

TRAXION

Anti-Money Laundering and Know Your Client Policy Statement

Traxion acknowledges that a decentralized payment system in which payments are processed, validated and secured by distributed ledger technology poses potential risk of illegal use. Indeed, all financial systems are susceptible to criminal abuse. However, Traxion believes that the legitimate uses of blockchain networks far outweigh these risks. To fully enjoy the advantages of blockchain and leverage the efficiencies brought by the technology, Traxion has outlined this policy statement on Anti-Money Laundering (AML), Know Your Client (KYC), Combatting Terrorist Financing (CTF) as well as sanctions monitoring.

By enforcing a strict policy on AML, KYC, CTF and sanctions monitoring, Traxion will be able to assess and manage the peculiar risks associated with cryptocurrencies, enabling the project to focus on building a robust platform and delivering innovative financial services. Traxion have established control mechanisms to manage AML and CTF risks, which are consistent with local laws and regulations as well as international standards set forth by the Financial Action Task Force (FATF).

Traxion is fully committed to comply with the relevant laws and regulations to prevent money laundering and terrorist financing, identify and verify the users of the Traxion Platform as well as the participants in Traxion's Initial Coin Offering (ICO). Traxion uses special analytics software to monitor, detect and prevent the use of the platform for money laundering or terrorist financing. Traxion respects and protects the privacy of its users and ICO participants, yet it will not allow the platform or its ICO be used to launder money, or to commit terrorist financing, fraud, financial crimes or any other illegal or nefarious activity.

As guide to implement this policy statement, Traxion maintains an internal AML KYC Framework. The AML KYC Framework is fundamentally designed to prevent criminal abuse by adhering to international standards set forth by the FATF including the need to have adequate systems and controls in place that would mitigate the risk of being used in facilitating financial crimes. The AML KYC Framework is founded on the best practices for KYC in Mobile Payments and Internet-based Payments Services according to the FATF Guidance on Risk-Based Approach (RBA) issued in 2013 as well as the FATF Guidance on RBA for Virtual Currencies issued in 2015. The AML KYC Framework will be updated periodically to take in consideration the latest typologies report and other relevant guidance notes published by the FATF.

As a basic principle of its KYC policy, Traxion strictly requires identity information received from users and ICO participants to be corroborated by official documents such as passport or other government IDs, and to be verified by online searches for adverse media, along with the use of other verification tools and techniques.

Regarding its sanctions policy, Traxion strictly prohibits individuals, companies and countries that are named on prescribed sanctions lists from using the Traxion platform or from participating in the ICO. In particular, Traxion will screen against US Office of Foreign Assets Control (OFAC), United Nations, European Union, and other sanctions lists in jurisdictions where the service is available. This critical policy is implemented through online searches and by using special screening software solutions that will track prospective users or ICO participants who are included in major and relevant sanctions lists.