least annually to the firm's governing body on the operation and effectiveness of the firm's systems and controls.
Monitor the day-to-day operation of the anti-money laundering policy in relation to the development of new products, the acquisition of new clients and changes in the firm's business profile.

POLICY

It is the policy of DAM FOREX to prevent money laundering and to prohibit any activity that facilitates money laundering or the financing of terrorism or criminal activity.

DAM FOREX is committed to AML compliance in accordance with applicable laws and requires its directors, officers and employees to adhere to these standards in order to

prevent the use of our products and services for money laundering purposes.

For purposes of this policy, money laundering is generally defined as engaging in conduct designed to conceal or disguise the true source of the proceeds of criminal activity and to make it appear that the illicit proceeds come from legitimate sources or are legitimate assets.

What is Money Laundering?

Money laundering is the process of converting money or other assets derived from a crime (criminal property) into "clean" money or other assets that have no apparent connection to the source of the crime.

Criminal property can take any form, including money, monetary value, securities, tangible property, and intangible property. It also includes funds used to finance terrorism.

Money laundering activities include Acquisition, use, or possession of criminal property.

Handling the proceeds of crimes such as theft, fraud, and tax evasion.

Knowingly engaging in any form of criminal or terrorist activity.

Making arrangements to facilitate the laundering of criminal or terrorist property.

Investing the proceeds of crime in other financial instruments.

Investing the proceeds of crime by acquiring property/assets.

Transferring proceeds of crime property.

The money laundering process consists of three steps

1. Disposal.

Disposal of the initial proceeds of the illegal activity, such as into a bank account.

2. Transfer.
The movement of funds in a series of financial transactions for the purpose of disguising thesource of the money and making it appear legitimate.

3. Use
Criminals are free to use the funds after they have been removed from the system as seemingly "clean" funds.

No financial sector is immune from the activities of criminals, and businesses need to consider the money laundering risks posed by the products and services they offer.

What is Anti-Terrorism Financing?

Terrorist financing is the process by which legitimate companies or individuals, for ideological, political, or other reasons, may choose to provide resources to terrorist activities or organizations.

Therefore, companies must ensure that The customer is not itself a terrorist organization.
The customer is not providing the means to finance a terrorist organization.
Terrorist financing may not be the proceeds of criminal activity, but rather an attempt to conceal the source or intended use of funds that are later used for criminal purposes.

Risk-Based Approach
The level of due diligence required when considering anti-money laundering procedures within a firm should take a risk-based approach. That is, the amount of resources devoted to conducting due diligence on a risky relationship should be proportional to the level of risk posed by that relationship.

These can be divided into the following areas:

Customer Risk
Different customer profiles present different levels of risk. A basic Know Your Customer (KYC) check can be performed to identify the risks posed by that customer.

For example, an individual nearing retirement who makes regular, small contributions to a savings account that matches his or her financial profile is less risky than a middle-aged individual who makes occasional payments of ever-changing amounts to a savings account that does not match the customer's financial data profile. The intensity of due diligence on the latter would be higher than on the former because the potential threat of money laundering is perceived to be greater in the latter case.

The corporate structure can be used as an example of a customer that may have a higher risk profile than the one we just saw because criminals can use it to add layers to
transactions to hide the source of funds, and as such, customers can be placed into different risk bands.

Product Risk
This is the risk posed by the product or service itself. Product risk is caused by its functionality as a money laundering instrument.
The Money Laundering Joint Operating Group classifies the products that a firm typically handles into three risk bands (reduced, intermediate and elevated). In general, pure
protection contracts are classified as low risk, while investments in mutual funds are classified as high risk. An additional factor that contributes to the risk classification is the sales process associated with the instrument: if the instrument is traded on an advisory basis
as a result of KYC, the risk is lower than in an execution-only transaction where less is
known about the client.

Country Risk
The geographical location of a client and the origin of its business activities present risks arising from the fact that countries around the world have different levels of risk.

The firm will use the four risk areas listed above to determine the level of due diligence required initially and on an ongoing basis.
Customer Identification Program DAM FOREX has adopted a customer identification program under which DAM FOREX notifies each customer that identification information will be requested, collects certain minimum customer identification information from each customer, and records such information, verification methods and results.

Notice to Customers
DAM FOREX notifies you that we are requesting information from you to verify your identity as required by applicable law.

Knowing the Customer
When a business relationship is established, the firm must determine the nature of the business the customer expects to conduct in order to determine what may later constitute normal activity in that relationship.

Once an ongoing relationship is established, the normal business conducted for that customer can be evaluated in light of the customer's expected pattern of activity. Any
unexplained activity can be investigated to determine whether money laundering or terrorist financing is suspected.

Information about the client's income, occupation, sources of wealth, trading habits, and the economic purpose of the transaction is typically collected as part of the advisory process.
Personal information such as nationality, date of birth and address is also obtained at the outset of the transaction. This information should also be considered in the context of financial crime risk. For high-risk

transactions, it would be appropriate to require verification of the information provided by the customer.
Source of Funds.

Whenever a transaction is made, the source of funds, i.e., from where, by whom and how payment is made, must be identified and recorded in the customer file (this is usually
accomplished by retaining a copy of the check or debit authorization).

Identification
The standard identification requirements for customers who are private individuals generally depend on the circumstances relating to the customer and the type of product being dealt
with, i.e. the level of risk associated with the product, whether it is a low-risk, medium-risk or high-risk product. Therefore, for reduced and intermediate risk products, the following information is required by default for identification purposes

Full Name.

Residential address.

Verification
Verification of information received must be based on a reliable, independent source (customer-generated documents, company-generated electronic documents, or a
combination of both). When conducting business in person, firms should see the originals of all documents involved in the verification.

If documentary evidence of a person's identity provides a high level of confidence, it is likely that authorities have confirmed the existence and characteristics of the person concerned, usually issued by a government department or agency or by a court of law.

If documentary evidence such as an identity card is not available from the person, other evidence of identity may allow the firm to reasonably

rely on the customer's identity, but the firm must weigh this against the risks involved.

If identity is to be confirmed by documents, it should be based on one of the following government-issued documents.

One of the following government-issued documents, including:

Customer's full name and residential address A government-issued photo ID

Valid passport

International identification card

It can also be done by means of a government-issued document without a photograph that shows the customer's full name and a second document that shows the customer's full name

and residential address:
Customer's full name and residential address.
DAM FOREX does not set a time limit for a customer to submit verification documents, but the submission of verification documents is considered a mandatory requirement for the customer to withdraw funds.

DAM FOREX undertakes to verify the submitted documents within three (3) business days from the date of receipt.
Monitoring and Reporting Transaction-based monitoring is conducted within the appropriate business unit of DAM
FOREX. Specific transaction monitoring will include, but is not limited to, transactions over $5,000 and transactions where DAM FOREX has reason to suspect suspicious activity. All reports are documented.

Suspicious Activity
There are signs of suspicious activity that may indicate money

laundering. These are commonly referred to as "red flags". When red flags are identified, additional due diligence should be conducted before proceeding with the transaction. If no reasonable explanation can be found, the suspicious activity must be reported to the AML Compliance Committee.

Examples of red flags include
A customer expresses unusual concerns about 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 disclose information about business activities, or provides unusual or questionable identification or business documents.

The customer requests a transaction that lacks business acumen or apparent investment strategy or is inconsistent with the customer's stated business strategy.
The customer's information identifying the source of funds is false, misleading or materially inaccurate.
Upon request, the customer fails to disclose or identify the legitimate source of funds or other assets; or The background of the customer (or a person publicly associated with the customer) is in question, or there are press reports indicating possible criminal, civil, or regulatory violations.

There is no concern about risk, fees or other transaction costs; or Appears to be acting as an agent for an undisclosed person, but is reluctant or unwilling to provide information or is evasive about that person or organization without a legitimate business reason.

The customer has difficulty explaining his or her business or lacks general industry knowledge.

The customer frequently requests frequent or large cash deposits, insists on dealing only in cash equivalents, or requests an exception to the company's cash deposit policy.

For no apparent reason, a customer has multiple accounts in one or more names and there are large amounts of transfers between accounts or between third parties.

There are unexplained or sudden large movements in the customer's accounts, especially in accounts that previously had little or no activity.

A customer's account has a high volume of wire transfers to unrelated third parties that are inconsistent with the customer's legitimate business objectives.

There are wire transfers to and from countries identified as money laundering risks or bank secrecy jurisdictions with no apparent business purpose.
Large or frequent wire transfers are made to a customer's account and immediately withdrawn by check or debit card without any apparent business purpose.

A customer deposits funds and then immediately requests that the funds be wired to a third party or another entity for no apparent business purpose.

A customer deposits funds to purchase a long-term investment and then immediately liquidates the position and withdraws the funds from the account.

The customer requests that the transaction be processed in this manner to avoid the firm's normal documentation requirements.

Know Your Customer - The Basics of Suspicious Transaction Recognition A suspicious transaction is often one that is inconsistent with a customer's known legitimate
business or personal activities, or with the normal operations of a customer of that type.

Therefore, knowing enough about the customer's business to

recognize that a transaction or series of transactions is unusual is the first key to recognition.
Questions to consider when determining whether an existing customer transaction is suspicious include Is the size of the transaction consistent with the customer's normal business?

Is the transaction consistent with the customer's business or personal activities?

Has the customer's trading pattern changed?

Suspicious Scenarios
Matters that should raise suspicion include the following Customers who are unwilling to identify themselves;
Customers who place undue trust in the originator (who may be hiding behind the originator to avoid revealing their identity and the true nature of their business);
Requests for cash-related services. For example, asking if investments can be made in cash; suggesting that there may be funds available for investment in cash;
Unclear source of funds available for investment;

Where the amount of funds available appears inconsistent with the client's other circumstances (i.e., the source of wealth is unclear). For example, a student or young person
with substantial investment funds;

If the transaction does not appear reasonable in the context of the customer's business or personal activities; or Particular care should be taken in this area if the customer changes trading practices without a reasonable explanation;

If the pattern of transactions has changed;

If a client who trades internationally appears to have no legitimate reason to do business with the countries involved (e.g., why hold

funds in a particular country where funds come and go? Are there circumstances under which it would be appropriate to hold funds in such countries?)

Customers who are unwilling to provide normal personal or financial information without apparent reasonable cause. (Care should be taken not to suspect all remote relationships,as in most cases there are legitimate reasons for doing so. Usually suspicion is based on cumulative problems, not isolated ones).

The money launderer is likely to make a convincing case for the reason for the transaction.

They should be interviewed to determine whether the transaction is suspicious.

Reporting Suspicions.
If for any reason you suspect that a client or its agent may be engaged in (or about to engage in) a transaction involving the proceeds of crime, you must report it in writing as soon as possible.

The report must be made regardless of whether any work has been or will be done.

Investigation
Upon notification to the AML Compliance Committee, an investigation will be initiated to determine whether the matter should be reported to the appropriate law enforcement or
regulatory authority. The investigation will include, but not necessarily be limited to, a review of all available information, including, but not limited to, payment history, date of birth and address. The investigation will result in a recommendation to the AML Compliance Committee to submit the SAR to the appropriate law enforcement or regulatory authority, if warranted. Notification or submission to law enforcement or regulatory authorities will be the responsibility of the AML Compliance Committee.

The results of the investigation will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances may an officer,
employee or designated representative disclose or discuss an AML concern, investigation, report or SAR submission with the subject or any other person, including a family member of the officer, employee or designated representative.

Freezing Accounts.
If funds in an account are known to have been derived from criminal activity or fraudulent instructions, the account must be frozen. If it is believed that the account holder may be involved in reported fraudulent activity, the account may need to be frozen.