

KNOW YOUR CUSTOMER (KYC) POLICY

An effective anti-money laundering compliance program must contain customer identification (KYC) procedures. It is necessary to collect information to confirm the authenticity of the client's identity, determine the nature of his activities and establish the intended purposes of his financial transactions. JPM Analytics, 192 Green Road, Penistone, Sheffield, South Yorkshire, England, is responsible for:

(a) Initiating the account opening process; (b) Implementation of AML (anti-money laundering) and KYC compliance procedures; (c) Ensuring clearing and supervision of all transactions; (d) Maintaining records of these accounts, funds and related documentation.

Individuals intending to open a trading account are required to undergo an approval and acceptance process by JPM Analytics prior to depositing funds and starting trading activities.

PERSONAL IDENTIFICATION

For each new individual customer, the organization requests the following information:

(a) The client's full name; (b) His/her date of birth; (c) Address of residence or place of business; (d) Proof of address (e.g. utility bill or similar); (e) A valid government-issued photo ID that proves citizenship or resident status.

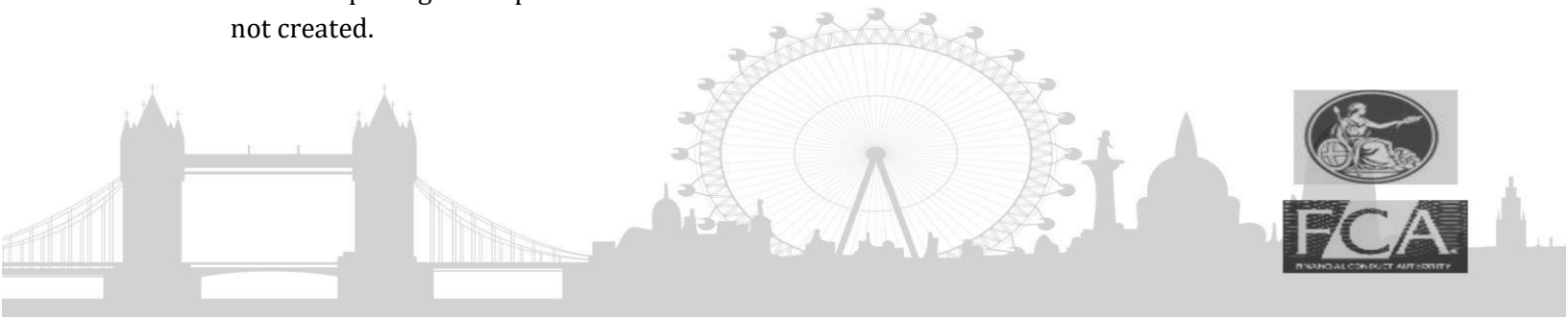
For each new customer who is a legal entity, the company requires: (a) Full name of the organization; (b) The principal address of the activity; (c) Proof of registered office (e.g. utility bill or equivalent); (d) Government identification or tax number; (e) Other official documents evidencing the existence and legal status of the entity (e.g. certified articles of association, business license, partnership or trust agreement).

Opening an account is not possible without providing the said identification information. In the event that the client acts through a trust or similar structure, the person exercising control over the account is obliged to provide personal data for identification in the manner specified above.

If the client does not present a valid state identity card, the company rejects the submitted documents, the client registers remotely without personal presence, or other circumstances arise that increase the risk of inability to verify his identity, the account will not be opened or will remain blocked until all requirements are met.

PROCEDURES

The Company verifies all information related to the client's activities and the origin of his income. Opening correspondent accounts is not allowed. Personal bank accounts are also not created.



PURPOSE OF INSPECTIONS

The Company examines the data related to the purposes for which the trading account is used. Although the list is not exhaustive, the following examples of conduct may raise doubts at the stage of opening an account: (a) The Client is overly concerned about confidentiality issues, in particular regarding his identity, the nature of the business or the origin of funds; (b) the corporate client demonstrates a lack of understanding of its industry; (c) the Client has no interest in the risks, commissions or other costs associated with trading activities; (d) A customer who is presumed to be acting on behalf of another person or entity evades disclosing their identity; (e) The Client is a resident of a jurisdiction known to have a high level of bank secrecy, money laundering or drug production.

SUSPICIOUS TRANSACTIONS

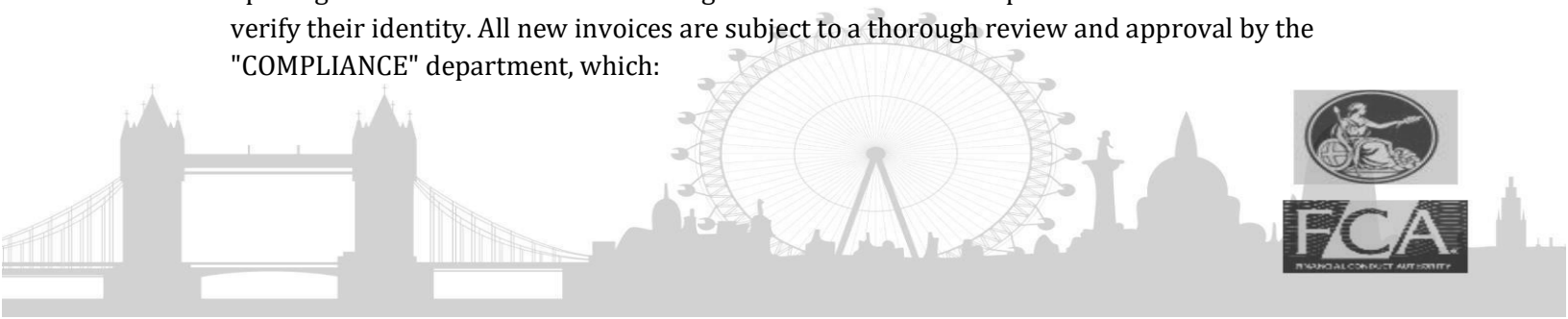
Suspicious transactions are transactions that do not have an obvious commercial or legitimate purpose, differ from the usual behavior of the client or do not have a logical justification. Examples of "alarms" include: (a) The customer's involvement in unexpected, large-scale, or unexplained wire activity, particularly when transferring through jurisdictions with bank secrecy laws; (b) Depositing funds into the account by the client with a subsequent request for their transfer (both incoming and outgoing); (c) A customer has multiple accounts in the same or different names with frequent transfers between them for no apparent reason.

The identification of suspicious transactions or sequences of transactions is based on the client profile and the correlation of operations with its normal behavior. All accounts are subject to a monthly review for suspicious activity (every 30 days). Funds from third parties are not accepted. Incoming and outgoing bank transfers must go through the same banking institution where the account is opened in the name of the client.

CUSTOMER IDENTIFICATION PROGRAM

JPM Analytics is required to identify its customers, understand the nature of their activities and determine the purposes of their transactions.

In the course of anti-money laundering procedures, the company is prohibited from opening accounts for individuals and legal entities that refuse to provide information to verify their identity. All new invoices are subject to a thorough review and approval by the "COMPLIANCE" department, which:



- Checks the correctness of filling out the account opening form;
- Assesses solvency and compliance with trade criteria;
- Performs verification within the framework of AML;
- Confirms that all identification data has been provided for the persons named in the application and that they are not available in the watchlists or in the databases of third parties used by the company.

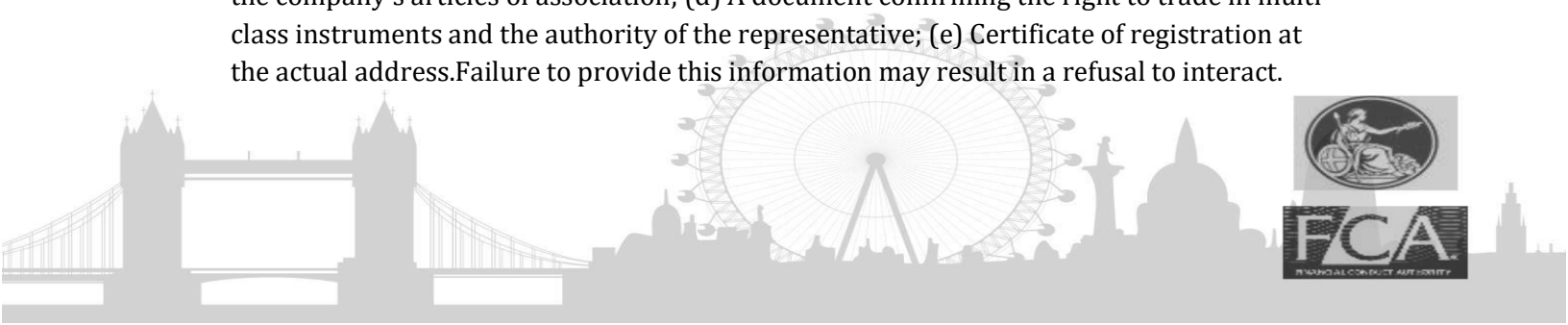
The purpose of clients' use of funds, in accordance with the client agreement, is to speculate and/or trade in contracts for difference (CFDs) on currencies, commodities, metals and indices. Any activity that is not related to trading in the Forex, CFD, Forex, Metals or Indices markets for profit is considered suspicious and must be immediately reported to the "COMPLIANCE" department. This department carries out the analysis and decides on the next steps in accordance with the regulations in force.

When assessing the risks of violation of the AML policy, the following factors are taken into account: (a) Category of the client (individual, intermediary, public or private company, regulated person, etc.); (b) The duration of the client's interaction with the company; (c) Customer acquisition method; (d) An association of the customer's activity or account type with an increased risk of illegal activity (e.g., cash transactions); (e) The client's residence in sanctioned, improperly cooperative jurisdictions or with strict bank secrecy laws; (f) Residence or registration of the client in areas requiring enhanced control.

When taking on a client from a country under UN sanctions or included in the list of non-cooperative jurisdictions, the COMPLIANCE department carries out in-depth monitoring of trade and financial activities, including the analysis of monthly statements in order to detect "red flags".

TYPES OF ACCOUNTS AND VERIFICATION MEASURES

Businesses To open an account, a company collects information to verify the identity of the person opening the account and to verify the authority of the entity's representative. The information received is checked against existing databases and lists. The list of documents requested varies depending on the type of legal entity, but includes: (a) Identification documents with photographs of all directors; (b) Taxpayer Identification Number (TIN); (c) the company's articles of association; (d) A document confirming the right to trade in multi-class instruments and the authority of the representative; (e) Certificate of registration at the actual address. Failure to provide this information may result in a refusal to interact.



TrustsThe company determines the main beneficiary of the trust, checks persons against lists and databases, and also requests information about permitted activities and authorized representatives. Failure to provide information within the established period deprives the right to cooperation.

Omnibus AccountsPrior to opening such an account, the financial institution is checked to ensure that adequate AML procedures are in place in accordance with applicable laws and the Company's policies.

Personal investment companies and holdingsAccounts are required to contain information about the beneficial owners. Their information is checked against existing lists and databases.

EMPLOYEE RESPONSIBILITY

Employees should be on the lookout for any indicators of potential money laundering, including: (a) Excessive confidentiality alertness or refusal to provide information about their business; (b) Involvement of the client in transactions that do not have business justification or are not in line with its strategy; (c) The fact that the client has a suspicious reputation in the media; (d) Failure of the client to provide an explanation as to the nature of his or her business.

In case of detection of such cases, employees immediately inform the "COMPLIANCE" department, which determines the next measures: opening an account, requesting information, refusal or contacting law enforcement agencies.

JPM Analytics (Financial Management Limited)

192

Green Road, Penistone,

Sheffield, South Yorkshire, England

