Anti - Money Laundering Policy

Tayo Rolls Limited

March 14, 2016

ANTI - MONEY LAUNDERING POLICY OF TAYO ROLLS LIMITED

I. POLICY STATEMENT AND PURPOSE

1. As a Tata company, we are committed to complying fully with all applicable Anti-Money Laundering ("**AML**") laws in the conduct of our businesses. Section D Clause 21 of the Tata Code of Conduct 2015 **("TCoC 2015")** states "*We shall comply with all applicable anti-money laundering, anti-fraud and anti-corruption laws and we shall establish processes to check for and prevent any breaches of such laws*". Towards this objective, we must conduct business only with reputable customers who are involved in legitimate business activities and whose funds are derived from legitimate sources. Appropriate measures must be set up to ensure that we do not, even inadvertently, accept forms of payment that are known or suspected to be means of laundering money. One such measure is in implementing risk-based "Know-Your-Customer" **("KYC")** due diligence procedures calibrated to the risk in question, as well as systemic 'Red Flags' to detect unacceptable or suspicious forms of payment. Our employees acknowledge that failing to detect customer relationships and transactions that place our Company or the TATA brand at risk, could cause irreparable harm to our reputation, leading to significant financial loss and severe penalties under applicable law.

2. The purpose of this Anti-Money Laundering Policy **("AML Policy")** is to prevent any involvement by our Company in money laundering activity even where the involvement may be unintentional. It requires our directors, officers, other employees and those who work with us to recognize questionable financial transactions, and to take steps to conduct appropriate additional due diligence. If any 'Red Flag', whether or not listed in this AML Policy is triggered, the **Designated Persons** *(as defined below)* need to promptly contact our Company's **Compliance Officer** *(as defined below)* to facilitate any further due diligence or action that may be needed. If any such 'Red Flags' are received by the Company Ethics Counsellor **("CEC"),** the CEC would promptly forward these to the Compliance Officer. Our Company is also committed to cooperate with law enforcement and regulatory agencies enforcing anti-money laundering laws and regulations.

3. This AML Policy constitutes a minimum standard. It must be complied with in any country in which our Company does business even when the policy is stricter than the anti-money laundering laws that are applicable in that country, including both applicable local laws and those laws with extra-territorial application. However, when applicable anti-money laundering laws are stricter than this policy, such laws must be complied with. In case of any doubts, Designated Persons must contact our Company's Compliance Officer.

4. The guidelines in this AML Policy supplement the Tata Code of Conduct 2015 **("TCoC 2015")** and should be read in conjunction with:

a) TCoC 2015;
b) The Whistleblower Policy;
c) The Anti-Bribery and Anti-Corruption Policy;
d) Any guidance published pursuant to this policy;
e) Any other relevant policies as may be implemented from time to time.

5. Because no code of conduct or policy can cover every possible situation, our Company relies on the Designated Persons to use good judgment and to speak up when they have either questions or concerns.

II. SCOPE AND APPLICABILITY

This AML Policy is applicable to our Company and to all individuals working at all levels and grades, including directors, senior managers, officers, other employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, interns, seconded staff, casual workers and agency staff, agents, or any other person associated with our Company and such other persons including those designated by the Compliance Officer from time to time (all of the aforesaid being collectively referred to as **"Designated Persons"**).

III. COMPLIANCE OFFICER AND DESIGNATED DIRECTOR

1. Our Company shall, from time to time, designate an employee of sufficient seniority, competence and independence as the Compliance Officer to ensure compliance with the provisions of this AML Policy ("**Compliance Officer**") and the same shall be notified to the Designated Persons. Mr Suresh Padmanabhan – Deputy Chief Financial Officer has been designated as the Compliance Officer of the Company. All reports, complaints, doubts or concerns in relation to this AML Policy shall be raised by the Designated Persons to the Compliance Officer.

2. All queries, concerns or complaints received by the CEC dealing with a money laundering issue should be reported to the Compliance Officer by the CEC. Any action required to be undertaken under this AML Policy shall be taken by the Compliance Officer in accordance with this AML Policy. The Compliance Officer shall have a functional reporting to the Designated Director (Dr S.K. Bhattacharyya – Chairman, Audit Committee) and shall submit quarterly compliance reports to the

Designated Director. Aggravated cases of breach of this AML Policy shall be escalated to the Board of Directors of our Company ("**Board**") through the Designated Director.

IV. GUIDANCE ON MONEY LAUNDERING

1. The phrase "money laundering" is generally understood to mean any act or attempted act to conceal or disguise the true origin and ownership of illegally obtained proceeds so that they appear to have originated from legitimate sources thereby avoiding prosecution, conviction and confiscation of the illegal proceeds. Money laundering can be used by terrorist organizations, tax evaders, smugglers, by those engaged in bribery, or anyone who receives money for illegal activities or through illegal means. Countering money laundering is of critical importance as it ensures that illegal funds do not remain hidden and do not get integrated into legal business and consequently into the legal economy.

2. The Government of India has enacted the Prevention of Money Laundering Act, 2002 and issued rules and regulations thereunder ("**PMLA**") for preventing money laundering and countering the financing of terrorism in India, with effect from July 1, 2005. The PMLA defines the offence of money laundering as "*Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering*."

The term 'proceeds of crime' has been defined under Section 2(u) of the PMLA as "*any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property.*" The definition of 'proceeds of crime' also implies that assets can be tainted by conversion. Therefore, if the 'proceeds of crime' are utilized to purchase another asset, by conversion, that asset could also be considered to be a 'proceed of crime' replacing the tainted money.

Under the provisions of the PMLA, proceeds of crime can be attached in the possession of any person, whether or not such person was involved in the offence of money laundering.

3. Money laundering usually consists of 3 (three) steps:

a. Placement: This is the initial stage and during this stage, the money generated from illegal/criminal activity such as sale of drugs, illegal firearms, etc. is disposed of. Funds are deposited into financial institutions or converted into negotiable instruments such as money orders or traveller's cheques. For example, cash received by a drug smuggler can be taken to a bank and changed into a money order or traveller's cheque.

b. Layering: In this stage, funds are moved into other accounts in an effort to hide their origin and separate illegally obtained assets or funds from their original source. This is achieved by creating layers of transactions, by moving the illicit funds between accounts, between businesses, and by buying and selling assets on a local and international basis until the original source of the money is virtually untraceable. Thus, a trail of unusually complex transactions is created to disguise the original source of funds and thereby make it appear legitimate. For example, money can be moved into and out of various offshore bank accounts through electronic funds transfers.

c. Integration: Once the illegitimate money is successfully integrated into the financial system, these illicit funds are reintroduced into the economy and financial system and often used to purchase legitimate assets, fund legitimate businesses, or conduct other criminal activity. The transactions are made in such a manner so as to appear as being made out of legitimate funds.

4. Money laundering is a global problem, and many countries, and organizations have enacted laws to combat it. Compliance with AML and anti-terrorism laws and regulations requires an awareness of possible 'Red Flags' or suspicious activities, which may arise in the course of conducting business. When 'Red Flags' are identified, an appropriate level of additional due diligence must be performed and additional approvals should be obtained.

V. POTENTIAL RED FLAGS

1. While an exhaustive list cannot be provided, set out below are indicative actions or situations or parties that Designated Persons should be careful about - which when appearing together or individually should raise 'Red flag' concerns (each, whether or not listed herein, a "Red Flag"):

a. Customers or suppliers who are connected to countries identified as non-cooperative by the 'Financial Action Task Force on Money Laundering' established by the G-7 Summit in 1987, and international organisations against money laundering;

b. Customers or suppliers who are reluctant to provide complete information and/or provide insufficient, false, or suspicious information or who are unwilling to comply with our Company's KYC norms as may be in force from time to time;

c. Customers or suppliers who appear to be acting as an agent for another company or individual, but decline or are reluctant to provide information regarding that company or individual;

d. Customers or suppliers who express concern about, or want to avoid, reporting or record-keeping requirements;

e. Payments of amounts in excess of 20,000/- (Rupees Twenty thousand only) made in cash or cash equivalents, such as money orders, traveller's cheques, internet currencies or prepaid cash cards. Acceptance of such amounts of cash or cash equivalents as a form of payment by our Company is strongly discouraged. Cash payments are commonly used by money launderers, and leave very little in the way of audit trails. Alternative methods of payment which provide a stronger audit trail should be offered. Particular care should be taken with regard to customers and suppliers who structure these payments to avoid the relevant government reporting requirements for cash and cash equivalent payments (for example by making multiple smaller payments or payments from multiple sources);

f. The purchase of products, or a larger volume purchase, that appears to be inconsistent with a customer's normal ordering pattern, and in the absence of any legitimate business reason such as a special price promotion;

g. Complex deal structures or payment patterns that reflect no real business purpose or economic sense;

h. Requests for payment to be made through an unrelated country or to an unrelated third party;

i. Multiple partial payments from various parties on behalf of a single customer and/or multiple partial payments from various locations. Also included are "double endorsed" or "third party"

cheques, where a customer endorses over to a company as payment for their invoice a cheque that was originally made out to the customer;

j. Customers or suppliers whose address is not a physical site;

k. Customers making a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose;

l. Customers paying in one form of payment and then requesting a refund of the payment in another form e.g. paying by credit card and requesting a wire transfer or cash refund.

VI. COMPLIANCE STEPS:

Each Designated Person is required to ensure that he/she undertakes the following steps in the course of the business operations of our Company:

1. Know your business partners: Where appropriate, Designated Persons should conduct integrity assessments and other due diligence exercises and be familiar with business practices of customers and suppliers.

2. Monitor financial activity: Designated Persons are required to observe and record payments and transactions consistent with all established policies and procedures and follow global financial standards for acceptable forms of payment.

3. Keep complete records: Designated Persons should always keep current, complete and accurate records of every business transaction.

4. Report any suspicious activity: Each Designated Person has an obligation under this AML Policy to immediately and, without delay, report to the Compliance Officer any **Suspicious Transaction** *(as defined below)* or suspicious activity or 'Red Flag' concern **("Report")**. Each Designated Person shall be aware of and follow country legal requirements for the reporting of cash transactions.

A "**Suspicious Transaction**" includes an attempted transaction, whether or not made in cash, which to a person acting in good faith:

a. gives rise to a reasonable ground of suspicion that it may involve the proceeds of an offence specified in the schedule to the PMLA, regardless of the value involved; or

b. appears to be made in circumstances of unusual or unjustified complexity; or

c. appears to have no economic rationale or bona-fide purpose; or

d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism or other forms of criminal activity.

5. Reporting/action by the Compliance Officer: When setting up internal procedures, the Compliance Officer may adopt a 'risk-based approach' to KYC and AML compliances. Consequently, there will be circumstances when it will be both necessary and permissible to apply commercial judgment to a Report received by the Compliance Officer. Based on the facts and circumstances of an incident covered in a Report, the Compliance Officer shall take one or more steps, such as (a) probe into the incident himself/herself, (b) set up an internal enquiry into the incident, (c) in case of Aggravated Cases determine and recommend whether a reporting of the incident should be made to the appropriate authority. (Aggravated Cases shall mean incidents of AML that need to be reported to relevant regulatory or enforcement authorities, for example the Financial Intelligence Unit, India. All Aggravated Cases must be escalated, without delay, by the Designated Director to the Board).

6. Cooperate fully for enforcing anti-money laundering laws: The Compliance Officer shall be the Company's point of contact for coordinating with all law enforcement and regulatory agencies for all compliance reporting and investigations. Designated Persons shall render full support to the Compliance Officer as well as cooperate fully with any internal investigation team set up by the Compliance Officer or the Designated Director or the Board, or with any external investigation.

7. Maintenance of records: Records confirming the identity of customers, suppliers, contractors, investors and other persons should be retained for such number of years as prescribed in the Document Retention and Archival policy of our Company.

VII. VIOLATIONS:

Violations under this AML Policy include the following actions by Designated Persons:

1. Any violation of the compliance steps under this AML Policy by a Designated Person;

2. On-boarding a customer, supplier, contractor, agent, or investor in contravention of the KYC policy;

3. Requesting others to violate the AML Policy;

4. Failure to promptly raise a known or suspected violation of the AML Policy or notify a potential 'Red Flag' or Suspicious Transaction;

5. Failure to cooperate in investigations of possible AML Policy violations;

6. Retaliation against another employee for reporting a concern under the AML Policy;

7. Failure to demonstrate leadership, initiative, and diligence to ensure compliance with the AML Policy, PMLA and other applicable laws;

8. Involvement in any form of money laundering activities, whether in the course of employment with our Company or otherwise.

VIII. CONSEQUENCES OF VIOLATION OF THIS AML POLICY BY DESIGNATED PERSONS

In case of violations of the AML Policy, the Compliance Officer shall, after considering inputs, if any, from the Designated Director, have the discretion to do the following:

1. Corrective Action: If necessary, corrective actions shall be prescribed by the Compliance Officer to appropriate managers, officers, or other employees for implementation.

2. Penalties: The Compliance Officer shall, based on the investigation reports (if any) have the discretion to recommend appropriate disciplinary action, including suspension and termination of service, against such a defaulting Designated Person. Depending on the nature and scale of default of the AML Policy by the defaulting Designated Person, the Compliance Officer may also recommend to the Board to commence civil and/or criminal proceedings against such a Designated Person in order to enforce remedies available to our Company under applicable laws.

******