Anti-Money Laundering and Counter-Terrorism Financing Policy

November 2020

1. Introduction

KONVI TECHNOLOGIES LIMITED is committed to the highest standards of Anti-Money Laundering (AML) and Anti-Financial Crime (AFC) including Anti-Bribery and Corruption (ABC), Counter Terrorism Financing (CTF), Anti-Fraud and other punishable criminal acts. The members of the Management Board and all employees are required to adhere to these standards to protect KONVI TECHNOLOGIES LIMITED and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes. The Republic of Ireland is a member country of the Financial Action Task Force (FATF) and the European Union (EU) and has enacted laws and rules designed to implement the anti-money laundering policies of both FATF and the EU. The goal of these laws is to detect and prevent money laundering and potential terrorist financing. KONVI TECHNOLOGIES LIMITED will adhere to all applicable laws and regulations in all countries where it conducts business, or has business relationships to. KONVI TECHNOLOGIES LIMITED will examine its AML and AFC strategies, goals and objectives on an ongoing basis and maintain an effective program for its business that reflects best practices. KONVI TECHNOLOGIES LIMITED addresses all AML-related topics, especially Know Your Customer (KYC) and Anti-Fraud. For all these topics KONVI TECHNOLOGIES LIMITED has implemented clear rules which must be complied with by all KONVI TECHNOLOGIES LIMITED appointed staff.

2. Governance Framework

The Compliance Department reports directly to the responsible member of the Management Board. It is responsible for adherence to applicable AML and Financial Crime regulations and obligations derived from the EU Anti-Money Laundering Directive. In addition, the Compliance Department is responsible for establishing and maintaining KONVI TECHNOLOGIES LIMITED's AML program to identify, assess, monitor and manage risks related to Money Laundering, terrorist financing and Financial Crime.

3. Money Laundering and Terrorist Financing

Money laundering involves disguising financial assets so they can be used without detection of the illegal activity that produced them. Through money laundering, the criminal transforms the monetary proceeds derived from criminal activity into funds with an apparent legal source. Money laundering is generally viewed as a three-stage process: placement, layering and integration.

- Placement: The physical movement of funds from illegal activity to a place less suspicious to law enforcement, and more convenient to the criminal, such as financial institutions or the retail economy. For example, placement can occur through breaking up large amounts of cash into less conspicuous smaller sums deposited directly into a bank account or prepaid card, or by purchasing a series of monetary instruments or gift cards.

Placement will often involve the practice of structuring, which is the illegal practice of breaking up large sums of money into small in order to avoid reporting requirements.
- Layering: The he process of separating proceeds from their illegal origins by using multiple, complex financial transactions. In this stage, funds may be channeled through the purchase or sale of investment instruments, or by wire transfers through accounts at various institutions.
- Integration: At this stage, illegal proceeds re-enter the legitimate economy and are converted into apparently legitimate business earnings through normal financial or commercial operations. For example, a money launderer might invest in a business venture, real estate, or luxury assets.

While terrorist financing is generally accomplished using the same methods, the ideology behind terrorist financing is vastly different from money laundering. Instead of trying to convert criminal funds into apparent legitimate funds, terrorist financing can also involve legitimate businesses and individuals providing funding for terrorist organizations or activities based on ideological, political, or other reasons.

4. Prohibited Business Relationship

KONVI TECHNOLOGIES LIMITED must refuse to open an account/enter into a relationship or has to close an existing account/terminate a relationship, if the company cannot form a reasonable belief that it knows the true identity of the client and/or UBOs and/or the nature of business or formal requirements concerning the identification of the client and/or UBOs are not met.

In particular, the KONVI TECHNOLOGIES LIMITED will not

- Accept assets that are known or suspected to be the proceeds of criminal activity
- Enter into/maintain business relationships with individuals or entities known or suspected to be a terrorist or a criminal organisation or member of such or listed on sanction lists
- Enter into relationships with clients from Special Risk Countries or
- Enter into relationships with clients operating in prohibited industries:
    - Check Cashing
    - Child or Animal Pornography
    - Collection Agencies
    - Bestiality
    - Unlawful Pharmaceutical Sales
    - Drug Paraphernalia Sales or Manufacturing
    - Unlawful Gambling
    - Rape, Violence or Hate Crimes

5. Research and Filing of Suspicious Activity Reports (SARs)/Suspicious Transaction Reports (STRs)

Suspicious activities must be properly handled and escalated within KONVI TECHNOLOGY LIMITED. It is the responsibility of the AML compliance department to ensure FIU and Revenue are notified of such suspicious activities. Regular AML training ensures that staff are reminded of their duty to timely report any suspicious activity to a respective Compliance Manager.

6. Management and Controls of AML and AFC Risk

KONVI TECHNOLOGIES LIMITED has developed and implemented a comprehensive set of measures to identify, manage and control its AML risk. These measures are:

- Transactions Monitoring and Reporting
- Account Monitoring and Reporting
- A robust “Know Your Customer” (KYC) program for both, corporate and personal accounts
- A training and awareness program for KONVI TECHNOLOGIES LIMITED staff
- A sound “Political Exposed Persons” (PeP) and Sanctions screening process.

7. Record Retention

All data obtained according to client identification and AML security measures must be documented. Records must be kept for a minimum of 5 years, notwithstanding potentially longer retention periods under local civil or commercial law.