Glossary

AML: Stands for Anti Money Laundering, it is mainly used in the financial, legal and compliance sector to refer to the standard controls that companies and organizations must have in place to prevent, identify and report suspicious money laundering or money laundering behavior.

BPM: Business Process Management. BPM is a working methodology based on a management system that is responsible for controlling the modelling, visibility and management of the company's production processes.

BSA (Bank Secrecy Act): From 1970, it is one of the first laws to fight money laundering in the United States. The BSA requires businesses to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax, and regulatory matters.

Convention on Transnational Organized Crime: It was adopted by General Assembly resolution 55/25 of 15 November 2000, and it is the main international instrument in the fight against transnational organized crime

CTF (Countering the Financing of Terrorism): This term involves the use of funds that may be licit or illicit in origin and using these funds to support terrorist activity.

Customer Risk Rating Assessment: They are one of three primary tools used by financial institutions to detect money laundering. The models deployed by most institutions today are based on an assessment of risk factors such as the customer's occupation, salary, and the banking products used.

Digital Payment Token: It refers to any cryptographically secured digital representation of value that is used or intended to be used as a medium of exchange.

FATF (Financial Action Task Force): It is an intergovernmental institution created in 1989 by the then G8. The purpose of the FATF is to develop policies to help combat money laundering and terrorist financing.

Financial Intelligence Units (FIUs): Investigative units established by individual countries to centralize the gathering of suspicious activity reports related to criminal financial activity and sharing the results of the analysis with relevant government agencies.

KYB (Know Your Business): These strategies focus on establishing optimal relationships with other companies that may be customers or suppliers, to mitigate the risk of doing business with an untrustworthy entity or one that has been involved in a compromising situation in the past.

KYC (Know Your Customer): These procedures are established around a process of identification and verification of a customer's identity in which a series of controls and checks are applied to prevent business relationships with persons linked to terrorism, corruption or money laundering.

KYS (Know Your Supplier): This practice provides more insights and transparency on suppliers and related supply chain risks, in order to address topics such as supplier performance, business continuity, sustainability, fraud & bribery, security risk, money laundering, child labor, and other legal/organizational compliance requirements.

Lines of Defense Model: The three lines of defense represent an approach to providing structure around risk management and internal controls within an organization by defining roles and responsibilities in different areas and the relationship between those different areas.

Money Mule: A person who transfers or moves illegally acquired money on behalf of someone else.

Peep Screening: It is a process that aims to identify and conduct customer due diligence on any politically exposed person as part of a robust Anti-Money Laundering and Know Your Customer (AML/KYC) program.

PEP: Politically Exposed Person.

Sanction Screening Program: is a combination of policies, procedures and technologies that enable a financial institution to ensure that it does not provide any form of services to sanctioned parties, directly or indirectly.

Transaction Monitoring Program: It helps financial institutions automatically spot suspicious transactions, such as high-value cash deposits or unusual account activity.