Anti-Money Laundering and Sanctions Compliance

Adopted Date: May 25, 2021
Geographical Scope: Global
Issued by: Nathan Cook
Published Date: May 25, 2021

Policy Statement

It is illegal under the laws of the various countries in which Tensator Holdings Limited and its subsidiaries ("**Tensator**") do business to knowingly engage in financial transactions involving the proceeds of certain criminal activities or that violate applicable sanctions laws. This policy is designed to assist our employees in understanding which behaviors to avoid and to understand their responsibilities in complying with this policy.

Tensator will not knowingly engage in financial transactions that involve proceeds from unlawful activity or that support terrorist activities (commonly referred to as "money laundering" or "terrorist financing," respectively, and described below in the *Additional Information* section).

Tensator and its employees will not engage in financial transactions or do business with individuals, groups, entities and sanctioned countries designated by the European Union (EU), the United Kingdom's (UK) HM Treasury, the U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) or similar sanctions or regulations in other countries where Tensator conducts business. For more information on OFAC, see the Anti-Money Laundering and Sanctions Compliance Standards.

Tensator and its employees conduct business in accordance with the Anti-Money Laundering and Sanctions Compliance Standards.

Additional Information

Descriptions of Money Laundering and Terrorist Financing

In general, money laundering or terrorist financing may involve one or more of the following activities:

- knowingly dealing with proceeds from criminal activity;
- knowingly dealing in funds to support or facilitate criminal or terrorist activities;
- being involved in any activity designed to hide the nature, location, source, ownership or control of proceeds of criminal activity; and/or
- advising a customer on how to structure a transaction to avoid reporting and recordkeeping requirements.

Anti-Money Laundering and Sanctions Compliance Standards

Anti-Money Laundering

Tensator management will take the necessary steps to prevent, detect and report suspicious activity, as defined by applicable money laundering regulation. To meet this obligation, the business will document,

implement and maintain processes for:

- Customer Due Diligence
- Transaction Monitoring
- Investigation and Reporting of Suspicious Activity
- Information Sharing
- Training
- Recordkeeping

Sanctions

Tensator will maintain screening processes in place to screen, where applicable, the following applicable parties with whom it does business against the required sanctions lists:

- Consultants
- Counterparties
- Customers
- Employees
- Vendors
- Other parties relevant to a business engagement or where there is a regulatory requirement

Tensator will implement accurate and updated initial and ongoing sanctions screening processes to prevent and detect potential sanctions violations

Any prospective transaction or new or existing business relationship that appears to involve an EU, UK or US sanctioned country must be immediately escalated to business compliance for review.

Responsibilities

The financial controllers in each business within Tensator are responsible for:

- establishing, operating and supervisory procedures regarding transactions involving cash, currency and other financial instruments that comply with this policy
- requiring and verifying that their employees are trained as required by laws and regulations;
- requiring prompt notification to the Group Finance Director (who is the AML Officer) of any questionable transactions for guidance or corrective action; and
- implementing appropriate monitoring policies and procedures to comply with anti-money laundering and sanctions regulation regimes and for the United States, the OFAC monitoring procedures.

The AML Officer is responsible for:

- establishing and implementing an anti-money laundering and sanctions policy and program that meets applicable local regulatory requirements;
- overseeing that the anti-money laundering and sanctions programs are performed in accordance with local laws and regulations; and
- delegating duties and processes, as needed, to the business.

Employees play an important role in detecting and preventing money laundering activity as part of their daily work. Anyone who suspects that a customer, potential customer or financial transaction may involve suspicious activity, money laundering or terrorist financing, must notify his/her supervisor, who must contact the AML Officer or designated control function immediately.

An important factor in detecting suspicious or money laundering activity is how well employees know their customers. It is through knowledge of their customers that employees may detect potentially improper financial activity. Employees, particularly sales branch/field office personnel, must make every reasonable effort to determine and verify the identity of customers, and to maintain well-documented and current information throughout the relationship, as required by applicable law. Employees should refer to their business group's compliance, new account and/or anti-money laundering procedures for information relating to their group's "know your customer" and "customer identification" requirements and procedures.

Training

Using a risk-based approach, Tensator will make sure that periodic AML and sanctions business-level training, as required by local regulation, is provided, which is tailored to the business and customized to the business unit’s risks.

Recordkeeping

Tensator will maintain and retain adequate customer records, transaction information, records of AML and sanctions investigations, and post-investigation activities in compliance with relevant regulatory requirements, policies, and standards, including applicable record management and retention policies and procedures.

For any questions about this policy please email the Group Finance Director or local Financial Controller. This copy of the policy is for immediate reference; for the most current policy, please see the online version.