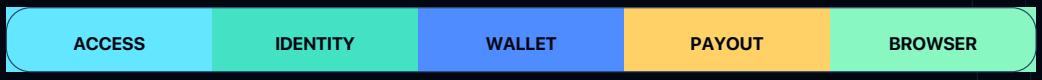
CoreStack
NEXUS

INVESTOR PROTECTION REFERENCE

Security Controls Brief

A plain-language brief explaining the CoreStack Nexus controls around account access, identity checks, wallet accuracy, payout review, browser protection, and security boundaries.



Current control summary

Investor-facing language

ACCESS CONTROLS

4

Login, reset, OTP/G2FA, and session safeguards.

ACTION THROTTLES

6

High-impact user actions have focused rate limits.

ASSET CHECKS

6

Wallet, network, payout, KYC, labels, and review records.

This brief describes implemented and documented safeguards. It is not a guarantee against loss, fraud, downtime, user error, or future security events.

CoreStack
NEXUS

ACCOUNT SAFEGUARDS

Access controls reduce abuse pressure

Authentication security is strongest when repeated failures, reset requests, OTP verification, G2FA checks, and session transitions are controlled together.

Login attempt throttling

Repeated failed sign-in attempts are limited by submitted identity and request IP.

5 per 60 sec

Password reset protection

Reset sends and reset-code verification attempts are throttled to reduce account abuse pressure.

Reset guard

OTP and G2FA abuse controls

OTP resend, login OTP verification, and user G2FA verification attempts are throttled and cleared on successful verification.

Code guard

Session cleanup

Authenticated session creation regenerates session IDs. Logout invalidates the session and regenerates the CSRF token.

Session guard

SESSION POSTURE

Session cookies are HTTP-only, default to SameSite lax, and default to HTTPS-only in production while remaining configurable for deployment edge cases.

CoreStack
NEXUS

HIGH-IMPACT ACTIVITY

Money movement actions have rate limits

Sensitive account actions are rate limited to help slow repeated invalid submissions and high-impact abuse attempts.

LIMIT SHAPE

6 **attempts per minute**

Sensitive action limits are shaped around the account, action type, and request source. P2P lookup uses a separate lower-risk lookup limit.

Per action

Per account

Per IP

Lookup guard

Normal browsing remains available while sensitive submissions receive stronger abuse protection.

- **Deposit request**
  Funding request creation is protected by action throttling.
- **Withdrawal request**
  Payout request creation is throttled before deeper processing.
- **Saved wallet creation**
  New payout destinations are treated as sensitive activity.
- **Investment allocation**
  Capital allocation and release actions are rate limited.
- **AI bot activation**
  Automation activation is included in high-impact controls.
- **P2P transfer**
  Transfer submission and recipient lookup have separate limits.

Control purpose: reduce repeated high-impact submissions without changing deposit, withdrawal, wallet, bot, investment, or P2P business logic.

CoreStack
NEXUS

ASSET MOVEMENT SAFEGUARDS

Wallet accuracy sits at the center

Security and custody information should make sensitive asset movement easier to understand without overstating what the platform has verified.

Wallet accuracy

Destination wallet, saved wallet status, and address ownership are part of payout review.

Network match

Selected asset and destination network must align before a payout can safely move forward.

Release review

Payouts can wait, queue, release, or be declined and returned based on policy status.

KYC readiness

Identity and account status inform investor readiness before higher-trust activity.

Custody labels

Current, account-specific, private, and under-review materials should remain clearly labeled.

Review records

Payout outcomes and policy context stay visible for account review decisions.

CLEAR SECURITY WORDING

Use clear phrases such as protected session, wallet review, release checks, account status, and identity review. Keep custody language precise and evidence-aware.

PLATFORM RESPONSE CONTROLS

Browser protections are conservative

The current browser-side controls improve baseline protection while avoiding risky CSP or HSTS changes before deployment compatibility is reviewed.

CONTROL	CURRENT POSTURE
Content type protection	X-Content-Type-Options: nosniff
Frame boundary	X-Frame-Options: SAMEORIGIN
Referrer boundary	Referrer-Policy: strict-origin-when-cross-origin
Permission boundary	Permissions-Policy blocks camera, microphone, and geolocation by default.
Cookie posture	HTTP-only sessions, SameSite lax default, and HTTPS-only session cookies by default in production.

DEFERRED CONTROLS

Content Security Policy and Strict Transport Security are deferred to production-readiness review so they can be tested against rendered pages, inline assets, HTTPS, and proxy behavior.

CoreStack
NEXUS

SECURITY BOUNDARIES

Controls should be clear and honest

A strong security brief is useful because it separates current safeguards from future improvements and keeps public claims clear.

Current safeguards

Login, reset, OTP/G2FA, session cleanup, browser headers, cookie posture, wallet review, and sensitive action throttles are presented as current safeguards.

Production readiness

Additional browser policies can be reviewed as deployment conditions and page compatibility are confirmed.

Custody clarity

Custody language should explain labels, wallet accuracy, review, and access boundaries in clear investor terms.

Clear security wording

Security language should sound protective, clear, and easy to understand without exposing operational detail.

DOCUMENT BASIS

This brief is based on CoreStack Nexus security and custody content, account-access safeguards, wallet review practices, payout controls, session-cookie posture, and investor verification language.

Document version: Public summary

Investor document set