



**TradeSpot**

# Anti-Money Laundering Compliance Policy

---

Last Updated  
August, 2023

# 1. Introduction

In today's global marketplace, financial services companies operate in a tightly regulated environment where rules are strictly enforced. Anti-Money Laundering (AML), Know Your Customer (KYC), and Counter-Terrorist Financing (CTF) regulations play a crucial role in keeping terrorists, drug traffickers, and other bad actors from manipulating the global financial system to launder money.

Over the last few years, financial institutions and financial services companies have been closely monitored by regulatory authorities; the close scrutiny has turned up unsettling findings about crucial missteps and lapses in compliance programs, with authorities slapping big banks with billions of dollars in regulatory fines.

In the wake of these exorbitant fines, financial institutions have been forced to become ever more prudent about regulatory compliance. Indeed, meeting AML, KYC, and CTF obligations has never been more important. Compliance failures not only force organizations to contend with exacting costs and exorbitant fines, they inflict reputational damage on their brand and credibility, which is sometimes harder to shake off and recover from.

**Such is also true for Tradespot Financial Services LLC, where the core business is focused on linking third parties together to conduct trade. It is therefore of utmost importance to make sure that Tradespot Financial Services LLC adopts KYC and AML compliance policies that are in line with**

**eIDAS and AML5, effectively safeguarding the business and mitigating any possible compliance issues for itself and its customers.**

## 2. eIDAS & AML5

eIDAS and AML5 are the new regulations on trust services and anti-money laundering in Europe, aimed at the creation of the concept of Digital Single Market (DSM).

eIDAS can be seen as the regulation that allows citizens to have a European national ID document, with the advantages that it has when using it in a wide range of industries and across borders. eIDAS came into effect for 28 member states on July 1, 2016 although it was the later work of the European commission and the e-trust services industry which has set off major changes to make electronic services a standard security framework for work that facilitates use cases such as Tradespot Financial Services LLC's score business.

AML5 / 5AMLD (5th EU Anti-Money Laundering Directive) came into effect on July 9, 2018 and is the new European Union Directive to prevent money laundering and terrorist financing. It was published in the Official Journal of the European Union on June 19th, 2018. This new directive establishes a legal framework to tackle the collection of funds for terrorist purposes, by requiring European Union Member States to identify, understand and mitigate the risks associated with money laundering and the financing of terrorism.

In addition to expanding coverage to virtual (crypto) currencies and electronic transactions, AML5-related updates affect the way EU companies conduct KYC (Know Your Customer) and KYB (Know Your Business) research.

**The main change in comparison with the previous directives is the requirement for exchange companies or cryptocurrency companies to strengthen their mechanisms for online identity verification within customer onboarding processes.**

### 3. User enrollment

The user enrollment process should be as fast and smooth as possible so it won't break customer engagement. Still, performing due diligence on customers and businesses is a regulatory obligation that might be both complex and time consuming.

Tradespot Financial Services LLC users will be required to provide all the required documentation upon their application being accepted. Users will be differentiated between individual and corporate users. This is of special interest while selecting the type of verification required, because distinct types of users require different types of verification.

Users - both individual and corporate, will also be checked for PEP and sanctions status.

Individual accounts will be verified under KYC screening, while corporate accounts will be verified under the KYB screening. This accounts for distinct

information and due diligence that are required in order to effectively conduct compliance checks.

### 3.1 Enrollment flow

The enrollment process starts when a user submits an application through our business platform and consists of the following steps:

1. User submits application request;
2. TRADESPOT FINANCIAL SERVICES LLC receives the application request and pre-screens the application using reputation and interest for the platform as checking parameters;
3. If the application is deemed unsafe or of low interest to the platform community it gets declined;;
4. If the application is accepted, the user is requested to start the enrollment procedure (KYC if it's an individual or KYB if it's a corporation);
5. If there are red lines identified - ex: fraudulent information, PEP, sanctions, the user application will be declined;
6. If there are no issues identified, but there are issues with the information or documentation provided that are not critical - ex: legibility, additional information, the user will be asked to resubmit the required information.
7. If the user fails to provide such information or documentation, or if any other critical issues are found, the application will be declined;
8. Upon successful completion of KYC/KYB procedure, the user will be assigned a risk profile for due diligence purposes and requested to pay an enrollment fee in order to proceed with account activation;

9. Upon clearance of the enrollment fee, the user account will be fully activated and ready to login and start using TRADESPOT FINANCIAL SERVICES LLC finance platform.

**TRADESPOT FINANCIAL SERVICES LLC will always have the final word when it comes to enrolling a user, even if the KYC/KYB checks are successful. These checks and validations might be complemented by additional due diligence carried out by TRADESPOT FINANCIAL SERVICES LLC before a final decision is made.**

### 3.2 KYC information

This process is aimed at fully identifying private users (individuals) that are natural persons that present applications for enrolling in TRADESPOT FINANCIAL SERVICES LLC platform.

When an individual applicant submits a registration request, it will be asked to provide the following information by email:

- ID document (ID card or Passport);
- Residential address document (utility bill, bank statement);
- A verification video with his face fully visible while holding the submitted ID document, which should also be fully visible.

General document acceptance rules:

- Annexes which are copies of original documents must be submitted as certified copies issued by a public notary, a lawyer, a solicitor or by any other person legally authorized to do so;
- The documents or videos must be clear and legible and have the person's name on all documents. If this is not the case, processing time may be longer and may result in the enrollment process being put on hold, until the required documents are submitted by the applicant;
- Document scans should be submitted in JPG or PDF file formats only with a maximum size of 20MB per document;
- Documents that state applicants' residential address should not be addressed to a PO Box number and will be rendered invalid in such cases, since they're unacceptable for validation.

Any changes to the information provided by the applicant while enrolling shall be communicated to TRADESPOT FINANCIAL SERVICES LLC within 15 days of their occurrence through an email to [compliance@tradespotfinance.com](mailto:compliance@tradespotfinance.com) advising of such changes, together with the respective annexes and any documents necessary to evidence the changes occurred.

The information collected from the applicant consists of:

- Full name
- Date of birth
- Place of Birth
- Country of birth
- Identification document:
  - Nature (Government ID, Passport)

- Number
- Validity Date
- Issuing Entity
- Full residential address

### 3.3 KYB information

This process is aimed at fully identifying corporate users (companies, organizations, etc) that present applications for enrolling in the TRADESPOT FINANCIAL SERVICES LLC platform.

When a corporate applicant submits a registration request, the following data is collected and used in order to conduct a Dun & Bradstreet inquiry:

- Country of incorporation;
- Registration number;
- Tax number (if not available, the registration number will be used).

If no information is available from Dun & Bradstreet, the following information will be requested by email:

- Corporate Register Name
- Address
- Main Activity
- Corporate Registration number
- Tax Registration Nr
- Legal Entity identifier Nr



- Does the Company have a Politically Exposed Person (PEP) on its executive board or shareholders? If so please provide:
  - PEP relationship
  - Full name
  - Date of birth
  - Place of Birth
  - Nationality
  - Office that qualifies this person as a PEP
- Information about shareholders with more 5% or more of the capital and voting rights: ( Natural Person / Legal Person ):
  - Full name
  - Date of birth
  - Place of Birth
  - Identification document:
    - Nature (Government ID, Passport)
    - Number
    - Validity Date
    - Issuing Entity
    - Nationality identified in the document provided
  - Percentage of shares capital / voting rights
- Information about Senior Executives:
  - Full name
  - Date of birth
  - Place of Birth
  - Identification document: [Attached]
    - Nature (Government ID, Passport)
    - Number
    - Validity Date

- Issuing Entity
    - Nationality identified in the document provided
- Information about Ultimate Beneficial Owners:
  - Full name
  - Date of birth
  - Place of Birth
  - Identification document: [Attached]
    - Nature (Government ID, Passport)
    - Number
    - Validity Date
    - Issuing Entity
    - Nationality identified in the document provided
- Certified copy of memorandum and articles of association or equivalent documentation in incorporation jurisdiction;
- Certified copy of certificate of incorporation or equivalent documentation in incorporation jurisdiction;
- Certified copy from a solicitor qualified in the jurisdiction in which the company is registered confirming that:
  - The company is properly incorporated;
  - Incorporation name;
  - Registered address;
  - Office-holders and shareholders;
- In case of complex company structures - a company structure chart must be provided;
- Personal identification in respect of all beneficial owners or principal controllers. Beneficial owners or principal controllers are those individuals who have an interest in any entity in the corporate structure of 25% or more. Beneficial owners must be natural persons, if no person

has an interest of 25% or more in relevant entities then relevant identification documents must be provided for those persons with significant control of the relevant entities.

**A minutes of meeting authorizing account opening and performing business transactions under TRADESPOT FINANCIAL SERVICES LLC platform is mandatory in all cases.**

General document acceptance rules:

- Annexes which are copies of original documents must be submitted as certified copies issued by a public notary, a lawyer, a solicitor or by any other person legally authorized to do so;
- The documents must be clear and legible and have the person's name on all documents. If this is not the case, processing time may be longer and may result in the enrollment process being put on hold, until the required documents are submitted by the applicant;
- Document scans should be submitted in JPG or PDF file formats only with a maximum size of 20MB per document;
- Documents that state applicants' residential address should not be addressed to a PO Box number and will be rendered invalid in such cases, since they're unacceptable for validation.

Any changes to the information provided by the applicant while enrolling shall be communicated to TRADESPOT FINANCIAL SERVICES LLC within 15 days of their occurrence through an email to [compliance@tradespotfinance.com](mailto:compliance@tradespotfinance.com) advising of such changes, together with

the respective annexes and any documents necessary to evidence the changes occurred.

## 4. AML and CTF policy

TRADESPOT FINANCIAL SERVICES LLC is required by regulation authorities to put in place appropriate systems and controls to forestall money laundering and terrorist financing. This policy contains the procedures that we have developed in order to comply with these obligations.

### 4.1 Compliance Officer

The Money Laundering Regulations require that an organization has a nominated officer to ensure that is up-to-date knowledge of issues relating to Anti-Money Laundering and Counter-Terrorist Financing throughout the organization, and implements appropriate policies and procedures and receive reports of suspicious activity.

**The Nominated Officer (Money Laundering Reporting Officer) for TRADESPOT FINANCIAL SERVICES LLC is Carlos Santo**, with full responsibility for TRADESPOT FINANCIAL SERVICES LLC AML program.

Carlos has a working knowledge of AML and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Compliance Officer include:

- monitoring compliance with AML obligations;
- overseeing communication and training for employees.

The AML Compliance Officer will also ensure that the firm keeps and maintains all of the required AML records and will ensure that any suspicious activity is checked and reported to the competent authorities, when appropriate, as well as providing all information requested by any regulation authorities. The AML Compliance Officer is vested with full responsibility and authority to enforce Tradespot Financial Services LLC's AML program.

## 4.2 AML Related Inquiries Contacts

All AML related inquiries should be addressed to:

TRADESPOT FINANCIAL SERVICES LLC

C/O Carlos Santo

Euro House, Richmond Hill Road, Kingston

St. Vincent and The Grenadines

Email: [compliance@tradespotfinance.com](mailto:compliance@tradespotfinance.com)

## 4.3 Definitions and scope

### What is money laundering and terrorist financing?

**Money laundering** is the process through which proceeds of crime and their true origin and ownership are changed so that the proceeds appear legitimate.

**Money laundering** is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets.

Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Typically money laundering involves three stages:

Placement:

The process of placing criminal property into the financial system. This might be done by breaking up large sums of cash into smaller amounts or by using a series of financial instruments (such as cheques or money orders) which are deposited at different locations.

Layering:

The process of moving money that has been placed in the financial system in order to obscure its criminal origin. This is usually achieved through multiple complex transactions often involving complicated offshore company structures and trusts.

### Integration:

Once the origin of the money is disguised it ultimately must reappear in the financial system as legitimate funds. This process involves investing the money in legitimate businesses and other investments such as property purchases or setting up trusts.

**Terrorist financing** is providing or collecting funds, from legitimate or illegitimate sources, to be used to carry out an act of terrorism.

**Terrorist financing** may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Typical signs of **money laundering** and **terrorist financing** are:

- Obstructive or secretive clients
- Instructions outside our usual range of expertise, i.e. why is the client using us?
- Clients based a long way from us with no apparent reason for using us
- Cases or instructions that change unexpectedly or for no logical reason, especially where:
  - The client has deposited funds with us

- The source of funds changes at the last moment
- We're asked to return funds or send funds to a third party
- Loss-making transactions where the loss is avoidable
- Complex or unusually large transactions
- Transactions with no apparent logical, economic or legal purpose
- Large amounts of cash being used
- Money transfers where there is a variation between the account holder and signatory
- Payments to or from third parties where there is no logical connection to the client
- Movement of funds between accounts, institutions or jurisdictions without reason
- Retainers involving high risk jurisdictions (e.g. Iran, Uzbekistan, Turkmenistan, Pakistan, Sao Tome and Northern Cyprus)
- Large payment on account of fees with instructions terminated shortly after and the client requesting the funds are returned
- Crypto deposits and withdrawal requests from multiple wallets

## **Why is anti-money laundering and counter-terrorist financing important to Tradespot Financial Services LLC ?**

The anti-money laundering (AML) and counter-terrorist financing (CTF) regime is designed to prevent our services being used by criminals. We have obligations under the AML/CTF regime to spot and report money laundering and terrorist financing. Failure to meet these obligations can lead to criminal penalties, substantial fines and untold damage to Tradespot Financial Services LLC's reputation.



## **What is deemed as a suspicious activity?**

Any client activity outside the normal or expected activity should be considered unusual and must be investigated. Understanding the business or client profile is crucial. Unusual activity or transactions outside the established profile should be considered as a potential indicator of suspicious activity.

In case of any suspicion, Tradespot Financial Services LLC should request any relevant documentation from the customer in order to confirm or dismiss it. Investigations should establish the reasons for the unusual activity or transaction. The customer account should be immediately put on hold while the investigation is ongoing, without the possibility to carry out any transaction.

The purpose of the investigation is to either remove or confirm our suspicion. If it is confirmed, we should report it to the relevant authorities, while keeping the report strictly confidential and without notifying the client.

## **Source of funds**

Understanding our client's source of funds is an important step in the client due diligence process.

Although we're not required to interrogate all clients about their entire financial history, we're required to take additional steps to ensure that the transaction is consistent with our knowledge of the client. This is part of the ongoing monitoring exercise that we must conduct on all matters; see further *Ongoing monitoring* below.

We're specially required to establish the source of funds and source of wealth in every matter where we're acting for a Politically Exposed Person (PEP).

Scrutinizing the source of funds is more than asking for the money to come from a bank account in the client's name. Our focus should be on understanding how the client can legitimately fund the transaction.

Supporting evidence might include:

- bank statements
- filed business accounts
- information confirming the sale of a house or shares
- confirmation of inheritance or judicial award.
- cryptocurrencies mining or trade records

For transactions involving PEPs we should consider whether there:

- Are any warning signs of corruption
- Is there any evidence that government or state funds are being used inappropriately

Where a third party is providing funding to any client transaction we need to establish the source of funds. We must also document our investigations into the source of funds, including any questions asked, responses received and supporting evidence provided.

CDD on beneficial owners is different from CDD on clients. We must:

- Identify any beneficial owners, and then
- Validate their identity on a risk sensitive basis

## Ongoing monitoring

Ongoing monitoring is an intrinsic part of the CDD process. It must be performed on all matters, regardless of their individual risk rating, in order to detect unusual or suspicious transactions.

How should we conduct ongoing monitoring? We must:

- Scrutinize transactions undertaken (including, where necessary, the source of funds) to ensure that the transactions are consistent with our knowledge of the client, their business and risk profile
- Stay alert to changes in the client's risk profile and anything that gives rise to suspicion
- Keep documents, data and information used for CDD purposes up to date

## Policy compliance and review

Compliance will be continually monitored through any or all of the following methods:

- File audits
- Review of records maintained by the nominated officer
- Reports or feedback from staff
- Any other method deemed appropriate

We will review this policy at least annually as part of our overall risk management process. We will also review this policy if:

- There are any major changes in the law or practice
- We identify or are alerted to a weakness in the policy
- There are changes in the nature of our business, our clients or other changes which impact on this policy

## 5. General dispositions

Senior management of TRADESPOT FINANCIAL SERVICES LLC understands legal and reputational risks associated with the financial services provided by the company and is fully committed to support local and international efforts to prevent money laundering, terrorist financing, tax evasion and other illicit activities.

It is a crime to engage knowingly in a transaction that involves the proceeds of criminal activity – Money Laundering. It is a crime to use legally or illegally obtained funds to support terrorism – Financing terrorism.

Additional to regulatory risk, a key risk to Tradespot Financial Services LLC is reputational risk, which is the possible damage to the company and its employees reputation if they happen to engage in money laundering or terrorist financing scheme.

In order to operate in compliance with all applicable laws and regulations, TRADESPOT FINANCIAL SERVICES LLC sets internal policy and procedures

which are standard throughout the organization and ensure safety and regulatory compliance of our services.

This policy is implemented in all departments and controlled affiliates of the company.

All employees of the company should know and follow these policy requirements, learn the red flags, carefully observe and escalate when something does seem unusual or suspicious.

Our AML department goal is to build a strong AML culture based on education and risk based approach. Appointed Compliance Officer is to define risks, countermeasures, consult colleagues, establish monitoring systems, and communicate with authorities. While overseeing that employees receive initial and periodic training.

Management of the company is responsible to ensure that commitment to this policy is supported by sufficient authority and resources. Employees are aware of the consequences of non-compliance.

The main goal of the dispositions, concepts and rules, laid out in this Policy is to assure that:

- Each service of the company has its risk assessed and mitigation processes are designed, developed and implemented;
- The team responsible for addressing AML issues is trained to define the level of KYC or KYB required and perform the due diligence procedures;

- Systems for identifying risks, monitoring unusual activity, investigating, reporting suspicious activities are developed and running constantly;
- Initial and regular training materials are provided to employees of the company according to the level of responsibility;
- The compliance processes are undergoing regular external and internal audit;
- Each compliance process: identification, verification, training, red flags, screening matches, investigations, internal and external reporting are properly documented and records are kept for at least 5 years.