MUFG

Global Anti-Money Laundering ("AML") Policy

Our Commitment to AML/Countering the Financing of Terrorism ("CFT") Compliance

MUFG Bank, Ltd., ("MUFG Bank" or "Bank"), a subsidiary of Mitsubishi UFJ Financial Group, Inc., recognizes that the Bank's continued success depends in large part upon the trust and confidence of its millions of clients across the globe. As a member of the Wolfsberg Group,[1] MUFG Bank is committed to supporting the integrity of the financial system and combating financial crimes.

Consistent with its zero-tolerance approach for acts of knowingly facilitating money laundering and terrorist financing as set forth in the MUFG *Group Code of Conduct*, MUFG Bank established the Global AML Policy to promote compliance with the letter and spirit of all applicable AML/CFT laws.[2]

Global AML Policy and Program

The Bank's Global AML Policy, which is made available to all employees, prohibits:

- Knowingly facilitating or participating in any financial crimes activity or any activity that facilitates financial crimes (e.g., money laundering and financing of criminal activities);
- Ignoring information or circumstances that may be indicative of financial crimes;
- Informing any person known to be involved or suspected of being involved in illegal or suspicious activity that such activity is being investigated or reported internally and/or to law enforcement authorities and regulatory agencies (known as "tipping off");
- Allowing a new customer to transact (other than initial deposit) prior to completion of the know-your-customer ("KYC") process;[3] or
- Onboarding a prohibited customer type, without appropriate exception or exemption, as detailed in MUFG Bank's *Global KYC Standard*.

Consistent with MUFG Bank's Global AML Policy, the Bank has established an AML compliance program including the following risk-based control processes to the extent applicable:

- Policies and Standards: Global Policy and standards with adherence to regulations in each jurisdiction in which the Bank operates;

- Responsible Officer for each Subsidiary: Designated persons responsible for the implementation and monitoring of the program, including a Global Head of AML and dedicated AML officers in each country of operation;

[1] An association of twelve banks seeking to develop frameworks and guidance for the management of financial crimes risk.

[2] Applicable AML/CFT laws include the Prevention of Transfer of Criminal Proceeds Act in Japan, the Currency and Foreign Transaction Reporting Act of 1970 (also known as the Bank Secrecy Act) as amended by the Anti-Money Laundering Act of 2020 and Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (also known as the USA PATRIOT Act) in the United States, the Proceeds of Crime Act 2002 and the Criminal Finances Act 2017 in the United Kingdom, and the local laws in every country in which the Bank does business.

[3] MUFG Bank may permit a potential customer to execute transactions before completing the customer verification process where doing so is essential to avoid interruptions to the normal conduct of business and does not conflict with local law. In limited circumstances, MUFG Bank may permit a temporary extension to complete the KYC process or an exemption/exception from a particular KYC requirement.

- Risk Assessment: Annual AML risk assessments covering the Bank's customers, products and services, and geographies and related controls;

- KYC Framework: Risk-based know-your-customer processes that require identification and appropriate verification of customer identities (including identification of ultimate beneficial owners, as appropriate), customer screening,[4] customer due diligence, enhanced due diligence, customer acceptance/rejection, and periodic customer reviews;

- AML Transaction Monitoring: Transaction monitoring systems and processes designed to detect unusual and potentially suspicious activity;

- AML Suspicious Activity Investigation and Reporting: Investigation processes to identify and report suspicious activity in compliance with applicable regulatory requirements;

- Prohibition on Certain Customer Types: Prohibitions on relationships with certain customer types, including a prohibition on relationships with shell banks;

- Information Sharing Protocols: AML information-sharing process to cooperate fully with regulators, law enforcement agencies, affiliates, financial institutions, and national investigative units, within the confines of applicable privacy laws and data protection controls;

- Training: Periodic employee training on applicable AML risks and controls (e.g., policy and procedure requirements);

- Recordkeeping: Maintaining comprehensive records related to the Bank's AML compliance program;

- Monitoring/Control-Based Reviews: Risk-based evaluations, including quality assurance reviews, of AML-related activities to confirm compliance with the Global AML Policy requirements; and

- Compliance Testing and Auditing: Periodic compliance testing and auditing of the design and effectiveness of AML-related control processes.

Employee Responsibilities and Consequences of Non-Compliance

Our people play an important role in the fight against for acts of money laundering and terrorist financing. All employees are responsible for complying with the Global AML Policy and are encouraged to proactively manage AML risks, including asking questions when unsure about any aspect of the *Global AML Policy* or associated controls, and escalating concerns promptly to management or through our anonymous reporting channels. The Bank prohibits retaliation against anyone who raises concerns in good faith. Employees who violate the Global AML Policy may be subject to disciplinary measures, up to and including termination and possible referral to regulators and other legal authorities.

[4] As per internal procedures, customer screening includes screening against, among other things, applicable lists of sanctioned parties, internally prohibited parties, and politically exposed persons.