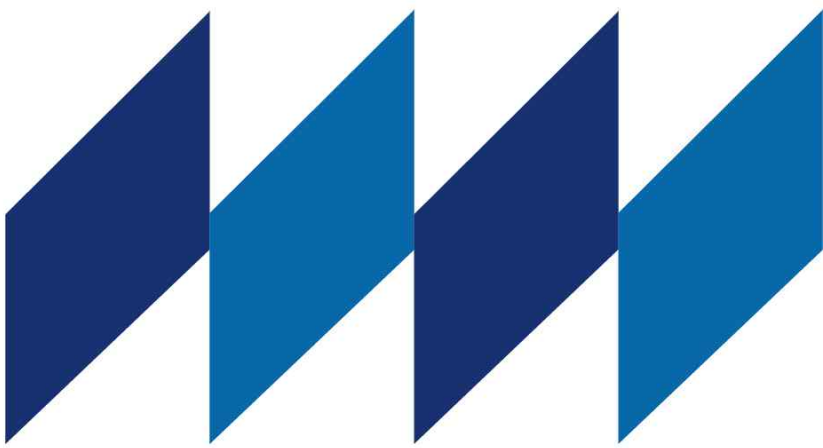
Anti-Money Laundering Policy

JB Financial Group



JB Financial Group

Anti-Money Laundering Policy

1. Due Diligence System to Identify Risky Customers

· Customer Due Diligence (CDD)
  - We conduct customer due diligence if we consider there are concerns over opening of new accounts, one-off financial transactions, money laundering, etc.
  - We inspect and verify the customer's identity, transaction purpose and the beneficial owner, etc.

· Risk Assessment
  - We identify and evaluate risks related to money laundering (country risk, customer type, product and service risk, etc.) and use them to verify the customer's identity.

· Verification of Beneficial Owner
  - Beneficial owner refers to a natural person who ultimately owns or controls an interest of a customer.

2. Non-face-to-face due diligence system to verify risky customers

· Non-face-to-face Real Name Verification
  - We conduct customer due diligence including non-face-to-face real-name verification when a customer opens an account.
  - In the case of non-face-to-face transactions, we conduct strengthened customer verification procedures.

3. Due Diligence System to Prevent Terrorist Financing

· Before a financial transaction is completed, we must verify whether the transaction customer falls under the category of person of interest as set forth in the following subparagraph through comparison with the information on the watch list, and take appropriate measures such as obtaining approval from the compliance officer before starting a business relationship with the person concerned.

- The list of persons whose financial transactions, etc., are restricted, as announced by the Financial Services Commission pursuant to the Act on Prohibition against the Financing of Terrorism;
- Persons subject to sanctions designated by the United Nations
- Nationals (including individuals, legal entity, and organizations) or residents of high-risk jurisdictions and non-compliance jurisdictions announced by the Financial Action Task Force (FATF)
- The list of persons whose financial transactions, etc., are restricted, as announced by the government of the country where overseas branches are located due to concerns about money laundering, etc.
- A list of Foreign Politically Exposed Persons, etc.

4. Politically Exposed Persons (PEP)

· 'Foreign Politically Exposed Person' refers to person who has or had political and social influence in a foreign country, or a person who has a close relationship with such person or his/her family.

· In the event of any of the following cases, approval from the compliance officer must be obtained in relation to foreign PEPs:

- When a foreign PEP opens a new account, whether or not to allow the transaction;
- When a customer (or beneficial owner) who has already opened an account is identified as a foreign PEP, whether or not to continue to do business with that customer.

5. Senior Management's Approval of Products and Countries with Risks such as Money Laundering/Terrorist Financing

· Approval of new-product risk assessment

- When a department in charge of the development of products and services develops new financial products and services, it must conduct a risk assessment in accordance with the 'New-Product Risk Assessment Table' to identify risks such as money laundering before obtaining approval from the compliance officer.

· Approval for high-risk jurisdictions
  - Nationals or residents of high-risk jurisdictions and non-compliance jurisdictions announced by FATF must obtain approval from the compliance officer to establish business relationships.

6. Independent Audit

· In accordance with Article 5 of the Act on Reporting and Using Specified Financial Transaction Information, an audit must be conducted by a department or an organ that is independent of the department in charge of the work of preventing money laundering and financing of terrorism.

7. Retention of Anti-money Laundering related Data

· In accordance with Article 5-4 of the Act on Reporting and Using Specified Financial Transaction Information' we must retain internal and external reports and related documents including customer identification records, financial transaction records, reports of suspicious transactions and large amounts of cash transactions for five years from the time the relationship involving a financial transaction, etc., is terminated.