MBFX Limited Ltd.

Policy guidelines for operation on Anti-Money Laundering (AML) Know You Customer (KYC)

Combatting financing of Terrorism (CFT)

Reviewed and approved on 14/06/2022

Contents

1. Introduction

As a Forex and CFD broker MBFX Limited Ltd required to implement a money laundering program. At a minimum, this program must include internal policies, procedures and controls to deter, detect, and report suspicious activity; a designated compliance officer; and an internal audit to test compliance. To the extent required MBFX Limited has implemented such a program.

Money Laundering is the involvement in any transaction or series of transactions that seek to conceal or disguise the nature of source of proceeds derived from illegal activities, including drug trafficking, terrorism, organized crime, fraud, and many other crimes.

It also includes the process of converting funds, received from illegal activities (such as fraud, corruption, terrorism, etc.), into other funds or investments that look legitimate to hide or distort the real source of funds.

The process of money laundering can be divided into three sequential stages:

Placement.

At this stage funds are converted into financial instruments, such as checks, bank accounts, and money transfers, or can be used for purchasing high-value goods that can be resold. They can also be physically deposited into banks and non-bank institutions (e.g., currency exchangers). To avoid suspicion by the company, the launderer may as well make several deposits instead of depositing the whole sum at once, this form of placement is called smurfing.

Layering.

Funds are transferred or moved to other accounts and other financial instruments. It is performed to disguise the origin and disrupt the indication of the entity that made the multiple financial transactions. Moving funds around and changing in their form makes it complicated to trace the money being laundered.

Integration.

Funds get back into circulation as legitimate to purchase goods and services. MBFX Limited is committed to the highest standards of the Anti-Money Laundering (AML)

compliance and Anti-Terrorist Financing and require the management, and employees to follow the named standards.

2. Policy Statement

Although MBFX Limited is a limited company formed in Republic of Vanuatu, in addition to any local jurisdictional AML and legal requirements, MBFX Limited is committed, to the extent possible, to following the laws and regulations of the FCA(UK) and CySec, which will be used as a guideline for MBFX Limited AML Program. MBFX Limited expects that its employees, or the employees of one of its affiliates, will conduct themselves in accordance with the highest ethical standards, and that they shall not knowingly provide advice or assistance to, or open accounts for, individuals who attempt to violate or avoid money-laundering laws.

MBFX Limited, like most companies providing services on the financial market, adheres to the principles of Anti-Money Laundering and actively prevents any actions that aim or facilitate the process of legalizing of illegally gained funds. AML policy means preventing the use of the company's services by criminals, with the aim of money laundering, terrorist financing or other criminal activity.

For this purpose, a strict policy on the detection, prevention and warning of the corresponding bodies of any suspicious activities was introduced by the company. Moreover, MBFX Limited has no right to report clients that the law enforcement bodies are informed on their activity. A complex electronic system for identifying every company's client and conducting a detailed history of all operations was introduced as well.

To prevent money laundering, MBFX Limited neither accepts nor pays cash under any circumstances. The company reserves the right to suspend any client's operation, which can be regarded as illegal or, may be related to money laundering in the opinion of the staff.

Important: Money Laundering laws apply not only to criminals who try to launder ill-gotten gains, but also to financial institutions and their employees who participate in those transactions if the employees know that the property is criminally derived. “Knowledge” includes the concepts of “willful blindness” and “conscious avoidance of knowledge”. Employees who are suspicious of illegal activity and yet who do not report that activity may be considered under the law to have the requisite “knowledge.”

Failure to adhere to this Policy may subject MBFX Limited or its affiliate’s employees to disciplinary action up to, and including, termination of employment.

Senior Management

3 Money Laundering Definition

What is Money Laundering?

Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for “clean” money or other assets with no obvious link to their criminal origins.

Criminal property may take any form, including money or money’s worth, securities, tangible property and intangible property. It also covers money, however come by, which is used to fund terrorism.

Money laundering activity includes:

- Acquiring, using or possessing criminal property
- Handling the proceeds of crimes such as theft, fraud and tax evasion
- Being knowingly involved in any way with criminal or terrorist property
- Entering into arrangements to facilitate laundering criminal or terrorist property
- Investing the proceeds of crimes in other financial products
- Investing the proceeds of crimes through the acquisition of property/assets
- Transferring criminal property.

There is no single stage of money laundering; methods can range from the purchase and resale of luxury items such as a car or jewelry to passing money through a complex web of legitimate operations. Usually, the starting point will be cash but it is important to appreciate that money laundering is defined in terms of criminal property. This can be property in any conceivable legal form, whether money, rights, real estate or any other benefit, if you know or suspect that it was obtained, either directly or indirectly, as a result of criminal activity and you do not speak up then you too are taking a part in the process.

The money laundering process follows three stages:

1. Placement

Disposal of the initial proceeds derived from illegal activity e.g., into a bank account.

2. Layering

The money is moved through the system in a series of financial transactions in order to disguise the origin of the cash with the purpose of giving it the appearance of legitimacy.

3. Integration

Criminals are free to use the money as they choose once it has been removed from the system as apparently “clean” funds.

No financial sector business is immune from the activities of criminals and Firms should consider the money laundering risks posed by the products and services they offer.

4 Counter Terrorist Financing (CTF) Definition

What is Counter Terrorist Financing (CTF)?

Terrorist financing is the process of legitimate businesses and individuals that may choose to provide funding to resource terrorist activities or organizations for ideological, political or other reasons. Firms must therefore ensure that:

(i) customers are not terrorist organizations themselves; and
(ii) (ii) they are not providing the means through which terrorist organizations are being funded.

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.

5 Risk Definition

Defining risk

The level of due diligence required when considering anti-money laundering procedures within the firm, it should take a risk-based approach. This means the number of resources spent in conducting due diligence in any one relationship that is subject risk should be in proportion to the magnitude of the risk that is posed by that relationship.

These can be broken down into the following areas:

Customer Risk

Different customer profiles have different levels of risks attached to them. A basic Know your Customer (KYC) check can establish the risk posed by a customer. For example, near-retired individuals making small, regular contributions to a savings account in line with their financial details poses less of a risk than middle-aged individuals making ad-hoc payments of ever-changing sizes into a savings account that does not fit into the profile of the customers' standing financial data. The intensity of the due diligence conducted on the latter would be higher than that carried out on the former as the potential threat of money laundering in the second case would be perceived as being greater. Corporate structures can be used as examples of customers that could carry a higher risk profile than the one just seen, as these can be used by criminals to introduce layers within transactions to hide the source of the funds, and like that, clients can be categorized into different risk bands.

Product Risk

This is the risk posed by the product or service itself. The product risk is driven by its functionality as a money laundering tool.

The Joint Money Laundering Steering Group has categorized the products with which Firms typically deal into three risk bands – reduced, intermediate and increased. Typically, pure protection contracts are categorized as reduced risk and investments in unit trusts as increased risk. Additionally, a factor that will contribute to the classification of the risk category is sales process associated with the product. If the transaction in the product takes place on an advisory basis as a result of a KYC, this will carry less risk than an execution only transaction, whereby you know significantly less about the customer.

Country Risk

The geographic location of the client or origin of the business activity has a risk associated with it, this stems from the fact that countries around the globe have different levels of risk attached to them.

A firm would determine the extent of their due diligence measure required initially and on an ongoing basis using the above four risk areas.

5 Real time risk monitoring

Real time risk monitoring provides all financial and non-financial institutions to perform continuous customer checks and monitor them for a certain time. This AI-powered solution deploys a wide range of algorithms for in-depth monitoring of the clients and develops comprehensive risk profiles that can prevent financial crimes like money laundering. Staying one step ahead of the criminals is what every firm needs and an ongoing AML solution can help companies in achieving the goal.

Why is Ongoing Monitoring Important?

Anticipating problems is the only way that can help companies in combating crime. However, it is impossible without robust identification measures. Any discrepancies in the anti-money laundering solutions can result in severe financial loss. Hence, an ongoing anti-money laundering solution is vital for businesses. It assists businesses in onboarding the right customers and continually monitoring them to secure businesses as long as possible. The global AML screening has many benefits including:

- Identity assurance
- AML onboarding solutions
- Accurate risk profiling
- Reduce false positives
- Updated risk status
- Enhanced compliance screening
- High-security standards, and
- Reduced cost of compliance

MBFX Limited will make sure that it is dealing with a real person or legal entity. MBFX Limited also performs all the required measures in accordance with applicable law and regulations, issued by monetary authorities. The AML policy is being fulfilled within MBFX Limited by means of the following:

- Know your customer policy and due diligence
- Monitoring of client activity
- Record keeping

The AML Officer is responsible for giving the written approval of the firm's AML program and will oversee all compliance matters. The new accounts supervisor, will:

- Receive reports of suspicious activity from firm personnel

- Coordinate required AML reviews/meetings with appropriate staff
- Gather all relevant business information to evaluate and investigate suspicious activity
- Determine whether the activity warrants reporting to senior management
- Design and implement training programs as required by this policy

8 Customer Identification Program / Know Your Client

An effective anti-money laundering program must include “Know your Customer” procedures. Information must be provided to learn the true Identity of the Customer, the nature of the Customer’s Business and the intended Purpose of the Customer’s transactions.

As broker, MBFX Limited shall be responsible for:

- Providing the account application
- Conducting AML and KYC procedures
- Clearing and monitoring of all trades
- Being the custodian of the accounts, funds and paperwork.

Each trading account applicant must first be approved and accepted by the broker before funding the trading account and trading.

- IDENTITY

For each new customer, who is an individual, MBFX Limited will collect:

- The customer’s name
- Date of birth
- Residential or business address
- Proof of address such as utility bill, etc
- Passport number and country of issuance
- Unexpired government identification card number showing nationality or residence, and photo id.

For each new customer which is an entity, MBFX Limited will collect:

- The customer’s business name
- Principal place of business
- Proof of business address such as utility bill, etc.
- Government issued identification
- Other government issued documentation certifying the existence of the business or enterprise such as certified articles of incorporation, a government issued business license, a partnership agreement or a trust instrument

MBFX Limited will not accept an account without the required identification information. If the entity is a trust or similar, personal identification information as outlined in the previous paragraph will be needed for the account controller.

In the event a customer does not present a valid government ID; or the firm is not familiar with the documents the customer provides; and any other circumstances that increase the risk that MBFX Limited will not be able to verify the true identity of the customer through documents an account will not be opened.

9 OFAC check

All individuals and entities will be checked against applicable lists of sanctioned countries published by the Office of Foreign Assets Control (OFAC) and periodically rechecked against updated lists. If a customer is from a country on the list, MBFX Limited will contact OFAC to determine the extent of the sanctions.

All new customers' names will be compared to the list of Specially Designated Nationals (SDN) and Blocked Persons, also found at the OFAC website, by the new account's supervisor. If a customer's name appears on the list, MBFX Limited will contact OFAC immediately.

When the OFAC lists are updated, MBFX Limited will review the existing client base to determine if any current customers are from a country on the sanctioned countries list or if any customer's name appears on the SDN list.

The broker's senior management will be notified immediately of any suspicious activity; Federal Law enforcement will be contacted if a match is found.

- **BUSINESS**

MBFX Limited will be verifying all information given pertaining to business and source of income of a customer. MBFX Limited will not be opening correspondent accounts. If a customer opens an account directly with the broker, and it is found out to be a correspondent account, MBFX Limited will close the account immediately.

- **PURPOSE**

MBFX Limited will be verifying all information given pertaining to the purpose of the trading account.

Although not all inclusive, some examples of behaviour that should cause concern at the account opening stage are:

• A customer exhibits an unusual level of concern for secrecy, particularly with regarding to the customer's identity, type of business or sources of assets;

• A corporate customer lacks general knowledge of its own industry.

• A customer is unconcerned with risks, commissions or other costs associated with trading.

• A customer appears to be acting as an agent for another entity or individual but is evasive about the identity of the other entity.

• A customer is from a country identified as a haven for bank secrecy, money laundering, or narcotics production.

10 UNFS Act screening

United Nations Financial Sanctions Act No. 6 of 2017

What are targeted financial sanctions?

Targeted financial sanctions are a tool used by the international community to prevent or suppress terrorism, the proliferation of weapons of mass destruction (WMD) and the financing of these activities.

The most common types are:

- asset freezes, which prohibit you from:

o dealing with a designated person or entity's property

o making property available to a designated person or entity

- blocking access by a designated person or entity to financial services, including:

o insurance related services

o banking services

o trust and company services.

'Property' includes funds and other assets, such as bank credits, cheques, money orders etc.

'Dealing' includes transferring, converting, disposing of, moving or using property.

'Designated person or entity' refers to individuals, groups, undertakings and entities that have

been designated by the United Nations Security Council (UNSC) or one of its Committees, or by

the Prime Minister under the United Nations Financial Sanctions Act No. 6 of 2017 (UNFSA) because they are associated with terrorism or proliferation of WMD.

Why do we have targeted financial sanctions?

An effective targeted financial sanctions regime is critical to combating the financing of terrorism and proliferation and can also have important deterrent effect. Vanuatu is obliged to implement targeted financial sanctions as a matter of international law, under the Charter of the United Nations and relevant UNSC Resolutions. The Financial Action Task Force Standards also require countries to implement targeted financial sanctions to comply with UNSC Resolutions related to terrorism and proliferation and their financing. Vanuatu implements UNSC sanctions and domestic sanctions under the UNFSA.

How to Comply with the ACT?

What constitutes an adequate compliance program largely depends on our customers and what kind of business you operate. Certain areas of bank operations, such as international wire transfers, are at higher risk than others of being abused for the purposes of terrorist or proliferation financing.

We must screen all customer data on Refinitiv and ShuftiPro (can be done through compliance manager)

What are the penalties for non-compliance?

The UNFSA establishes serious criminal offences for non-compliance. Penalties may include a term of imprisonment up to 25 years, a fine or both. Penalties can apply to natural persons and body corporates.

What do I do if there is a match to the sanctions list?

If you hold, possess or control property of a designated person or entity, you must freeze the property immediately and you must report it to the Sanctions Secretariat within five working days of being notified of the designation; the date of publication of the designation in the Official Gazette; or coming into the possession of the property (whichever is sooner). You must also make a report within two working days of a suspicious transaction or activity, or a transaction involving terrorist property, in accordance with the Anti-Money Laundering and Counter Terrorism Financing Act No. 13 of 2014 (AML/CTF Act).

Failure to make a report is an offence under both the UNFSA and the AML/CTF Act.

You must not:

- deal with the property, or
- make property or a financial service available to the designated person or entity, or a person or entity owned, controlled or acting on their behalf.

What do I do if someone claims there has been a false positive match to the Consolidated List?

A false positive occurs when an individual or entity with the same or similar name as a designated person or entity is inadvertently identified as being a match to a person or entity on the Consolidated List.

If you are approached by an individual or entity that believes they have had their assets frozen in error, you should:

Step 1: conduct an internal investigation in order to determine whether the match is a false positive. Check birth dates and other identifying information to determine whether the account holder is the designated person or entity.

Step 2: If you are unable to determine whether the person is a designated person or entity through an internal investigation, you may seek assistance from the Commissioner of Police to verify whether the person is a designated person or entity.

Step 3: If the Commissioner of Police is unable to advise you whether the person is a designated person or entity, you should direct the person to apply directly to the Sanctions Secretariat for assistance using the form available on the VFIU website.

What is an 'authorisation'?

An authorisation is a permission granted by the Prime Minister to deal with frozen property or make property or a financial service available to a designated person or entity. The Prime Minister will only grant such authorisations where the property or financial service is required to meet a 'basic expense', a 'contractual obligation' or an 'extraordinary expense'

It is permissible to deal with frozen property or make property or a financial service available to a designated person or entity in accordance with an authorisation granted by the Prime Minister under the UNFSA.

11 Suspicious transaction reporting

Suspicious transactions are those that have no business or apparent lawful purpose, are unusual for the customer, or lack any reasonable explanation.

A few examples of “red flags” are:

- A customer engages in extensive, sudden or unexplained wire activity (especially wire transfers involving countries with bank secrecy laws);

- A customer makes a funds deposit followed by a request that the money be wired out, (in and out).

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

For all MBFX Limited accounts, a determination of whether any transaction or series of transactions is suspicious will depend on the customer and the particular transaction(s) compared with the customer’s normal business activity. All accounts will be monitored for suspicious activity every 30 days.

MBFX Limited does not accept third party funds. Also, incoming and outgoing bank wires must be from or to a banking institution having the customer’s name on the account.

The Company’s anti-money laundering procedures mandate that individuals and entities that refuse to provide information verifying their identities will not be permitted to open accounts at MBFX Limited

12 Compliance

Compliance

All new accounts will be approved finally by Compliance manager. Compliance manager will ensure that the new account form is complete. He will review all new accounts for financial credit worthiness and trading suitability purposes. However, he will also review for anti-money laundering purposes.

COMPLIANCE will check to ensure that identifying information is listed for all individuals named on the new account form and that none of the individuals named on OFAC, UNFSA or any other watch lists are opened at the Company.

The stated purpose of customers in placing funds with MBFX Limited is set forth in the MBFX Limited Customer Agreement, to wit: speculation in foreign currencies. Any conduct or account activity that is inconsistent with trading foreign currencies with a goal of profiting thereby, must be considered suspicious activity and reported immediately to COMPLIANCE who will evaluate the situation and determine whether to take further action consistent with these procedures.

The process of "knowing one's customer," through the Customer Identification Program, is not concluded once the initial account opening information has been obtained. Even after the account is established, in the normal course of the relationship, the Company must continue

to build upon the information initially provided by the customer and update their records accordingly.

- Whether the customer is an individual, an intermediary, public, private, domestic or foreign corporation, a financial or non-financial institution, or regulated person or entity;
- Whether the customer has been an existing customer for a significant period of time;
- How the customer became a customer of the Company;
- Whether the business of the customer or the particular type of account, is the type more likely to be involved in illicit activity (e.g., cash intensive businesses)
- Whether the customer's home country is listed on FATF's list of non-cooperative countries or OFAC's/UNFSA list of sanctioned countries or is otherwise subject to adequate anti- money laundering controls in its home jurisdiction; and
- Whether the customer resides in, is incorporated in or operates from a jurisdiction with bank secrecy laws, or one that has otherwise been identified as an area worthy of enhanced scrutiny.

If it is determined to accept a foreign customer account where the country of residence is listed on FATF's list of non-cooperative countries or OFAC's list of sanctioned countries, additional monitoring of the customer's trading and cash activity will be conducted by COMPLIANCE. He will review, in detail, all transactions and cash activity by examining the monthly account statements to ensure that none of the "red flags" set forth in the Wire Activity and Management Review Sections below should be raised.

Subject to the Company's own assessment of any additional due diligence necessary to assess risk, the following procedures are ordinarily appropriate for the following types of accounts:

- US Individual Accounts

Due to the Dodd-Frank Wall-Street Reform Act, we are unable to accept or process an applicant from the United States.

- Non-US Individual Accounts

For accounts opened by an individual, the Company will obtain the following information at the commencement of the business relationship:

- The name and address of the Customer(s);
- A copy of the Customer's Passport and/or driver's license;
- The Customer's date of birth and tax identification number;
- The Customer's investment experience and objectives, if applicable;
- The Customer's net worth and annual income; and
- The Customer's occupation and employment data, such as the employer's address (generally understood to be the Customer's source of income).

- Domestic Operating or Commercial Entities

As part of the requirement to open account, the Company will obtain information sufficient to ascertain the identity of the corporate or business entity opening the account and the authority

of the business representative to act on the corporation's or entity's behalf. This information will also be checked against existing OFAC lists and current databases. The type of documentation obtained by Company may vary depending upon the nature of the corporate or business entity. Accounts that lack this information may not be permitted to continue to do business with the Company. Below is the basic information MBFX Limited requiring:

- Unexpired photo id of all directors
- Articles of Incorporation
- Bylaws' stating that they can trade Forex and that the officer trading has the authority to trade in the company's behalf.
- Business Registration for current address

- Domestic Trusts

The Company will identify the principal ownership of a trust. Identities will be checked against OFAC lists and current databases. In addition, the Company will obtain information regarding the authorized activity of the trust and the persons authorized to act on behalf of the trust. Accounts that do not provide this information on a timely basis will be forbidden to conduct business with the Company.

- Omnibus Account

If such an account is presented to Company management, the Company will first investigate the Financial Institutions to ascertain whether it has adequate anti-money laundering procedures in place to comply with the current regulations and the policies of MBFX Limited

- Commodity Pools

The Company will demand the names, addresses, and dates of birth of all commodity pool participants. Identities will be checked against OFAC lists and current databases. In addition, the Company will obtain information regarding the authorized activity of the pool and the persons authorized to act on behalf of the pool. Commodity Pool Accounts that do not provide this information on a timely basis will be forbidden to conduct business with the Company.

- Foreign Operating Commercial Entities

Commercial entities will be expected to produce forms indicating the identity of persons authorized to place orders on behalf of the commercial entity. COMPLIANCE will review these documents to ensure completeness. The names of the commercial entity and the authorized principals will be compared against the OFAC list and a current database.

- Personal Investment Corporations or Personal Holding Company

Accounts must identify the principal beneficial owner(s) of offshore corporate accounts where such owners are personal investment corporations or personal holding companies. The names of the holding company and the principal owner will be compared against the OFAC list and a current database.

- Offshore Trusts

Accounts must identify the principal ownership of a trust established in a foreign jurisdiction. The Company will ask for information about the trust and its participants in order to conduct additional due diligence for trusts established in jurisdictions which lack regulatory oversight over trust formation. Although the documentation may vary, the Company must obtain

sufficient documentation regarding the principal ownership of the account. Additional due diligence may also be warranted depending on a number of factors, including the location of the offshore entity and the location of the principal owner(s). The names of all entities will be compared against the OFAC list and current database.

Accounts will not be opened for “foreign shell banks,” A foreign shell bank is defined as a foreign bank that does not have a physical presence (such as headquarters building, staff of employees, etc.) in any country.

All employees should be alert for any situations that may be “indicators” for potential money laundering activities.

- Customer exhibits an unusual concern regarding the Company’s compliance with government reporting requirements, 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.

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

- Customer has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations.

- Customer has difficulty describing the nature of his business or lacks general knowledge of his or her industry.

Employees, who become aware of any such situations when accounts are being opened, should promptly notify COMPLIANCE of the potential suspicious activity. COMPLIANCE will make the decision if the account should be opened as is, request additional information, reject the account and/or report the activity to the Company’s DSRO or the FIU.

- **Intermediary Accounts**

MBFX Limited will accept business only from intermediaries whom we are confident are regulated and registered by a local exchange/authority with AML policies, and that a complete, in- house review of those policies shows compliance, compatibility and enforcement in line with the policies followed by MBFX Limited This will include risk-based analysis of the money laundering risks posed by the particular intermediary and their reputation in the industry. The policy’s implementation will be reviewed and audited as part of the ongoing relationship on a not less than annual basis and more often if suspicious activity occurs. This process will include reviewing the entities own internal review notes, changes, audits and follow through.

We will do our own client verifications and activity monitoring as stated in this document as rigorously for Introducing Brokers as for our immediate clients since we share direct responsibility with them for its accuracy and have access to these clients’ documents. Since it is unlikely that our International carrying brokers who have the direct relationship with the customer will want to

disclose their client’s identities they must assume the responsibility for verifying the accuracy of the client information. This puts a greater emphasis on the risk-based analysis of the money laundering potential and the reputation of both the entity and the regulatory agency they are registered with in their area in our initial decision whether or not to do business with the particular company.

If after suspicious activity has been reported to any of the above entities, the response of the intermediary is not in line with their own or MBFX Limited policies, the relationship with them will be terminated.

- **Rejected Accounts**

No account will be allowed to trade until all account documents have been received and processed. If we are unable to verify the identity of the individual or entity, the account will be rejected. If it becomes apparent after an account has been funded that the sources provided were fraudulent or the circumstances have changed and cannot be verified, all trades will be closed and the account closed immediately.

Other events which can cause an account to be rejected include

- Previous violations or sanctions by the Vanuatu Financial Intelligence Unit (FIU)
- Account funded by someone other than the account holder
- Client attempts to fund the account with cash.
- The country of origin is on the OFAC list
- The applicant is included in the OFAC/FIU list of blocked persons and entities

13 Money Flow Policies

Clients will deposit their funds directly into a MBFX Limited brokerage bank account.

MBFX Limited does not accept third party funds. All deposits and withdrawals must be from and to the same bank account.

MBFX Limited will monitor all accounts for suspicious activity. Anything causing concern must be reported to senior management within one business day.

14 FIU Reporting

To the extent required and/or permitted by law, MBFX Limited may file a suspicious activity report (SAR) for a transaction or series of transactions that are conducted, attempted by, at or through the firm, involving an aggregate of at least $5,000 in funds or other assets (not limited to currency), and the firm knows, suspects, or has reason to suspect that the transaction or pattern of transactions involves funds that come from illegal activity or are a part of a transaction designed to conceal that the funds are from illegal activity; and are designed, such as through structuring, to evade the reporting requirements of the FIU; and do not appear to serve any business or apparent lawful purpose; and use the firm to facilitate a criminal transaction. The SAR will be filed with FIU within 30 days after MBFX Limited becomes aware of a suspicious transaction or if identity is unknown, an additional 30 days. If filed, a copy of the SAR and any supporting documentation that assisted in the decision to file a SAR will be maintained in the AML Compliance. The documentation will be kept in a file per each SAR, as well as scanned and maintained in a data file by the compliance officer.

UNDER NO CIRCUMSTANCES MAY SUCH INDIVIDUAL BE INFORMED THAT A SAR HAS BEEN CONSIDERED OR FILED.

MBFX Limited is prohibited from notifying any person involved in the transaction that the transaction has been reported. Also, any person who has been subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR must decline to produce the SAR and must notify the FIU that such a request was made, except where disclosure is requested by the FIU, law enforcement, or a regulatory authority.

MBFX Limited will require verification that any requests for SAR supporting documentation come from a representative of the FIU or an appropriate law enforcement or supervisory agency. Acceptable verification could include calling the phone number given, checking on-line, or reviewing the letterhead.

MBFX Limited will require a written request from any law enforcement agency requesting that the firm keep a particular account open. A copy of this request will be maintained for five years after the request has expired.

MBFX Limited will, from time to time, monitor the FIU's website for information on foreign jurisdictions, institutions, classes of transactions, or types of accounts that have been designated as a primary money laundering concern and any special measures that have been imposed. If any special measures have been imposed, MBFX Limited will follow through with those measures.

To the extent required by law MBFX Limited may monitor and review the FIU's restricted country list. If a customer comes from a country on the list, additional due diligence may be taken. If the customer has not opened an account, the account will not be opened until due diligence has been completed.

To the extent required by law MBFX Limited may monitor and review lists of known or suspected terrorists or terrorist organizations issued by a Federal government agency and designated as such by Treasury. If a customer is found to be on any of these lists, the account will either be closed immediately or not allowed to open.

15 Qualified Staff and trainings

All employees involved in the handling of customer money will be subject to background/credit checks before they are allowed duties that involve customer money or securities.

Employee training regarding the firm's AML policies and procedures will occur upon hiring and follow-up training will take place not less than once a year.

MBFX Limited will maintain a record that identifies all employees that have received AML training, the dates of the training, and materials covered.

The only employees exempted from this training will be those with no customer contact and no handling of customer funds. Marketing and public relations employees will normally fall into this exempt category.

Updates and changes to the firm's policies/procedures will be provided in writing.

16 Record Keeping

Records may be maintained in either electronic or hard copy for a length of time required by law. The records to be kept include: all identifying information obtained from the customer, a copy of any document that was used to verify identity, a description of any non-documentary verification methods or additional methods used to verify, and a description of how MBFX Limited resolved all substantive discrepancies noted.

17 Independent Audit

If necessary, an annual audit will be conducted of MBFX Limited money laundering compliance program. The audit will test all areas to ensure that personnel understand and are complying with the anti-money laundering policies and procedures, and that these policies and procedures are adequate. The results of this audit will then be documented and reviewed by Senior Management.

Appropriate supervisory personnel for MBFX Limited have reviewed and evaluated the current procedures of MBFX Limited Ltd, and it appears that the current AML procedures are adequate to meet its supervisory responsibilities.

18 GENERAL DATA PROTECTION REGULATION (GDPR) and Policy

WHAT IS GDPR AND HOW DOES IT AFFECT YOU?

The General Data Protection Regulation (GDPR) introduced on the 25 May 2018 seeks to protect European Union citizens in regards to the processing and movement of their personal data. The rules apply to all institutions in the EU that process such personal information and give consumers the right to know what kind of data a company has on them and to choose to delete such information. In this respect, a company needs to have the consent of its clients to use their information.

This is a very positive change for clients. The new regulation reinforces your personal data rights, introduces higher standards for keeping such data secure and gives you more opportunities to question what you are signing up for, opt out from future communications and make a claim for damage resulting from the misuse of your data.

WHAT WE DID IN ORDER TO COMPLY WITH GDPR:

We have updated our Privacy Policy, Cookies Policy and Client Agreement on how we collect, use, control and process your personal data.

The following are changes we made to protect your rights:

- Your consent to process your data is now required.
- You are aware of the reasons and the kind of personal data we collect: contact, family and professional data, tax and financial data.
- You know who receives your data.
- You can object to the use of your data for marketing activities.
- Your personal data is kept for an additional 5 years after the end of our business relationship with you.
- You have a clear outline of your rights in regards to the data we hold on you.
- Your data may be processed outside the EU, when these are shared and processed with other companies of the MBFX LIMITED Group.

- You can decide which cookies to accept with our Cookie control.

You can further review the changes by reading the respective policies.

Privacy Policy

MBFX Limited provide our customers with foreign exchange contracts (FX) and contracts for differences (CFD) trading.

This policy sets out the basis on which any personal information we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal information and how we will treat it. By using our website, you agree to be bound by this privacy policy.

Purpose of the Information processing

We are required to maintain certain personal information about individuals for the purposes of satisfying our operational and legal obligations (to open an account, transact business effectively and to safeguard your assets and your privacy). We recognize the importance of correct and lawful treatment of personal information as it helps to maintain confidence in our organization and to ensure efficient and successful outcomes when using this information.

We only use personal information as appropriate to provide you with a high quality of service and security. For example, we may use the information collected from you to verify your identity and contact information and to establish the business relationship with you. We may also use this information to establish and set up your trading account, issue an account number and a secure password, maintain your account activity, and contact you with account information. We also use your personal information to process and execute your trading orders. We also may use your personal information in order to receive or send payments to you / from you. In this case, we may share your personal information with external payment provider, which you use to process the payment to us / from us, for example: your bank, corresponding banking institution, payment services provider. All this information helps us improve our services and inform you about new products, services or promotions that may be of interest to you.

Security of Personal Information

We maintain strict security standards and procedures with a view to preventing unauthorized access to your information by anyone, including our staff.

We use different organizational and technological measures to protect your personal information such as pseudonymization and encryption. As a part of the pseudonymization process when you establish a business relationship with us, we assign to your accounts (both ewallet and trading account) the unique identifiers (UID) which make your personal information no longer be attributed to you without the use of additional information from our information system. Your UID instead of your name is used in most of the information systems we utilize to provide you with our services. Only a limited number of our staff and third parties have an access to the information system where your personal information in conjunction with UID is stored.

We use leading encryption technologies to secure your information on a hardware and software levels. The hardware protection includes Cisco security products. The software protection tools include strict control mechanisms as follows: SSL, TLS with keys larger than 2048-bit.

All Foxen members, all our staff and third parties whenever we hire them to provide support services, are required to observe our privacy standards and to allow us to audit them for compliance.

Where Personal Information is stored and processed

Personal information collected by MBFX Limited may be stored and processed in your region or in any other country where MBFX Limited or its affiliates, subsidiaries or service providers maintain facilities. Typically, the primary storage location is in the European Union, with a backup to the information centers in another regions. The storage location(s) are chosen in order to operate efficiently, to improve performance, and to create redundancies in order to protect the information in the event of an outage or other problem. We take steps to ensure that the information we collect under this privacy statement is processed according to the provisions of this statement and the requirements of applicable law wherever the information is located.

We transfer personal information to other countries. When we do so, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your information.

Retention of Personal Information

As a general rule, MBFX Limited retains your personal information for the whole period of the business relationship with you and 5 years from the moment termination of such relationship. However, the period of your personal information retention can vary for different information types in the context of different products, actual retention periods can vary significantly. The criteria used to determine the retention periods include, for instance:

- The period of information processing needed to provide the services. This includes such things as maintaining and improving the performance of those services, keeping our systems secure, and maintaining appropriate business and financial records. This is the general rule that establishes the baseline for most information retention periods.

- The information subject's consent for a longer retention period. If so, we will retain information in accordance with the consent.

- MBFX Limited is subject to a legal, contractual, or similar obligation to retain the information. Mandatory information retention laws including AML/CFT regulations can be applied in the applicable jurisdiction, government orders to preserve information relevant to an investigation, or information that must be retained for the purposes of litigation.