

AML & KYC Policy

How identity is verified and how the platform is kept clear of money laundering and terrorist financing.

ISSUER	LL CAPITAL & PARTNERS LIMITED (trading as North Stone Capital)
REGULATOR	Malta Financial Services Authority (MFSA)
MBR REGISTRATION CODE	C 46015 · Authorised Person ID: LLCP
COMPANY REGISTRATION DATE	13-01-2009 · LEI code: 5493008QRPT09QVP0C32
REGISTERED OFFICE	TAGLIAFERRO BUSINESS CENTRE, LEVEL 6 Gaiety Lane SLIEMA Malta SLM 1551
VERSION / STATUS	1.1 · Effective 19 September 2025 · Issued 19 September 2025
LANGUAGE	English (language of record). Paper copies free on request: support@northstonecapital.net

How North Stone Capital verifies who its clients are and prevents the use of its platform for money laundering and terrorist financing. It covers the checks performed before an account can trade, the monitoring applied for the life of the relationship, and the reporting obligations owed under LL CAPITAL & PARTNERS LIMITED's Malta/MFSA framework.

1. Introduction

LL CAPITAL & PARTNERS LIMITED operates northstonecapital.net and provides the services described on this website. LL CAPITAL & PARTNERS LIMITED, trading as North Stone Capital, was registered in Malta on 13-01-2009 (MBR Registration Code C 46015). Authorised Person ID: LLCP. LEI Code: 5493008QRPT09QVP0C32. Registered address: TAGLIAFERRO BUSINESS CENTRE, LEVEL 6 Gaiety Lane SLIEMA Malta SLM 1551. The company is regulated by the Malta Financial Services Authority under the Investment Services Act to provide investment services.

This policy has two equal pillars. The first is our Know Your Client (KYC) programme: before you can trade, we must establish who you are, where you are resident and, where risk requires it, the source of your funds. The second is our anti-money-laundering and counter-terrorist-financing (AML/CTF) framework: the controls we use to detect, deter and report attempts to use the platform for criminal proceeds or terrorist financing.

Neither pillar is optional, for us or for you. We cannot open an account, accept a deposit or release a withdrawal until relevant KYC checks are complete, and we will not maintain a relationship with any client who refuses to provide information required by this policy. This document explains what information we collect, how it is verified, how accounts are monitored over time and what happens when activity cannot be explained.

2. Regulatory Framework

LL CAPITAL & PARTNERS LIMITED's AML/CTF framework is aligned with the Recommendations of the Financial Action Task Force (FATF), the international standard-setter for combating money laundering and terrorist financing. The FATF Recommendations inform our risk-based approach, customer due diligence standards, record-keeping periods and suspicious-activity reporting procedures.

As a Malta-based investment-services firm regulated by the Malta Financial Services Authority, LL CAPITAL & PARTNERS LIMITED is subject to applicable Maltese AML/CTF laws, rules and guidance, including obligations relating to customer due diligence, ongoing monitoring, sanctions screening, reporting and record keeping.

Where local law or an applicable regulator imposes a stricter requirement, we apply the stricter standard. Compliance reports to senior management and, where required, to the relevant competent authorities.

3. Know Your Client (KYC) and Customer Due Diligence

Our KYC programme is the front line of this policy. Customer due diligence is not a one-off form-filling exercise: it begins before an account is opened, deepens when risk indicators appear, and continues for as long as the relationship lasts. The programme has three stages — identification, verification and ongoing monitoring — set out below.

Due diligence is applied in proportion to risk. Standard due diligence applies to most retail clients; simplified measures are never applied to the identification of the client itself; and enhanced due diligence applies where the client, their location, their funding or their behaviour presents elevated risk, including where the client is a politically exposed person.

Client Identification

Before establishing a business relationship, we identify every client. For individuals we collect, at a minimum: full legal name, date of birth, nationality, residential address, and a valid government-issued photographic identity document such as a passport, national identity card or driving licence. We also collect contact details and information about the client's occupation, trading experience and the intended purpose of the account.

For corporate and other non-natural clients we identify the legal entity itself — its name, registration number, registered address and constitutional documents — and the natural persons behind it. This includes directors, persons authorised to operate the account, and every ultimate beneficial owner, each of whom must be identified and verified to the same standard as an individual client. We do not open accounts where ownership cannot be traced to identifiable natural persons.

Verification Process

Identification information is verified against reliable and independent sources before an account may be funded or traded. Identity documents are checked for authenticity, validity and consistency using a combination of trained human review and electronic verification tools, including document forensics and biometric matching where available. Residential address is verified against the identity document or separate proof of address, such as a utility bill or bank statement issued in the client's name.

Where verification cannot be completed remotely, we may request additional documents, certified copies or a live video verification session. An account that has not completed verification remains restricted: it cannot trade, and any funds received are returned to their source.

Enhanced due diligence applies to clients assessed as higher risk, including politically exposed persons, their family members and close associates. For these clients we obtain additional information on the source of funds and source of wealth, corroborated by documentary evidence such as payslips, tax records, bank statements or proof of asset sales, and senior compliance approval is required before the relationship is established or continued.

Ongoing Monitoring

Verification does not end at onboarding. We monitor business relationships throughout their life to ensure that activity on the account is consistent with what we know of the client, their declared profile and their source of funds. Automated transaction monitoring flags patterns that warrant review, including deposits inconsistent with declared income, rapid movement of funds with little or no genuine trading, structuring of payments, and the use of multiple or changing payment methods.

Client records are kept current. We periodically refresh identification documents — more frequently for higher-risk clients — and we re-verify identity when documents expire, when account details change materially, or when activity triggers a review. Clients must keep their information up to date and respond to reasonable requests for updated documents; failure to do so may result in the account being restricted or closed.

Screening is continuous as well as event-driven: clients are screened against applicable sanctions lists, politically-exposed-person databases and adverse-media sources at onboarding and on an ongoing basis thereafter.

4. Risk Assessment

We operate a risk-based approach, as the FATF Recommendations require. Every client is assigned a risk rating at onboarding, derived from factors including: country of residence and citizenship; the jurisdictions involved in funding the account; occupation, business activity and source of funds; expected deposit size and trading pattern; whether the client is a politically exposed person or closely associated with one; and the channel through which the relationship was established.

Risk ratings are not static. They are recalculated when client circumstances change, when monitoring detects unexpected activity, and at periodic review. A higher rating triggers enhanced due diligence, closer monitoring and more frequent document refresh; an unacceptable rating means we decline or exit the relationship.

The group also conducts a business-wide risk assessment, reviewed by senior management, covering the products we offer, the jurisdictions we serve, our client base and our delivery channels. The output of that assessment drives the calibration of our controls, including the thresholds applied in our transaction-monitoring systems.

5. Suspicious Activity Reporting

Every employee is trained to recognise indicators of money laundering and terrorist financing and is required to escalate concerns internally, without delay, to the compliance function of the relevant entity. Internal reports are investigated by appointed compliance officers, who determine whether the activity can be explained or must be reported externally.

Where an entity is required to do so, it files a suspicious activity or suspicious transaction report with the financial intelligence unit or other competent authority of its jurisdiction. Filing decisions rest with the compliance function alone; no employee may decide that a matter is too small, too uncertain or commercially too sensitive to report.

We are prohibited by law from informing a client that a report has been made or that an investigation is under way (tipping off). For this reason, we may be unable to explain why a withdrawal is delayed, an account is restricted or a relationship has been ended. We may also suspend the processing of a transaction while a report is under consideration, where the law requires or permits us to do so.

6. Record Keeping

We retain all records obtained through customer due diligence — identification documents, verification results, risk assessments and account files — together with records of all transactions, for a minimum of five years after the end of the business relationship or the date of the transaction, whichever is later, and for longer where the law of the relevant entity's jurisdiction requires it.

Records are kept in a form that allows individual transactions to be reconstructed and produced promptly in response to lawful requests from regulators, financial intelligence units and law enforcement. Storage and access are subject to the safeguards described in our Privacy Policy; retention for AML/CTF purposes is a legal obligation and takes precedence over a client's request for erasure for the duration of the statutory period.

7. Training and Awareness

All employees receive AML/CTF and KYC training on joining and at regular intervals thereafter, with content tailored to their role. Client-facing and operations staff are trained to recognise suspicious behaviour at onboarding and in payment flows; compliance staff receive deeper training on typologies, regulatory developments and reporting obligations; senior management receives training appropriate to its oversight responsibilities.

Training covers, at a minimum: the legal framework applicable to the relevant entity; client identification and verification requirements; recognition of red flags and suspicious patterns; the internal escalation procedure and the prohibition on tipping off; and the personal consequences, including criminal liability, of failing to comply. Completion is tracked and forms part of each employee's record.

8. Prohibited Activities

North Stone Capital will not, under any circumstances: open or maintain anonymous accounts or accounts in fictitious names; establish or continue a relationship with a shell bank, or with an institution that permits its accounts to be used by shell banks; accept clients from, or process transactions involving, countries and territories subject to applicable comprehensive sanctions; or knowingly facilitate any transaction connected with money laundering, terrorist financing or the proceeds of crime.

We additionally prohibit practices that are common vehicles for the abuse of brokerage accounts: third-party payments — deposits must come from, and withdrawals must return to, a payment method held in the client's own name; cash deposits; the use of an account as a pass-through to move funds without genuine trading activity; and the opening of multiple accounts to circumvent verification or monitoring controls. Withdrawals are returned to the source of the original deposit wherever the payment method allows.

9. Cooperation with Authorities

LL CAPITAL & PARTNERS LIMITED cooperates fully with competent law-enforcement agencies, financial-intelligence units, the Malta Financial Services Authority and other authorities with lawful jurisdiction in the prevention, detection and investigation of money laundering and terrorist financing.

Cooperation includes responding promptly and completely to lawful requests for information, producing records within statutory deadlines, freezing or blocking accounts and transactions where a competent authority lawfully requires it, and giving effect to court orders and sanctions designations. Where information must be shared to meet these obligations, it is shared on a confidential basis and in accordance with our Privacy Policy.

10. Policy Review

This policy is reviewed at least annually by the compliance function and approved by senior management. Reviews take account of changes in the FATF Recommendations, Maltese law, MFSA expectations, sanctions regimes, typologies identified through monitoring and lessons learned from suspicious-activity reviews.

We may update this policy at any time. Material changes are reflected on the website and, where required, communicated through account notices or direct messages. Continued use of the services after an update means you accept the revised policy.

11. Reporting Concerns

If you have information about, or suspect, money laundering, terrorist financing or other financial crime connected with a North Stone Capital account or service, contact our compliance team at compliance@northstonecapital.net. Reports may be made by clients, employees, counterparties or members of the public, and may be made anonymously.

All reports are treated as confidential, are reviewed by the compliance function of the relevant entity, and are escalated to the competent authorities where required. We do not tolerate retaliation against anyone who raises a concern in good faith, whether or not the concern is ultimately substantiated.

12. Consequences of Non-Compliance

For employees, breach of this policy is a serious disciplinary matter that may result in dismissal and may expose the individual to regulatory penalties and criminal prosecution under applicable law.

For clients, refusal to provide required information, provision of false or misleading information, attempts to circumvent KYC or sanctions controls, unexplained suspicious activity or any suspected use of the account for financial crime may result in refusal to open an account, restrictions on deposits or withdrawals, suspension or closure of the account, cancellation of transactions where legally required, and reports to competent authorities.

We do not compensate clients for losses caused by lawful freezes, blocks, delays, closures or reports required by AML/CTF, sanctions, court-order or regulatory obligations.

Questions about this document may be sent to support@northstonecapital.net or to the registered office above. The current version of every regulatory document is published at northstonecapital.net/regulatory.