



peaksight

Anti-Money Laundering Policy

Version 0.1 – September 2025



By accepting this Anti-Money Laundering Policy, you acknowledge and confirm that our official legally binding language is English. In the event of any discrepancy or inconsistency between any documentation, information and communications in any other language other than English, the English documentation, information and communications shall prevail.

1. INTRODUCTION

Peaksight Ltd (hereinafter referred to as 'Peaksight' or the 'Company') is registered in Cyprus under the Companies Law, with registration number HE 433420. The Company's business address is located at 204, P. LORDOS CENTER, Block B, Corner Makarios Avenue 240 & Vyrinos 1 Street, 3105, Limassol. The Company is authorized and regulated by the Cyprus Securities and Exchange Commission (the "CySEC") as a Cyprus Investment Firm (CIF) to offer certain Investment and Ancillary Services and under the Investment Services and Activities and Regulated Markets Law of 2017 (L87(I)/2017) (the "Law"), which has transposed Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (the "MiFID II Directive") into national law, with CIF license number 440/23 .

Additionally, Peaksight Ltd carries out its activities in line with Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), Council Directive (EU) 2016/2258 of 6 December 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities, Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) and the Prevention and Suppression of Money Laundering and Terrorist Financing Laws of 2007-2018, Law No. 188(I)/2007.

Furthermore, Peaksight is operating in line with the FATF Recommendations. The "Financial Action Task Force" ("FATF") set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Starting with its own members, the FATF monitors countries' progress in implementing the FATF Recommendations; reviews money laundering and terrorist financing techniques and counter – measures; and promotes the adoption and implementation of the FATF Recommendations globally.



2. PEAKSIGHT AML POLICY

At Peaksight we are devoted in preventing money laundering activities and identifying suspicious transactions, therefore we have implemented the following measures in order to comply with our regulatory requirements:

- Identifying and verifying our client's identity, place of residence, and origin of funds to be credited to client's Trading Account.
- Identifying, monitoring and reporting any kind of suspicious transactions.
- Keeping documents and records for at least 5 years after the termination of the business relationships with our clients.
- Continuous training of our staff to recognize suspicious transactions, fulfill all reporting obligations and keep up to date with the AML regulatory requirement.
- Depending on client location, report any suspicious activities to authorities in several countries.

In addition to the abovementioned Peaksight:

- Collects, verifies and updates at least annually the personal identification information of all account holders.
- Tracks any suspicious transactions made by clients and any transactions executed under non-standard trading conditions.
- The general practice of the Company is not to accept any third-party deposits, although exceptions may apply, from time to time, under certain circumstances and subject to the agreement of the provision of further due diligence documents to be provided to the Company, in order to verify the source of funds and wealth of the third-party deposits. Matches each deposit to the account name held on file for that customer.
- Monitors funding from bank accounts held outside the account holder's home country.
- Reserves the right to refuse to process a transaction where it believes the transaction to be connected in any way to money laundering or criminal activity. In accordance with international law, Peaksight is under no obligation to inform the client when suspicious activity is reported to any corresponding regulatory or legal bodies.

! All Peaksight's client funds are held in separate, segregated accounts that are designated solely for client deposits and withdrawals.



3. ACCOUNT OPENING PROCEDURES - KNOW YOUR CUSTOMER POLICY ("KYC")

Account Opening Requirements

To open a trading account with Peaksight, the potential client must have a permanent residence in a country within the European Economic Area (EEA) and be **over 18 years old**. In addition, the steps listed below must be followed:

- complete the account opening application, which includes providing personal information (name, date of birth, etc.), information relating to his/her economic profile (annual income, estimated net worth, employment status, etc.).
- complete the appropriateness test.
- provide identification documents which consist of a valid form of government-issued identification and a proof of residence. (The Company reserves the right to request additional documentation as it thinks fit and based on the AML regulatory requirements).

! Please note that from the day of receipt of the account opening application a timeframe of 15 days is given to provide the required information and documentation. If the potential client fails to provide these within the timeframe, the Company will decline the application and in case of any deposits, will refund the available balance back to the method used to deposit the funds. The returned funds (deposits) include any profits the Client has gained during the fifteen days period and deducting any losses incurred.

In the event the Client has not provided the Company with the required verification documents, such as Proof of Identity and Proof of Residency within fifteen (15) days from the date of registration of his/her/their Trading Account(s) (i.e., the acceptance of the present Client Agreement), the Company reserves the right to perform an electronic identity verification (eIDV), using the personal information provided on the Client Questionnaire during the onboarding process. When Clients are verified by the performance of an Electronic Verification, they shall be informed accordingly through an email within a timely manner.

Identification Documents:

1. Proof of Identity

Following documents are accepted as a Proof of Identity:

- A valid Passport (for non-CY residents)
- A valid National Identity Card

The document must be issued on your name and all information on the document including your photo must be visible.

! Please keep in mind that you have the obligation to inform the Company once your Proof of Identity has been expired.

! All photo IDs are verified through a third-party compliance software.



The Company reserves the right to ask for certified true copies of the abovementioned documents.

2. Proof of Residence

Following documents are accepted as a Proof of Residence:

- A utility or phone bill
- A bank statement
- Governmental documents such as tax bill or residence certificate (stamped)

Please note that your proof of residence document must be recent (not older than 6 months), show your name, permanent address and date of issue.

! Please keep in mind that your Proof of Residence must be updated at least once per year.

The Company reserves the right to ask for certified true copies of the abovementioned documents.

Additionally, the company reserves the right to request additional documents from its clients whenever it deems necessary.

4. BANK ACCOUNT REQUIREMENTS

Peaksight account holders must have a valid bank or credit card account in their name, established within the EU. In case the Clients' bank account is established within a third country, the same or equivalent AML regulations and standards should govern the said financial institution. The bank/credit card statement must show their name and the same registered address as that shown on their application.

5. FUNDS WITHDRAWAL PROCEDURE

The withdrawal procedure at Peaksight detailed below follows strict principles to ensure that the funds are sent back to their originating source.

- a. Peaksight customers must complete a signed paper or digital withdrawal request containing *inter alia*, their correct account information.
- b. The withdrawal form must be submitted to the Peaksight Back Office department for processing. The Back Office department will do the following:
 - confirm the account balance;
 - confirm that the account is approved and the provided documents are up-to-date;
 - verify that there are no holds or withdrawal restrictions on the account;
 - verify that the original funds are being withdrawn through the same method of deposit and to the name of the account holder on file;



- examine the withdrawal request against the customer's deposit history to ensure there is no suspicious activity;
- verify the bank account details held on file;

c. If there is no mismatch or suspicious activity the Back Office Department will approve the withdrawal, and the funds are released to the client.

d. If the Back Office Department believes there was suspicious activity on the account, the Peaksight Anti-Money Laundering Compliance Officer (AMLCO) will be informed, in order to perform further investigation.

e. If the withdrawal will be flagged for suspicious activity by the Peaksight AMLCO, the withdrawal is placed on hold, and sent to the Company's Management.

f. Peaksight Management along with the Company's AMLCO will decide if further action is needed and which, if any, relevant regulatory bodies need to be contacted.

! Please note that your trading account must be verified in order for the withdrawal to be processed.

6. EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES

- Transactions without clear economic purpose or unnecessarily complex transactions. Use of foreign accounts of companies or groups of companies with complicated ownership structure which is not justified based on the needs and economic profile of the customer.
- Transactions or the size of transactions requested by the customer do not comply with his/her normal practice and business activities.
- Large volume of transactions and/or money deposited or credited into an account when the nature of the customer's business activities would not appear to justify such activity. When the business relationship of the customer consists of only one transaction or lasts for a short period of time.
- There is no visible justification for a customer using the services of the company. For example, a client whose address is located quite far from the company and in an area where he could be served by another Company.
- There are frequent transactions in the same financial instrument without obvious reason or under circumstances that appears unusual (Churning).
- There are frequent small purchases of a particular financial instrument by a customer who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the customer's instructions, in an account other than his usual account.
- Any transaction the nature, volume or frequency appears to be unusual. For example, the cancellation of an order, especially after the deposit of the consideration. Transactions which are inconsistent with normal market practice, in relation to the size of the order and the frequency.
- The settlement of any transaction, especially large transactions in cash.



- Settlement of the transaction by a third person which is different than the customer which gave the order.
- Instructions of payment to a third person which has no obvious link/connection with the instructor.
- Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on money laundering and terrorist financing.
- Customer is unwilling to provide complete information when establishes a business relationship regarding the nature and purpose of its business, anticipated account activity, prior banking relationships, names of its officers and directors, or information on its business location. The customer usually gives little or misleading information that is difficult or costly for the company to verify.
- Client gives unusual or suspicious identification documents that their authenticity cannot be directly verified.
- Customer's home/business telephone is disconnected.
- Customer makes frequent or large transactions and has no record of past or present employment experience.
- Difficulties or delays on the submission of the financial statements or other identification documents, of a customer/legal person.
- A customer who has been introduced by an overseas Financial Institution or a third person, whose countries or geographical areas of origin do not apply or they apply inadequately FATF's recommendations on money laundering and terrorist financing.
- Shared address for individuals involved in cash transactions, especially when the address is also a business location and/or does not appear to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc.).
- The declared profession of the customer is not commensurate with the level or size of the executed transactions.
- Financial transactions for non-profit or charitable organizations, for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- Unexplained inconsistencies arising during the customer identification (e.g. regarding previous or current county of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth etc.).
- Transactions or company structures established or working with an unneeded commercial way, e.g. companies with bearer shares or bearer financial instruments or use of a postal box.
- Use of general nominee documents in a way that restricts the control exercised by the company's Board of Directors.
- Changes in the lifestyle of employees, for example luxurious way of life or avoidance or absence from the office due to holidays.
- Changes in performance and behavior of employees.



Terrorist Financing

The funding or terrorist organizations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include:

- Kidnapping – requiring ransom
- Extortion – demanding protection money
- Smuggling
- Thefts
- Robbery
- Narcotics trafficking

Legal fund-raising methods used by terrorist groups include:

- Collection of membership dues and/or subscriptions
- Sale of books and other publications
- Cultural and social events
- Donations
- Community solicitations and fund raising appeals

Funds obtained from illegal sources are laundered in the following ways:

- Cash smuggling by couriers or bulk cash shipments
- Structured deposits to or withdrawals from bank accounts
- Purchases of monetary instruments – traveler's cheques, bank cheques, money orders
- Use of credit or debit cards
- Wire transfers by using straw men
- False identities
- Front and shell companies
- Nominees from among their close family members, friends and associates

Non-profit organizations:

The use of a non-profit and charitable organization for raising funds and/or serving as cover for transferring funds in support of terrorists' acts can be made in the following ways:



- Establishing a non-profit organization with a stated charitable purpose but which actually exists only to channel funds to a terrorist organization
- A non-profit organization with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group
- A sudden increase in the frequency and amounts of financial transactions for the account of a nonprofit organisation.
- Large and unexplained cash transactions
- The absence of contributions from donors located within the country of origin of the nonprofit organisation

7. COMPLIANCE FOOTNOTE

The compliance procedure related to AML listed above is only a brief summary of the compliance function guidelines followed by the Peaksight Compliance Team. A detailed copy of our Compliance Policy is available for qualified institutions, regulatory bodies and related counterparties.

No substitutions or modifications will be accepted to the requirements above. The Peaksight's Compliance Department reserves the final determination regarding the validity of these documents.

Clients should assume that all information provided to the Company is available to the competent regulatory authorities in

- a. the country of incorporation of the Company, i.e., the Republic of Cyprus;
- b. the country of origin of any funds transmitted to Peaksight;
- c. the destination country of any funds refunded by or withdrawn from the Company.

Peaksight does not wish to enter into a business relationship if the funds are sourced from criminal activities or if the nature of your account transactions is illegal in any manner whatsoever.

The Company reserves the right to review and/or amend its Anti Money Laundering Policy, at its sole discretion, whenever it deems fit or appropriate.

Our AML Policy is a policy only but is not part of our Terms and Conditions of Business and is not intended to be contractually binding.

For additional questions concerning Peaksight policies, please contact our Compliance Department:

Email: aml@peaksgighthtd.com

Attn. Compliance Department, Peaksight Ltd, registration number HE 433420.

Business Address: 204, P. LORDOS CENTER, Block B, Corner Makarios Avenue 240 & Vylonos 1 Street, 3105, Limassol