AML Compliance Guide

Checklist for Anti-Money Laundering Compliance

SANCTION SCANNER

Anti-Money Laundering

Money laundering is the process and activities aimed at showing the values of the assets they obtained from the crime in a different way, in order to hide the crimes of the people or to bring a legal image to the crime income. Anti-Money Laundering (AML) also refers to a set of regulations and procedures implemented to prevent criminals from making illegal funds acquired.

There are global and local regulators around the world to prevent financial crime. Apart from global regulators, each country has different AML policies. Companies have to comply with these AML regulations. Money laundering is a big crime, so companies have to comply with regulations, otherwise they are subject to criminal sanctions imposed by regulators.

Global comprehensive AML regulations are implemented by the Financial Action Task Force (FATF). The establishment purpose of FATF is to establish international standards for the prevention of money laundering and FATF has 39 member countries. Some of the AML procedures implemented worldwide are Know Your Customers (KYC), Customer Due Diligence (CDD).

AML Screening and Monitoring

One of the basic requirements of the risk-based approach is AML Screening and Monitoring. In 2019, 58 AML fines were issued by regulators worldwide, and the total amount of the fines was $ 8.14 billion. Audits and penalties by regulators are expected to increase further. There are sanctions and PEP lists growing and changing every day in the world. Due to the dynamic nature of these lists, companies need to scan sanction, PEP and Adverse Media data with third-party software. In addition, implementing the "Customer Due Diligence (CDD)" and "Know Your Customer (KYC)" procedures are some of the most important components of AML / CFT regulations.

The Risk-Based Approach

The Risk-Based Approach is that organizations perform AML controls according to their risk perception and the risk level of their customers. The risk perception of each company and the risk level of each customer are different. Therefore, it will be insufficient for each firm to apply the same AML controls to every customer.

Therefore, there are 2 basic steps for organizations to take a Risk-Based Approach. The first is the Risk Assessment. The second is the implementation of control processes appropriate to risk levels.

Know Your Customer(KYC)

Know Your Customer (KYC) is a process in which information that can identify a customer is collected. Financial ınstitutions implement KYC procedures to reduce their risks and identify their customers, such as money laundering and financing terrorism. Know Your Customer procedures are implemented in new business relationships, untrusted customer documents, and money laundering suspicion. KYC procedures have a number of obligations.

These procedures are as follows; Identification of the customer's personal information, such as name, photograph, identity, address, customer activities are examined, checking customer profiles in progress, in the absence of a customer, it must be identify the useful property of the company. Also, companies have to learn about the overall purpose of business relationships.

Customer Due Diligence (CDD)

Customer Due Diligence is the control procedures that financial institutions that provide financial services apply to exist and new customers to identify and prevent risks. CDD plays an important role in eliminating risks related to money laundering, terrorist financing, fraud, corruption, arms trade, bribery, drug trafficking, and other illegal financial activities.

When opening a customer account according to legal requirements, a number of checks are required to follow the Know Your Customer procedures. One of the control methods implemented for risk assessment is sanction, PEP and adverse media screening.

Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) is an AML control process that requires us to examine higher levels of customer risks. Risky customers and transactions pose a greater risk for the financial sector and cannot be detected by CDD. On this percentage, companies apply EDD procedures. EDD is designed to perform high risk and large transactions. Politically Exposed Persons (PEP), their close partners, or family members should undergo a more comprehensive review process. Moreover, EDD procedures are used in collaboration with industries that have a higher risk of money laundering.

Politically Exposed Person (PEP)

A politically exposed person (PEP) is an individual with a high profile political role, or who has been entrusted with a prominent public function. Due to their position, they may be more options for bribery, corruption, or other money laundering offenses. Therefore, PEPs are defined as higher risk customers. According to the FATF, senior government officials, close family members of these individuals, senior executives of a state-owned business enterprise, are closely related to PEP, and officers of a large political party are high-risk.

Sanction Check

Sanctions are penalties for individuals or institutions that do not comply with laws or rules. Governments or global organizations usually make the sanction decision. Organizations must not violate sanction decisions. Sanctions checks are special searches that include a set of government sanction databases that identify people banned from certain activities or sectors.

Sanctions checks are often required for industries and government agencies, such as financial services. There are several reasons for sanctions. The main reasons are political and economic disputes.

Identity Verification (IDV)

Authentication is to check the accuracy of the information provided by customers. The process of identity verification is very important. The first step begins with the authentication of the user. After identity verification of the client, the business checks whether it poses a threat to them. In this way, companies can prevent money laundering, bribery, and terrorist financing. Since manual ıdentity verification is very dangerous today, financial institutions use electronic ıdentıty verification (e-IDV).

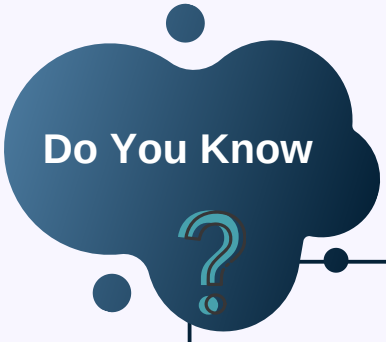
Ultimate Beneficial Owner (UBO)

Ultimate Beneficial Owner (UBO) means the legal entity of the company. Financial institutions have to control UBO to prevent serious crimes such as money laundering and terrorist financing. People who have at least 25% share in the capital of the legal entity, have at least 25% voting rights in the general assembly and are beneficiaries of at least 25% of the capital of the legal entity, acquire UBO status. FATF and the European Union have reported that UBOs have ML / TF risk, so financial institutions have important information and obligations regarding UBOs.

Adverse Media Screening

Adverse Media is any negative information about the customer or business from various sources. In the commercial world, these are usually news covering an individual or a company. Adverse Media reveals whether a person or organization is involved risks in money laundering and terrorist financing, organized crime, smuggling, and trafficking.

Adverse Media Screening Software, provided by Sanction Scanner, enables businesses to control their customers in adverse media data.



According to the 4th AML directive of the EU Risk Factors Directives, legal entities are required to make Adverse Media searches for high-risk customers. Likewise, FATF emphasized that Adverse Media controls should be made for high-risk customers to understand the reputation of customers.

AML Transaction Monitoring

Transaction Monitoring is one of the AML and anti-fraud security processes. AML Transaction Monitoring Software provides instant monitoring of financial institutions' customer transactions. Transaction Monitoring detects suspicious transactions, examines these transactions, generates reports on these transactions, and determines the risk level of customer transactions that carry out the transactions.

Sectors such as Money Services, Banks, Money Transfer Companies, Insurance Companies and Financial Services need AML Transaction Monitoring procedures.

AML Transaction Screening

Financial institutions mediate a large number of financial transactions throughout the day. One of the AML obligations of financial institutions is to control the receiver and the sender in money transfer transactions. To detect whether there are any suspicious transactions, sanctions, PEP, and adverse media scans are made to buyers and senders.

AML Transaction Screening Software controls the receiver and sender in the money transfer processes of financial institutions in the AML database. Financial institutions automatically perform all controls with the API and meet AML obligations without delay in customer transactions.

Suspicious Activity Report (SAR)

Suspicious Activity Report (SAR) is a tool used to track suspicious activities that will not be flagged normally in other reports under the Bank Secrecy Act (BSA). The overall purpose of SAR is to report illegal activities such as money laundering and terrorist financing, tax evasion, and other financial fraud. The report is usually sent to the country's financial crime enforcement agency to collect and analyze transactions and then report to the relevant law enforcement agencies.

Currency Transaction Report (CTR)

Currency Transaction Report (CTR) is a bank form used to help prevent money laundering. CTR is one of the financial industry's anti-money laundering (AML) responsibilities. Financial institutions use Currency Transaction Report (CTR) to report any bank transaction exceeding $10,000 to regulators. The Bank Secrecy Act (BSA) launched the use of this report in 1970. Any organization that uses state authority, for example federal, state-covered departments, or agencies are institutions exempt from the Currency Activity Report (CTR)

About Sanction Scanner

Sanction Scanner enables your business to comply with AML laws with AML Screening and Monitoring, AML Transaction Monitoring, AML Transaction Screening, and Adverse Media Screening. As Sanction Scanner, we are committed to the protection of all financial companies, large or small, from financial crimes.

Financial Institutions can easily integrate and use Sanction Scanner's global and real-time sanction, PEP, and adverse media screening tool. Thus, they can speed up your workflow by meeting all your compliance needs in one place. As a result, We aim to provide the best support and service to our customers

Contact Us

27 Old Gloucester Street, London, United Kingdom,
WC1N 3AX
+44 20 4577 0427

Yıldız Technical University - Yıldız Technopark
C1 - No:106-2, Istanbul, Turkey
+90 (212) 963 01 84

info@sanctionscanner.com