GBBC Digital Finance

Code of Conduct

Part VIII: Principles for KYC / AML

These additional principles must be read in conjunction with the Overarching Principles and the GDF Taxonomy. For the avoidance of doubt, where the principles herein conflict with local legislation, the latter shall prevail.

1. Definitions and Scope

a. Money Laundering (ML) is the generic term used to describe the movement, conversion or any other use of the proceeds of criminal conduct.

b. Terrorist Financing (TF) is the process by which terrorists fund their operations in order to perform terrorist acts. While different from money laundering, terrorists often exploit similar weaknesses in the financial system[1].

c. These principles are intended to apply to firms conducting activities within the remit of the definition of a Virtual Asset Service Provider (VASP) as laid out in the Financial Action Task Force (FATF) Glossary[2].

2. Compliance with Existing Laws

a. We recognise that criminals may seek to use our facilities to access the financial system and / or to facilitate ML / TF activities. We are committed to preventing the use of our facilities for the laundering of money derived from criminal activities, and for the financing of terrorism.

b. We understand that each jurisdiction may have AML / CFT legislation that requires us to be licensed or registered before conducting activities with residents of that jurisdiction, and we will take reasonable steps to ensure that we either: do not conduct activities; or obtain the requisite licenses and authorisations before engaging in such activities.

c. Our AML / CFT response to legislative requirements will be commensurate with the nature, volume and complexity of our firm's business dealings.

3. Governance

a. Our shareholders, board, executive management, and senior leadership are committed to ensuring:

   i. A 'tone-from-the-top' on the importance of AML / CFT within the firm.

   ii. Effective implementation and oversight of the AML / CFT programme.

   iii. That the firm has sufficient resources to support its AML / CFT programme.

   iv. That all employees receive regular AML / CFT training.

   v. That potential AML / CFT issues receive the appropriate prioritisation within the firm.

b. We will designate a named individual as the firm's Compliance Officer (or an equivalent title in line with local requirements), with responsibility for oversight of our AML / CFT obligations. Our firm's Compliance Officer will:

   i. Possess the necessary competence and knowledge to lead the firm's AML / CFT programme.

   ii. Have sufficient independence and authority to carry out their responsibilities, including direct access to the relevant regulators and financial intelligence units.

   iii. Have sufficient seniority within the firm to undertake their responsibilities effectively, including being part of senior management or reporting directly to senior management.

   iv. Control or be able to draw upon the necessary resources (including staff and budget) to ensure that the firm's AML / CFT obligations are met.

   v. Be responsible for filing Suspicious Activity / Transaction Reports or other equivalent reports to the relevant regulators and financial intelligence units.

c. We will develop, implement and maintain an effective written AML / CFT policy that is reasonably designed to prevent our business from being used for ML and / or TF. This policy is to be approved by the board of directors and senior management of the business. We will aim to ensure that our policy will:

   i. Apply to all jurisdictions in which we operate.

   ii. Apply to all entities within our firm's group, including majority owned subsidiaries.

1 https://www.acams.org/aml-resources/combatting-terrorist-financing/

2 https://www.fatf-gafi.org/glossary/u-z/

d. We will ensure that our AML / CFT programme is subject to regular testing and independent review, and is updated when necessary.

4. Training

a. We will ensure all employees receive regular and appropriate AML training suitable to their roles:

   i. Our training programme will be risk-based to ensure staff with the most exposure to ML / TF risks, as well as those with specific AML / CFT compliance duties, receive comprehensive training on understanding and detecting such ML / TF risks.

   ii. We will provide regular briefings to staff on new and emerging ML / TF risks, and the red flags that may assist in identifying them.

5. Risk-Based Approach

a. We will take steps to identify, assess and take effective action to mitigate ML / TF risks that apply to our firm.

b. We will assess our ML / TF risks taking into account jurisdiction, client profile, products / services, and distribution channel risks.

c. We will maintain a written assessment of ML / TF risks identified, together with mitigations and overall residual risk. This assessment will be kept up-to-date.

d. We will apply a risk-based approach within our business towards our AML / CFT obligations.

6. Due Diligence

a. We will conduct Customer Due Diligence (CDD) using a risk-based approach before establishing business relationships with our customers.

b. Where CDD cannot be completed on a customer, we will not establish a business relationship and will consider filing a Suspicious Activity / Transaction Reports where there is a suspicion of ML / TF.

c. We will take appropriate steps to ensure the reliability and authenticity of the documents, data and / or information obtained for the purpose of verifying a customer's identity.

d. We will take appropriate steps to identify the natural person who ultimately owns or controls a customer (the "beneficial owner").

e. We will take appropriate measures to identify customers subject to economic sanctions, or who may be politically exposed persons (PEP), or those who pose a higher risk of ML / TF.

f. We will apply a risk-based approach to PEPs, and will apply an Enhanced Due Diligence (EDD) procedure as required by local legislation.

g. Where a customer is identified as high risk, we will conduct EDD.

h. Following a risk-based approach, we will take appropriate steps to identify our customers' source of funds as having not derived from ML / TF, whether fiat or virtual assets.

i. Where our business model involves virtual asset transfers, and where required to do so by local legislation, we will obtain and hold required and accurate originator information and required beneficiary information and submit the information to beneficiary institution, if any.

j. If we are a beneficiary institution to a virtual asset transfer, and where required to do so by local legislation, we will obtain and hold required originator information and required and accurate beneficiary information.

k. We will take appropriate measures to ensure that we do not onboard or transact with any party where to do so would be in breach of sanctions imposed by the United Nations or any jurisdiction with whom our firm has a nexus.

7. Ongoing Monitoring

a. We will take appropriate measures, using a risk-based approach, to periodically review our customers and identify those subject to economic sanctions, who may be PEPs, or those who pose a higher risk of ML / TF.

b. Our periodic reviews will be both on a regular cycle as well as where a clearly defined event takes place that may result in a change of the information we hold about a customer.

c. We will conduct transaction monitoring on all transactions, whether fiat or virtual asset, to detect unusual behaviour that may be indicative of money laundering or terrorist financing, or that may violate economic sanctions measures.

d. We will periodically test the effectiveness and accuracy of our AML / CFT controls as well as our compliance technology.

8. Suspicious Activity Reporting

a. We will investigate and promptly report suspicious activities and / or transactions in accordance with relevant legislation in the jurisdictions in which we operate.

b. We will ensure we are familiar with the processes of law enforcement requests in the jurisdictions in which we operate, and will have processes in place to respond appropriately where required to do so.

9. New Technologies

a. We understand that new technologies may increase the efficiency and efficacy of AML / CFT risk management and governance, but that such technologies can also introduce new risks. Such technologies might include Artificial Intelligence, Self-Sovereign Identity, etc.

b. Before introducing new technology, we will assess what impact it may have on the ML / TF risks our firm faces, and take appropriate steps to ensure the continued effectiveness of our AML / CFT programme.

c. Where new technology has been introduced into our AML / CFT programme, we will periodically review it for accuracy, effectiveness, and compliance with legal and regulatory requirements.

10. Reliance on Outsourcing

a. We understand that while the operational aspects of AML / CFT can be outsourced, the ultimate responsibility for compliance remains with our firm.

b. We will conduct risk-based due diligence on any third-party vendor, and their data, software, or service to satisfy ourselves that our AML / CFT risk management is not compromised.

c. We will ensure adequate testing is periodically performed on any third-party data, software, or service to satisfy ourselves that our AML / CFT risk management is not compromised.

d. We will risk-assess third-party vendors that we work with, and where applicable require appropriate controls in higher risk situations such as, but not limited to, code escrow, regular penetration test reports, and / or SOC2 reports.

e. We will ensure that any third-party vendors are subject to appropriate contractual arrangements to protect the firm.

11. Record Keeping

a. We will process and maintain all AML / CFT records securely as required of us by AML and data privacy laws within the jurisdictions in which we operate. This may include, but is not limited to: risk assessment records, client due diligence information, transaction monitoring records, suspicious activity / transaction reports (internal and external), and training records.

b. Records will also be kept for off-boarded clients including the date and reasons for off-boarding.