KYC/AML Technical Integration Guide

Implementing regulatory compliance for financial crime prevention

Version: 1.0

Author: Compliance & Engineering Team

Category: Regulatory Compliance | AML/KYC

Regulatory Framework: UK MLR 2017, FCA Handbook, PSD2

Last Updated: December 11, 2025

This technical guide provides comprehensive integration patterns for implementing Know Your Customer (KYC) and Anti-Money Laundering (AML) controls within the Monzo API ecosystem. Following the FCA's £21M fine for AML control weaknesses (2018-2022), this documentation establishes robust technical patterns to ensure regulatory compliance and effective financial crime prevention.

Regulatory Context

UK financial institutions must comply with the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (MLR 2017) and FCA Handbook requirements. Key obligations include:

Customer Due Diligence (CDD): Verify identity of all customers before establishing business relationship

Enhanced Due Diligence (EDD): Apply enhanced measures for high-risk customers (PEPs, high-risk countries, complex ownership structures)

Ongoing Monitoring: Continuous transaction monitoring to detect suspicious activity

Suspicious Activity Reporting: File SARs to National Crime Agency (NCA) within required timeframes

Record Keeping: Maintain audit trails for minimum 5 years

> **✓ COMPLIANCE: This guide implements MLR 2017 Regulations 27-30 (Customer Due Diligence), Regulation 33 (Ongoing Monitoring), and Regulation 35 (Enhanced Due Diligence).**

KYC Verification Workflow

Customer onboarding requires multi-stage identity verification combining document checks, biometric verification, and data validation.

Stage 1: Identity Document Verification

Accept government-issued ID documents and verify authenticity using third-party verification providers (Onfido, Jumio, or similar).

Document Type	Accepted	Verification Method	Risk Level
UK Passport	Yes	Chip reading + OCR + visual inspection	Low
UK Driving License	Yes	DVLA verification + OCR	Low
National ID Card (EU)	Yes	OCR + visual security features	Medium
BRP/BRC (Immigration)	Yes	Home Office verification	Medium
Non-EU Passport	Yes	OCR + MRZ reading + watchlist check	Medium-High
Birth Certificate	No	Insufficient for primary ID	N/A

API Integration: Document Submission

```
POST /api/v1/kyc/document-verification Authorization: Bearer {access_token} Content-Type:
multipart/form-data { "customer_id": "user_00009238aqC8c79WTZ", "document_type":
"passport", "document_country": "GBR", "document_images": { "front":
"base64_encoded_image_data", "back": "base64_encoded_image_data" // For driving license },
"verification_provider": "onfido", "callback_url": "https://yourapp.com/webhooks/kyc" } #
Response { "verification_id": "kyc_00008zIcpb1TB4yeIFXMzx", "status": "pending",
"estimated_completion": "2024-12-11T14:30:00Z", "checks_performed": [
"document_authenticity", "data_extraction", "watchlist_screening" ] }
```

Stage 2: Biometric Liveness Check

Capture selfie video to confirm customer is physically present and matches ID document photo. Prevents identity fraud using stolen documents.

```
POST /api/v1/kyc/biometric-verification Authorization: Bearer {access_token} Content-Type:
application/json { "customer_id": "user_00009238aqC8c79WTZ", "verification_id":
"kyc_00008zIcpb1TB4yeIFXMzx", "selfie_video": "base64_encoded_video_data",
"liveness_type": "active", // active (user follows prompts) or passive
"verification_provider": "onfido" } # Response { "biometric_match_score": 0.97, // 0-1
scale, threshold typically 0.85 "liveness_passed": true, "face_comparison_result":
"clear_match", "verification_status": "approved" }
```

■■ WARNING: Biometric match threshold must be calibrated to balance fraud prevention with customer friction. Monzo uses 0.87 threshold based on false positive/negative analysis.

Stage 3: Data Validation & Address Verification

Cross-reference customer data against electoral roll, credit bureaus, and utility databases.

```
POST /api/v1/kyc/address-verification Authorization: Bearer {access_token} Content-Type:
application/json { "customer_id": "user_00009238aqC8c79WTZ", "address": { "line1": "123
High Street", "line2": "Flat 4B", "city": "London", "postcode": "SW1A 1AA", "country":
"GBR" }, "verification_sources": [ "electoral_roll", "credit_bureau", "utility_database" ]
} # Response { "verification_status": "confirmed", "matches": [ { "source":
"electoral_roll", "match_confidence": "high", "residency_duration": "3_years" }, {
"source": "credit_bureau", "match_confidence": "high", "address_on_file_since":
"2021-08-15" } ], "risk_flags": [] }
```

PEP & Sanctions Screening

Politically Exposed Persons (PEPs) and individuals on sanctions lists require Enhanced Due Diligence. Screening must occur at onboarding and ongoing intervals.

Screening API Integration

```
POST /api/v1/aml/screening Authorization: Bearer {access_token} Content-Type:
application/json { "customer_id": "user_00009238aqC8c79WTZ", "screening_type":
"comprehensive", "search_parameters": { "full_name": "John Smith", "date_of_birth":
"1985-06-15", "nationality": "GBR", "countries_of_residence": ["GBR"], "fuzzy_matching":
true, // Allow name variations "threshold": 85 // Match confidence percentage },
"screening_lists": [ "uk_hmt_sanctions", "eu_sanctions", "un_sanctions", "ofac_sdn",
"pep_domestic", "pep_foreign", "adverse_media" ] } # Response { "screening_id":
"scr_00009A1BK4MH8sY4y3Qm", "status": "completed", "overall_risk_level": "low", "matches":
[], "screened_at": "2024-12-11T14:25:00Z", "next_screening_due": "2024-12-11T14:25:00Z" //
12 months for low-risk }
```

Handling PEP Matches

When screening identifies a PEP, automatically trigger Enhanced Due Diligence workflow:

PEP Category	Risk Level	EDD Requirements	Approval Level
UK Domestic PEP	Medium	Source of wealth, senior management approval	Head of Compliance
Foreign PEP (High Risk Country)	High	Source of wealth + source of funds, board approval	MLRO + Board
International Organization Official	Medium	Source of wealth, senior management approval	Head of Compliance
Family Member of PEP	Medium	Verify relationship, source of wealth	Head of Compliance
Known Close Associate	Medium-High	Document relationship, source of wealth	MLRO

✓ COMPLIANCE: MLR 2017 Regulation 35 requires ongoing monitoring of PEP relationships for entire business duration, with annual reviews minimum.

Transaction Monitoring Patterns

Implement real-time transaction monitoring to detect suspicious patterns indicative of money laundering, terrorist financing, or fraud.

Monitoring Rules Engine

Common suspicious activity patterns to detect:

Rule ID	Pattern	Threshold	Action
TM-001	Rapid movement (in/out same day)	>£5,000 within 24h	Alert + Review

TM-002	Structuring (avoiding reporting)	Multiple txns <£9,000 same day	Alert + SAR
TM-003	High-risk country transfers	Any amount to FATF blacklist	Block + Review
TM-004	Round number transactions	>£5,000 in exact hundreds	Alert + Review
TM-005	Inconsistent activity pattern	>3x normal monthly volume	Alert + Review
TM-006	Crypto exchange deposits	>£10,000 to known exchanges	Alert + Review
TM-007	Cash deposit pattern	>3 ATM deposits per month	Alert + Review
TM-008	Gambling transaction volume	>£20,000 monthly to gambling	Alert + EDD

Real-Time Monitoring API

```
POST /api/v1/aml/transaction-monitor Authorization: Bearer {access_token} Content-Type:
application/json { "transaction_id": "tx_00008zIcpb1TB4yeIFXMzx", "customer_id":
"user_00009238aqC8c79WTZ", "amount": 8500, "currency": "GBP", "type": "bank_transfer",
"counterparty": { "name": "ABC Trading Ltd", "account_number": "12345678", "sort_code":
"20-00-00", "bank_country": "GBR" }, "monitor_rules": [ "TM-001", "TM-002", "TM-004",
"TM-005" ] } # Response { "monitoring_id": "mon_00009K2HL5PQ9tX8x2Rm", "risk_score": 67, //
0-100 scale "triggered_rules": [ { "rule_id": "TM-004", "rule_name": "Round number
transactions", "severity": "medium", "details": "Transaction is exact round number >£5,000"
} ], "action_required": "manual_review", "transaction_status": "pending_review",
"assigned_to": "aml_team_queue" }
```

Suspicious Activity Reporting (SAR)

When transaction monitoring identifies potential money laundering, generate and file Suspicious Activity Report to UK National Crime Agency.

SAR Decision Workflow

```
POST /api/v1/aml/sar-submission Authorization: Bearer {access_token} Content-Type:
application/json { "customer_id": "user_00009238aqC8c79WTZ", "sar_type":
"suspicious_activity", "reporter": { "name": "Jane Doe", "role": "AML Analyst",
"employee_id": "emp_00001" }, "suspicion_details": { "activity_type": "structuring",
"transactions": [ "tx_00008zIcpb1TB4yeIFXMzx", "tx_00008zJdqc2UC5zfJGYNzy" ],
"total_amount": 17500, "time_period": "2024-12-01 to 2024-12-10", "reason_for_suspicion":
"Customer made 7 transactions of £2,500 each over 10 days, all to different recipients,
pattern consistent with structuring to avoid detection.", "additional_context": "Customer
occupation is listed as 'student' with no declared income source to support this
transaction volume." }, "submit_to_nca": true, "consent_required": false // Set true if
need NCA consent to proceed } # Response { "sar_reference": "SAR-2024-12345",
"nca_submission_id": "NCA-UK-2024-456789", "submitted_at": "2024-12-11T14:45:00Z",
"status": "submitted", "actions_taken": [ "customer_account_flagged",
"enhanced_monitoring_enabled", "transaction_limits_applied" ] }
```