ANTI-MONEY LAUNDERING AND KNOW YOUR CUSTOMER (AML/KYC) POLICY

Entity: Numberly Ltd.

Platform: smspva.com

Last Updated: May 2026

---

1. INTRODUCTION

Numberly Ltd (hereinafter — the "Company") is committed to the highest standards of Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF). The purpose of this Policy is to ensure that smspva.com (the "Platform") is not used for money laundering, fraud, or any other illegal activities. This Policy is designed to comply with international standards, including the FATF recommendations and GDPR.

2. RISK-BASED APPROACH (RBA)

The Company applies a Risk-Based Approach. This means that we apply enhanced due diligence to users and transactions that pose a higher risk of fraud or money laundering. Transactions involving bank cards are classified as high-risk and require mandatory identity verification.

3. COMPLIANCE OFFICER

The Company appoints a Money Laundering Reporting Officer (MLRO). The MLRO is responsible for:

- Overseeing the Platform’s AML/KYC compliance.
- Ensuring that transaction monitoring systems are functioning correctly.
- Reporting suspicious activities to relevant financial intelligence units if required.

4. CUSTOMER DUE DILIGENCE (CDD) AND KYC

We do not allow anonymous use of high-risk payment methods. To verify our customers, we have integrated a solution from Sum and Substance Ltd (Sumsub). The KYC process includes:

- Identification: Collection of full name, date of birth, and nationality.
- Document Verification: Automated OCR analysis of government-issued IDs (passports, ID cards, driver’s licenses) for authenticity and tampering.
- Biometric Verification (Liveness Check): 3D biometric face scanning to ensure the user is physically present and not using a mask or photo.
- Sanction & PEP Screening: Automated cross-referencing of all users against global sanction lists (OFAC, UN, EU, HMT) and Politically Exposed Persons (PEP) lists.

5. TRANSACTION MONITORING

Our internal systems, combined with payment provider tools, monitor all transactions in real-time. We flag the following suspicious patterns:

- Use of multiple cards for a single account.
- Rapid succession of top-up attempts from different IP addresses.
- High-velocity transactions that deviate from normal user behavior.
- Attempted use of stolen or blacklisted cards.

6. REFUND-TO-SOURCE POLICY (ANTI-LAYERING)

To prevent the "layering" stage of money laundering, the Company strictly enforces a Refund-to-Source policy:

- Funds can only be returned to the exact same payment instrument (the specific bank card) that was used for the initial deposit.
- Refunds to third-party accounts or alternative payment methods (e.g., crypto, e-wallets) are strictly prohibited for card-based deposits.

7. RECORD KEEPING

In accordance with international AML standards and GDPR requirements, the Company maintains records of:

- Customer identification data and verification results.
- Transaction history and logs. Retention Period: All records are securely stored for a period of 5 years after the business relationship ends, regardless of account deletion requests, to satisfy regulatory audit requirements.

8. SANCTIONS COMPLIANCE

The Company does not provide services to individuals or entities located in countries sanctioned by the UN, OFAC, or the EU. If a user is identified as being on a sanctions list, their account will be immediately frozen, and the payment gateway will be blocked.

9. TRAINING

All employees involved in processing payments and customer support undergo regular AML/KYC training to identify "red flags" and suspicious behavior.

10. CONTACT INFORMATION

For any compliance-related inquiries, please contact our MLRO at: contact@smspva.com.