AML POLICY (Last updated July 09, 2019)

ANTI-MONEY LAUNDERING/COUNTER-TERRORIST FINANCING AND KNOW YOUR CUSTOMER POLICY

The purposes of the SIMEX's Anti-Money Laundering and Counter-Terrorist Financing Policy and Know Your Customer Policy (hereinafter - the "AML/CFT and KYC Policy") is to identify, prevent and mitigate possible risks of SIMEX being involved in illegal activity.

In conformity with international and local regulations, SIMEX has implemented effective internal procedures to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to react correspondingly in case of any form of suspicious activity from its Users.

Money Laundering can be defined as: 'the conversion or transfer of property, knowing that such property is derived from criminal activity, or from an act of participation in such activity, for the purposes of concealing or disguising the illicit origin of the property, or assisting any person who is involved in the commission of such activity to evade the legal consequences of his action.'

Terrorist Financing can be defined as: 'the willful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts.' All firms must adhere to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), and be aware of the guidance set down by the Joint Money Laundering Steering Group (JMLSG) which provides guidelines within the United Kingdom on how firms should conduct Due Diligence on their customers, and the recommendations from the Financial Action

Task Force (FATF), an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing.

Other legislation in relation to AML/CTF are:

The Proceeds of Crime Act (POCA), which covers all crimes and any dealing in criminal property, and creates investigative powers for law enforcement agencies and criminal offences in relation to money laundering, for the criminal, the firm and individual employees.

The Terrorism Act, which details a series of offences related to the involvement in arrangements for facilitating, raising or using funds for terrorism purposes.
AML/CFT and KYC Policy includes:

- Verification procedure;
- Compliance Officer;
- Transactions Monitoring;
- Risk Assessment.

The SIMEX’s identification procedure requires the User to provide SIMEX with reliable, independent source documents, data or information (for example, a national ID card, an international passport, a bank statement, a utility bill). For such purposes, SIMEX reserves the right to collect the User's identification information for the purposes of AML/CFT and KYC compliance.

SIMEX take steps to confirm the authenticity of documents and information provided by Users. All legal methods for double verification of identification information will be used, and SIMEX reserves the right to investigate the cases of certain Users whose identities have been identified as dangerous or suspicious.

SIMEX reserves the right to verify the identity of the User on an ongoing basis, especially when its identification information has been changed or its activities appear suspicious (unusual for a particular User). In addition, SIMEX reserves the right to request from the Users current documents, even if they have been authenticated in the past.

Information about the user's identification will be collected, stored, shared and protected strictly in accordance with the SIMEX's Privacy Policy and relevant rules. After confirming the identity of the user, SIMEX may refuse to provide services to the User if SIMEX's services are used for the purposes of conducting illegal activities.

Users who intend to use payment cards for the purpose of consuming services must undergo a card check in accordance with the instructions available on the SIMEX's website.

Compliance Officer

The Compliance Officer is the person, duly authorized by SIMEX, whose duty is to ensure the effective implementation and enforcement of the AML/CFT and KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of SIMEX's anti-money laundering and counter-terrorist financing procedures, in particular:

- collecting Users' identification information;
- establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations;
- monitoring transactions and investigating any significant deviations from normal activity;
- implementing a records management system for appropriate storage and retrieval of

documents, files, forms and logs, updating risk assessment regularly, providing law enforcement with information as required under the applicable laws and regulations.

The Compliance Officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing and other illegal activities.

Transactions Monitoring

The Users are known not only by verifying their identity (who they are) but, more importantly, by analyzing their transactional patterns (what they do).
Therefore, SIMEX relies on data analysis as a risk-assessment and suspicious activity detection tool. SIMEX performs a variety of compliance-related tasks, including capturing data, filtering, record-keeping, investigation management, and reporting.
System functionalities include:

- Daily check of Users on the presence in the recognized "black lists" (e.g. OFAC), aggregating transfers by multiple data points, placing Users on watch and service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, if applicable;
- Case and document management.

In connection with the AML/CFT and KYC Policy, SIMEX will:

- monitor all transactions and it reserves the right to ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Officer;
- request the User to provide any additional information and documents in case of suspicious transactions;
- suspend or terminate User's Account when SIMEX has a reasonable suspicion that such User is engaged in illegal activity.

However, the above list is not exhaustive and the Compliance Officer will monitor

Users' transactions on a regular basis in order to define whether such transactions are to be reported and treated as suspicious or are to be treated as bona fide.

Risk Assessment

SIMEX, in line with the international requirements, has adopted a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, SIMEX is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks.

Last updated: July 8, 2019