This KYC (Know Your Customer) & CDD (Customer Due Diligence) checklist is designed to help crypto businesses verify customers in compliance with AML regulations, including the UK Money Laundering Regulations 2017 (MLR 2017) and Financial Conduct Authority (FCA) guidelines.

Customer Identification & Verification (CIP - Customer Identification Program)

- Collect full legal name of the customer.
- Obtain date of birth (for individual customers).
- Obtain residential address (for individuals) or registered business address (for corporate customers).
- Collect a government-issued identification document (passport, driving license, or national ID).
- Verify the document's authenticity using an automated identity verification system or manual review.
- Conduct facial recognition or liveness check (if applicable).
- Obtain proof of address (utility bill, bank statement, or official government correspondence - not older than 3 months).
- Verify phone number and email address via OTP (One-Time Password) verification.

Enhanced Due Diligence (EDD) for High-Risk Customers

- Identify and flag high-risk customers (e.g., politically exposed persons (PEPs), high-value traders, cross-border clients).
- Request additional proof of identity or documentation (e.g., second government-issued ID).
- Obtain information on the source of funds and source of wealth.
- Conduct enhanced transaction monitoring and periodic reviews.
- Check against global watchlists and sanctions lists (HM Treasury, OFAC, FATF, EU Sanctions List).
- Request additional business documentation for corporate clients (e.g., certificate of incorporation, shareholder structure).
- Conduct adverse media screening for potential negative associations.

4. Ongoing Monitoring & Risk-Based Approach

- Establish risk categories for customers based on transaction volume, geography, and nature of activities.
- Implement real-time transaction monitoring to detect suspicious activities.
- Flag and investigate unusual transaction patterns (e.g., rapid deposits/withdrawals, use of multiple accounts, mixing services).
- Conduct periodic reviews of customer profiles, especially for high-risk accounts.

- Report suspicious activities to the UK National Crime Agency (NCA) via Suspicious Activity Reports (SARs) when required.
- Ensure that high-risk customers undergo periodic Enhanced Due Diligence (EDD) checks.

5. Record-Keeping Requirements

- Maintain customer identification records for at least 5 years after the business relationship ends.
- Store transaction history and SAR filings securely and make them accessible for regulatory audits.
- Keep logs of all communication with customers regarding KYC/AML verification.
- Ensure compliance with GDPR and data protection laws when storing personal data.

6. Compliance & Staff Training

- Train employees on AML/KYC requirements and risk assessment methodologies.
- Conduct regular refresher training for compliance teams handling KYC/CDD processes.
- Ensure all staff understands red flags of money laundering in the crypto sector.
- Implement internal escalation procedures for reporting suspicious activities.