Yes — we authenticate every person who contacts Support before we disclose account data or carry out sensitive actions.

Below is the high-level flow we follow today:

Stage	How We Verify	Typical Triggers
1. Channel authentication (low-risk)	• If the ticket is opened while the user is already logged-in to the web app or mobile SDK, we treat the in-session JWT + MFA as sufficient proof of identity. • For email tickets we require the message to originate from the **registered e-mail address**; our help-desk only accepts whitelisted domains.	Balance enquiries, general “how-to” questions
2. Secondary challenge (medium-risk)	• Support system automatically sends a **magic link** or **TOTP challenge** that must be completed inside the user dashboard. • Alternatively, the user can quote a one-time code taken from the last successful transaction (e.g., the final 4 chars of `pi_…`).	Refund requests ≤ US $500, minor profile edits
3. KYC re-check (high-risk)	• For payout-bank-account changes, e-mail swap, GDPR data-export/erasure or any request ≥ US $500, we trigger a **Stripe Identity / Onfido selfie-and-document check**. Only the pass/fail token is stored; no raw ID images persist on our servers	Payout changes, high-value refunds, personal-data-rights requests
4. Manual escalation	• If automated checks fail or the account is flagged as high-risk (e.g. EDD tier), an L2 specialist reviews the ticket and may request a live video call or notarised ID. • All agent actions are RBAC-controlled and audit-logged	Suspicious behaviour, regulatory enquiries

Additional controls and policies

- **Data-rights requests** (access, erasure, portability, etc.) are only honoured after we “require additional information to verify identity”; otherwise we must refuse the request .

- Every support interaction is linked to the customer’s **KYC status and Trust-Score record**, so agents immediately see risk tiering and can select the appropriate verification path .

- All correspondence, verification artefacts and agent actions are retained in encrypted audit logs for ≥ 5 years to meet GDPR/AML record-keeping rules .

In short: we apply a **risk-based ladder of authentication** — from session tokens to full document re-checks — so that simple queries stay friction-free while any request that could expose, change or move customer data or funds is backed by strong, independent identity proof.