International Anti Money Laundering Standards

Transaction Monitoring and Controls

Account Aggregation – a technique that consolidates multiple accounts belonging to the same customer to provide a holistic view of activity. Related terms: Customer Profile, KYC. By linking accounts, analysts can detect patterns that would be invisible in isolation. Example: a client holds a savings, checking, and foreign currency account; aggregated monitoring reveals a rapid inflow of funds across all accounts. Challenge: ensuring accurate linkage without violating privacy regulations.

Alert Generation – the process of creating notifications when transactions meet predefined criteria indicating potential suspicious activity. Related terms: Threshold, Rule-Based System. Alerts trigger further investigation by compliance officers. Example: a cash deposit exceeding $10,000 generates an alert. Challenge: balancing sensitivity to avoid excessive false positives that overwhelm staff.

Anti-Money Laundering (AML) Framework – the set of policies, procedures, and controls designed to prevent and detect money laundering. Related terms: Regulatory Compliance, Risk Assessment. The framework guides transaction monitoring, reporting, and training. Example: a bank adopts a risk-based AML framework aligned with FATF recommendations. Challenge: keeping the framework up-to-date with evolving threats.

Baseline Transaction Profile – the normal range of transaction behavior established for a customer based on historical data. Related terms: Statistical Modeling, Customer Segmentation. Deviations from the baseline may indicate suspicious activity. Example: a retail customer typically makes weekly $200 purchases; a sudden $5,000 transfer stands out. Challenge: dynamic baselines must adapt to legitimate changes in behavior.

Black-List Screening – checking customers and transactions against lists of sanctioned individuals, entities, or countries. Related terms: Sanctions List, OFAC. Screening prevents prohibited parties from accessing services. Example: a wire transfer to a country on the UN sanctions list is blocked. Challenge: maintaining up-to-date lists and managing false matches due to name similarities.

Business Rule Engine – software that applies logical conditions to transaction data to identify anomalies. Related terms: Rule-Based Monitoring, Alert Logic. Rules can be static (e.g., “amount > $10,000”) or dynamic (e.g., “frequency exceeds average”). Example: a rule flags any outbound transfer to a high-risk jurisdiction exceeding $5,000. Challenge: rule fatigue and the need for regular tuning.

Cash Transaction Reporting – mandatory filing of reports for cash transactions above a statutory threshold. Related terms: CTR, Currency Transaction Report. The report is submitted to the financial intelligence unit (FIU). Example: a casino reports a $15,000 cash purchase of chips. Challenge: distinguishing legitimate

high-value cash use from structuring.

Case Management System – an application that tracks the lifecycle of alerts, investigations, and SARs (Suspicious Activity Reports). Related terms: SAR, Workflow. It ensures documentation, audit trails, and timely escalation. Example: an analyst assigns an alert to a senior investigator, records findings, and closes the case. Challenge: integrating disparate data sources into a single view.

Customer Due Diligence (CDD) – the process of verifying a customer's identity and assessing risk before establishing a business relationship. Related terms: KYC, Risk Rating. CDD informs monitoring parameters. Example: a new corporate client provides incorporation documents and beneficial owner details. Challenge: obtaining reliable information for high-risk jurisdictions.

Enhanced Due Diligence (EDD) – additional scrutiny applied to high-risk customers or transactions beyond standard CDD. Related terms: Risk Mitigation, Source of Funds. EDD may involve site visits or deeper background checks. Example: a politically exposed person (PEP) requires verification of the source of a $2 million deposit. Challenge: resource intensity and potential delays in onboarding.

Entity Resolution – the process of identifying and linking records that refer to the same real-world entity across multiple data sources. Related terms: Data Matching, Master Data Management. Accurate resolution reduces duplicate alerts. Example: "John Doe" with differing address records is recognized as a single customer. Challenge: handling variations in spelling, transliteration, and incomplete data.

False Positive Rate – the proportion of alerts that are generated but ultimately deemed non-suspicious. Related terms: Alert Fatigue, Precision. A high rate indicates inefficient monitoring. Example: 80 % of alerts for a retail bank are false positives, straining resources. Challenge: optimizing algorithms to reduce noise without missing true threats.

Financial Action Task Force (FATF) – an inter-governmental body that sets international AML and counter-terrorism financing standards. Related terms: Recommendations, Mutual Evaluation. FATF's 40 Recommendations form the global baseline. Example: a country adopts FATF's "risk-based approach" to AML. Challenge: translating broad standards into actionable controls.

Frequency Analysis – statistical examination of how often certain transaction types occur within a defined period. Related terms: Pattern Recognition, Time Series. Unusual frequency may signal structuring. Example: a client makes ten $9,900 cash deposits in a month, just below reporting threshold. Challenge: distinguishing legitimate high-frequency activity from illicit behavior.

Geographic Risk Scoring – assigning risk levels to jurisdictions based on factors such as corruption, terrorism links, or regulatory quality. Related terms: Country Rating, Risk Matrix. Scores influence monitoring thresholds. Example: transactions involving a high-risk country trigger lower alert thresholds. Challenge: updating scores as political situations evolve.

High-Risk Customer – a client classified as having a greater likelihood of involvement in money laundering due to factors like industry, geography, or PEP status. Related terms: Risk Rating, EDD. Monitoring for such customers is intensified. Example: a hedge fund operating in a jurisdiction with weak AML enforcement is labeled high-risk. Challenge: balancing business opportunities with compliance obligations.

Identifier Normalization – standardizing identifiers (e.g., names, addresses) to a consistent format before matching. Related terms: Data Cleansing, Entity Resolution. Normalization improves matching accuracy. Example: converting "St." to "Street" and removing punctuation in addresses. Challenge: handling multilingual and culturally specific naming conventions.

In-House Transaction Monitoring System (TMS) – a proprietary platform developed by an institution to detect suspicious activity. Related terms: Rule Engine, Dashboard. Custom systems can be tailored to specific risk profiles. Example: a bank builds a TMS that integrates real-time payment data with customer risk scores. Challenge: ensuring scalability and maintaining regulatory compliance.

International Sanctions Compliance – adherence to sanctions regimes imposed by bodies such as the UN, EU, or OFAC. Related terms: Blacklist Screening, Export Controls. Non-compliance can result in severe penalties. Example: a trade finance transaction is blocked because the beneficiary is on the OFAC SDN list. Challenge: reconciling overlapping sanctions lists and exemptions.

Key Risk Indicator (KRI) – metrics used to monitor the effectiveness of AML controls and highlight emerging threats. Related terms: Dashboard, Risk Appetite. KRIs support proactive adjustments. Example: a rising KRI for "large cash deposits in low-risk branches" prompts a review of monitoring rules. Challenge: selecting KRIs that are both meaningful and measurable.

KYC Refresh Cycle – the periodic review and update of customer information to ensure ongoing compliance. Related terms: CDD, Risk Re-assessment. Refresh cycles vary by risk tier. Example: a medium-risk client's information is refreshed every 24 months. Challenge: managing the workload while avoiding "customer fatigue."

Layered Controls – multiple, overlapping safeguards designed to detect and deter money laundering. Related terms: Defense-in-Depth, Redundancy. Layers may include screening, monitoring, and reporting. Example: a transaction passes both rule-based checks and AI-driven anomaly detection before settlement. Challenge: ensuring layers complement rather than duplicate each other.

Machine Learning (ML) Models – algorithms that learn patterns from historical transaction data to predict suspicious activity. Related terms: Supervised Learning, Feature Engineering. ML can uncover non-linear relationships. Example: a gradient-boosted tree model flags a series of low-value transfers that together form a suspicious pattern. Challenge: model interpretability and regulatory acceptance.

Money Laundering Lifecycle – the three-stage process of placement, layering, and integration of illicit funds. Related terms: Structuring, Smurfing. Understanding the lifecycle aids in designing controls. Example: cash is

deposited (placement), moved through multiple accounts (layering), and finally used to purchase assets (integration). Challenge: detecting activity that spans multiple institutions and jurisdictions.

Negative News Screening – checking customers against adverse media reports that may indicate illicit behavior. Related terms: Adverse Media, Reputation Risk. Screening is often automated. Example: a client appears in a news article about a fraud investigation, prompting a review. Challenge: filtering out irrelevant mentions while retaining material risk indicators.

Operational Risk in AML – the risk of loss resulting from inadequate or failed internal processes, people, or systems. Related terms: Process Failure, Business Continuity. Operational lapses can undermine AML effectiveness. Example: a system outage disables real-time transaction monitoring for several hours. Challenge: building resilient processes and maintaining documented controls.

Outbound Transaction Monitoring – surveillance of funds leaving an institution to detect suspicious disbursements. Related terms: Payment Screening, Beneficiary Verification. Outbound monitoring is critical for preventing the export of illicit funds. Example: a large wire to a high-risk jurisdiction triggers an outbound alert. Challenge: obtaining reliable information on ultimate beneficiaries.

PEP (Politically Exposed Person) Identification – the process of recognizing individuals who hold or have held prominent public functions. Related terms: Enhanced Due Diligence, Risk Rating. PEPs require additional scrutiny. Example: a senior government official opening a corporate account triggers a PEP flag. Challenge: managing family members and close associates who may also be high-risk.

Pattern Recognition – analytical techniques that identify recurring sequences or structures in transaction data. Related terms: Clustering, Anomaly Detection. Patterns can indicate money-laundering schemes. Example: a “round-trip” pattern where funds are transferred out and back within days. Challenge: distinguishing benign repeat business from illicit looping.

Payment Service Provider (PSP) Monitoring – oversight of third-party providers that facilitate electronic payments on behalf of customers. Related terms: Third-Party Risk, Outsourcing. PSPs must adhere to AML standards. Example: a fintech PSP is required to share transaction data with the sponsoring bank for monitoring. Challenge: ensuring data integrity across platforms.

Periodic Review of Controls – scheduled assessment of AML policies, procedures, and technology to confirm effectiveness. Related terms: Audit, Continuous Improvement. Reviews may be internal or external. Example: an annual audit evaluates the rule set of the transaction monitoring system. Challenge: maintaining objectivity and addressing identified gaps promptly.

Positive Identification – the confirmation that a customer’s presented identity matches reliable source documents. Related terms: KYC, Verification. Positive identification is a prerequisite for onboarding. Example: a passport and utility bill are cross-checked to verify a new client. Challenge: dealing with documents from jurisdictions with limited verification infrastructure.

Predictive Analytics – statistical techniques that forecast future transaction behavior based on historical trends. Related terms: Risk Scoring, Machine Learning. Predictive models help set dynamic thresholds. Example: a model predicts that a client's transaction volume will increase by 30 % next quarter, adjusting monitoring parameters accordingly. Challenge: model drift as customer behavior changes.

Regulatory Reporting – mandatory submission of AML-related reports to authorities, such as SARs, CTRs, and suspicious transaction filings. Related terms: SAR, FIU. Timely reporting is a legal requirement. Example: a bank files a SAR within 30 days of detecting a suspicious wire. Challenge: ensuring accuracy and completeness while protecting confidentiality.

Risk-Based Approach (RBA) – tailoring AML controls proportionally to the risk level of customers, products, and geographies. Related terms: Risk Assessment, Controls. RBA optimizes resource allocation. Example: a low-risk retail customer receives basic monitoring, while a high-risk corporate client undergoes enhanced scrutiny. Challenge: quantifying risk and avoiding subjective bias.

Sanctions Evasion Detection – identifying attempts to circumvent sanctions through indirect or complex transactions. Related terms: Black-List Screening, Transaction Structuring. Detection requires deep analysis. Example: a series of small transfers to multiple entities in a sanctioned country masks the underlying prohibited activity. Challenge: tracing ultimate beneficial ownership across layers.

Scenario-Based Testing – simulation of money-laundering schemes to evaluate the effectiveness of monitoring rules. Related terms: Test Cases, Validation. Scenarios emulate real-world tactics. Example: a test scenario creates a "smurfing" pattern to verify that alerts are generated. Challenge: maintaining up-to-date scenarios that reflect emerging threats.

Structured Query Language (SQL) Auditing – reviewing database queries used in monitoring to ensure they retrieve accurate data. Related terms: Data Integrity, Log Review. Auditing prevents hidden gaps. Example: an audit discovers that a query excludes transactions above a certain amount due to a coding error. Challenge: coordinating audits across multiple data warehouses.

Suspicious Activity Report (SAR) – a confidential filing to the FIU describing transactions that may involve money laundering. Related terms: Regulatory Reporting, Confidentiality. SARs are a core AML instrument. Example: an analyst submits a SAR after identifying a series of layered transfers to offshore accounts. Challenge: balancing thoroughness with the need to protect customer privacy.

Transaction Aggregation – combining multiple related transactions into a single analytical unit to assess cumulative risk. Related terms: Batch Processing, Cumulative Threshold. Aggregation reveals hidden patterns. Example: ten $9,500 cash deposits in a month are aggregated to a $95,000 total, surpassing the reporting threshold. Challenge: defining appropriate aggregation windows.

Transaction Monitoring Dashboard – a visual interface that displays alerts, trends, and key metrics for compliance staff. Related terms: Key Risk Indicator, Case Management. Dashboards support rapid

decision-making. Example: a heat map highlights regions with increasing alert volumes. Challenge: preventing information overload and ensuring real-time data refresh.

Transaction Monitoring Parameters – the specific settings (e.g., amount, frequency, geography) that define when an alert is triggered. Related terms: Rule Engine, Threshold. Parameters are adjusted based on risk appetite. Example: a parameter sets a $20,000 threshold for outbound transfers to high-risk countries. Challenge: maintaining optimal balance between detection and false positives.

Transaction Screening – the process of evaluating each transaction against lists of prohibited parties and risk criteria. Related terms: Sanctions Screening, Beneficiary Verification. Screening occurs pre- and post-settlement. Example: a payment to a vendor is screened against the OFAC list before processing. Challenge: handling large volumes with minimal latency.

Transfer Pricing Abuse Detection – monitoring for artificial pricing in intra-company transfers that could conceal illicit funds. Related terms: Beneficial Ownership, Tax Evasion. Detection involves comparing pricing to market benchmarks. Example: a subsidiary receives services at unusually low fees, prompting investigation. Challenge: accessing reliable external pricing data.

Trusted Third-Party Verification – reliance on external entities to confirm customer information or transaction legitimacy. Related terms: Outsourcing, Data Provider. Third parties can enhance due diligence efficiency. Example: a bank uses a reputable data vendor to validate a corporate client's registration details. Challenge: ensuring the third party's compliance standards align with the institution's obligations.

Unusual Activity Indicator (UAI) – a flag that denotes a transaction deviating from expected patterns, prompting review. Related terms: Alert Generation, Anomaly Detection. UAIs may be based on amount, counterparties, or timing. Example: a sudden large wire to a new beneficiary triggers a UAI. Challenge: calibrating sensitivity to avoid excessive manual workload.

Virtual Asset Service Provider (VASP) Monitoring – oversight of entities that facilitate the exchange of cryptocurrencies and other virtual assets. Related terms: Crypto AML, FATF Guidance. VASPs are subject to AML obligations. Example: a VASP must report suspicious wallet transfers exceeding a certain value. Challenge: dealing with pseudonymous addresses and rapid transaction speeds.

Watch-List Management – the ongoing process of maintaining and updating internal lists of high-risk individuals and entities. Related terms: Blacklist Screening, Data Governance. Effective management reduces missed matches. Example: a new sanction is added to the watch-list, and the system automatically re-screens recent transactions. Challenge: reconciling multiple source lists and handling duplicate entries.

Workflow Automation – the use of software to route alerts, assign investigators, and document decisions without manual intervention. Related terms: Case Management, Process Efficiency. Automation speeds response times. Example: an inbound alert is automatically assigned to a junior analyst based on risk tier. Challenge: retaining flexibility for complex cases that require human judgment.

Zero-Tolerance Policy – an institutional stance that any confirmed AML breach results in immediate remedial action, often including termination. Related terms: Compliance Culture, Enforcement. The policy underscores the seriousness of AML obligations. Example: an employee who deliberately falsifies KYC documents is terminated under a zero-tolerance policy. Challenge: ensuring the policy is applied consistently and fairly.