



AML Policy

Vorbex Capital Markets (UK) Limited
Authorised and regulated by the Financial Conduct Authority – FRN 186171
St Clement's House, 27-28 Clement's Lane, London EC4N 7AE
Email: info@vorbex.com
Tel: + 44 203 906 7347



VORBEX AML/CTF policy

This document is developed for Vorbex (reg. No HY00623410) clients to get acquainted to Vorbex Anti Money Laundering policies, practice principles, risk appetite and to understand the principles of Anti Money Laundering in general, which Vorbex complies with.

Vorbex (reg. No HY00623410) is registered in Comoros Islands with its registration address at Bonovo Road – Fomboni, Island of Moheli, Comoros Union. Vorbex operates under International Brokerage and Clearing House License (license number: T2023320), issued by Mwali International Services Authority (https://mwaliregistrar.com/list_of_entities/authorised_brokerage_companies).

Vorbex is regulated under Mwali International Services Authority Anti-Money Laundering Law 2014, LAW N°13-003/AU Regulating the activities of financial institutions and complies with Guidelines for the implementation of AML/CFT measures by financial institutions covered by banking law no. 13-003/AU.

Under these regulations and according to Vorbex internal procedures we obligated to execute client's due diligence processes (i.e., client's identification, transactions analysis, beneficial owner analysis, source of funds analysis, suspicious transactions monitoring and reporting, etc).

By accepting Vorbex Customer Agreement on the website, you acknowledge and understand that Vorbex may execute above mentioned processes without your prior notice and permission.

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 jewellery 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:

Placement:

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

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.

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.



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 organisations for ideological, political, or other reasons. Firms must therefore ensure that:

- clients are not terrorist organisations themselves;
- and (ii) they are not providing the means through which terrorist organisations 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.

Risk-Based Approach

The level of due diligence required when considering anti-money laundering procedures within the company, it should take a risk-based approach. This means the amount 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:

Client Risk

Different client profiles have different levels of risks attached to them. A basic Know your Client (KYC) check can establish the risk posed by a client. For example, near-retired individuals making small, regular deposits poses less of a risk than middle-aged individuals, registered in high risk countries making ad-hoc deposits of different amounts and different deposit methods.

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 client 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 categorised into different risk groups.

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.



Channel risk

Channel risk is determined by whether the delivery of a product or service involves face to face contact with the client, as face to face contact limits the ability for client anonymity and facilitates establishing whether the client is who they are claiming to be. Vorbex uses non face to face delivery channels.

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 AML / CTF risk attached to them, and the financial system is complied with different laws in different jurisdictions, this means to inject illicit funds into financial system might be easier in one country, compared to another.

Customer Due Diligence

Vorbex has adopted a Customer Due Diligence. Vorbex will provide notice that they will seek documents / information from the client; collect client identification information and verify such information.

Identification

The standard identification requirement for client who are private individuals are generally governed by the circumstances relating to the client, i.e., country of residency, deposit volumes, etc..

The following pieces of information are required as a standard for identification purposes:

Name, surname

date of birth,

country of residency

Client identification verified from government issued documents, such as

Valid passport

Valid national identity card

Valid residence permit
etc.



Know your client

When a business relationship is formed, in order to establish what might constitute normal activity later in the relationship, it is necessary for the Vorbex to ascertain the nature of the business a client expects to conduct (e.g., volumes, deposit methods, etc.). Information regarding a client's income, occupation, source of funds (if applicable), is also typically gathered.

Once a business relationship has been established, any regular business undertaken for that client can be assessed against the expected pattern of activity of the client. Any unexplained activity can then be examined to determine whether there is a suspicion of money laundering or terrorist financing.

Source of Funds

When a deposit takes place, the source of funds confirmation might be requested. The purpose of this request is to eliminate chances of receiving illicit funds by Vorbex.

Monitoring and reporting

The Company ensures ongoing monitoring of its clients and their transactions during the entire business relationship period.

Ongoing monitoring measures consist of:

Transaction screening

Client's screening

Identification, assessment and reporting of suspicious transactions.



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 department.

Examples of red flags are:

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

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

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

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

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

The client 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 client has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

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

The client's account has a large number of wire transfers to unrelated third parties inconsistent with the client's legitimate business purpose.

The client'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 client requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.

A suspicious transaction will often be one which is inconsistent with a clients' known, legitimate business or personal activities or with the normal business for that type of client. Therefore, the first key to recognition is knowing enough about the client's business to recognise that a transaction, or series of transactions, is unusual.

Possible suspicious scenarios:

Clients who are reluctant to provide proof of identity;

Clients who place undue reliance on an introducer (they may be hiding behind the introducer to avoid giving you a true picture of their identity or business);

Where the source of funds for investment is unclear;

Where the volumes of the available funds appear inconsistent with the client's other circumstances (i.e., the source of wealth is unclear).

Where the transaction doesn't appear rational in the context of the client's business or personal activities. Particular care should be taken in this area if the client changes their method of dealing with you without reasonable explanation;

Where the pattern of transactions changes;

Where a client who is undertaking transactions that are international in nature does not appear to have any good reason to be conducting business with the countries involved;

Clients who are unwilling to provide you with normal personal or financial information, for no apparent or rational reason.

Reporting a Suspicion

Where, for whatever reason, we suspect that a client, or anybody for whom they are acting, may be undertaking (or attempting to undertake) a transaction involving the proceeds of any crime it must be reported as soon as practicably possible. Internal reports must be made regardless of whether any business was, or is intended to be, actually written.

Freezing of accounts

Where we know that the funds in an account derive from criminal activity, or that they arise from fraudulent instructions, the account could be frozen. Where it is believed that



the account holder may be involved in the fraudulent activity that is being reported, then the account may need to be frozen.

Record keeping:

the Company shall maintain records of:

- the client identification documents, and information obtained during the client identification and due diligence procedures, as applicable
- the details of all relevant records with respect to the provision of payment processing and money transmission services to clients
- the suspicious activity detection and reporting records

The documents/data mentioned above shall be kept for a period of at least five (5) years, which is calculated after the execution of the transactions or the termination of the Business Relationship.

Geography:

Although Vorbex welcomes clients all over the world, unfortunately governmental restrictions, regulations, AML best practices prohibit Vorbex from opening accounts originated or somehow related to some countries, that's why some account applications may be unable to proceed, however, in some cases, additional questions can be asked regarding country of residency confirmation.

