
Compliance and Anti Money Laundering

Anti Money Laundering Investigations

Adverse Media – A source of information that reports negative or suspicious activity about an individual or entity.

Related terms: negative news, media screening, reputational risk.

Explanation: Investigators use adverse media to corroborate other intelligence and assess the credibility of a potential money-laundering risk.

Example: A news article linking a client to a drug cartel prompts further transaction analysis.

Challenge: Distinguishing factual reporting from rumor, especially in jurisdictions with limited press freedom.

Aggregated Transaction Monitoring – The process of consolidating transactions across multiple accounts, products, or entities to detect patterns that might be hidden in isolated data sets.

Related terms: data integration, cross-product monitoring, pattern analysis.

Explanation: By aggregating data, AML systems can identify cumulative thresholds or repeated behaviors that trigger alerts.

Example: A corporate client moves funds through several subsidiaries, each staying below the reporting limit, but the total exceeds the risk threshold.

Challenge: Managing large data volumes while preserving privacy and ensuring real-time detection.

Alert – A notification generated by an AML monitoring system indicating a possible breach of policy or regulatory thresholds.

Related terms: trigger, investigation file, case management.

Explanation: Alerts are the first step in the investigative workflow; they must be prioritized, reviewed, and either resolved or escalated.

Example: An automated rule flags a \$12,000 cash deposit from a high-risk jurisdiction.

Challenge: High false-positive rates can overwhelm staff and lead to alert fatigue.

Anti-Money Laundering (AML) – A set of laws, regulations, and procedures designed to prevent the generation of income through illegal actions.

Related terms: counter-terrorism financing (CTF), compliance program, risk assessment.

Explanation: AML frameworks require institutions to identify customers, monitor transactions, and report suspicious activity.

Example: A bank implements KYC procedures to verify the identity of new clients.

Challenge: Keeping pace with evolving typologies and regulatory expectations across multiple jurisdictions.

Beneficial Owner – The natural person who ultimately owns or controls a legal entity, directly or indirectly.

Related terms: ownership structure, control hierarchy, UBO register.

Explanation: Identifying the beneficial owner is crucial for assessing the true risk associated with a client.

Example: A shell company listed in a tax haven is ultimately owned by a politically exposed individual.

Challenge: Complex corporate layers and nominee arrangements can obscure true ownership.

Customer Due Diligence (CDD) – The process of gathering and verifying information about a client to assess risk.

Related terms: enhanced due diligence (EDD), risk rating, KYC.

Explanation: CDD is performed at onboarding and periodically thereafter, focusing on identity, purpose of the relationship, and source of funds.

Example: A new corporate client provides incorporation documents, shareholder lists, and audited financial statements.

Challenge: Balancing thoroughness with customer experience, especially for low-risk clients.

Designated Non-Financial Business and Professions (DNFBPs) – Sectors that are not banks but are vulnerable to money-laundering, such as lawyers, accountants, and real-estate agents.

Related terms: non-financial institution, risk-based approach, reporting obligations.

Explanation: DNFBPs must implement AML controls proportionate to their exposure.

Example: A law firm must file a suspicious activity report (SAR) when a client uses a trust to purchase high-value property without a clear source of wealth.

Challenge: Limited resources and varying regulatory expectations across professions.

Enhanced Due Diligence (EDD) – Additional investigative steps applied to high-risk customers or transactions.

Related terms: high-risk client, risk matrix, source-of-wealth verification.

Explanation: EDD may include deeper background checks, senior-management approvals, and ongoing monitoring.

Example: A politically exposed person (PEP) opening a multi-currency account triggers an EDD file that includes media searches and senior officer sign-off.

Challenge: Determining the appropriate depth of EDD without causing undue friction.

Financial Action Task Force (FATF) – An intergovernmental body that sets international AML/CTF standards.

Related terms: Recommendations, mutual evaluations, high-risk jurisdictions.

Explanation: FATF's 40 Recommendations form the basis for most national AML legislation.

Example: A country adopts FATF's "Risk-Based Approach" to tailor its AML controls.

Challenge: Aligning domestic law with FATF updates while managing industry compliance costs.

Financial Intelligence Unit (FIU) – A government agency that receives, analyzes, and disseminates suspicious transaction reports.

Related terms: SAR, STR, law enforcement liaison.

Explanation: FIUs serve as the central hub for AML data, providing intelligence to investigators and prosecutors.

Example: The FIU of Country X shares a SAR with the national police for a money-laundering probe.

Challenge: Ensuring timely feedback loops to reporting institutions and protecting data confidentiality.

Foreign Direct Investment (FDI) Screening – The review of cross-border investments for AML and national security concerns.

Related terms: investment vetting, beneficial ownership, risk assessment.

Explanation: Authorities assess whether incoming capital may be linked to illicit proceeds.

Example: A sovereign wealth fund's purchase of a domestic manufacturing plant is examined for hidden benefactors.

Challenge: Coordinating between AML and foreign-investment regulators, especially in fast-moving deals.

High-Risk Jurisdiction – A country or territory identified as having weak AML controls or a high level of illicit activity.

Related terms: non-cooperative jurisdiction, sanctions list, risk rating.

Explanation: Transactions involving high-risk jurisdictions often trigger enhanced monitoring or mandatory approvals.

Example: An offshore wire transfer to a jurisdiction on the FATF "gray list" requires senior-management sign-off.

Challenge: Keeping jurisdictional risk ratings up-to-date amid frequent political changes.

Illicit Finance – The movement of funds derived from criminal activity, including money laundering, terrorist financing, and fraud.

Related terms: proceeds of crime, laundering stages, financial crime.

Explanation: Illicit finance aims to conceal the origin, ownership, or destination of illegal proceeds.

Example: A drug cartel uses a chain of shell companies to layer and integrate profits into the legitimate economy.

Challenge: Detecting sophisticated layering techniques that exploit emerging technologies.

KYC (Know Your Customer) – The process of verifying the identity of a client and understanding the nature of their activities.

Related terms: CDD, client onboarding, identity verification.

Explanation: KYC is the foundation of AML compliance; it informs risk rating and ongoing monitoring.

Example: A retail bank collects a passport, proof of address, and a selfie for biometric verification.

Challenge: Balancing robust verification with seamless digital onboarding experiences.

Layering – The second stage of money laundering, where illicit funds are moved through a series of complex transactions to obscure their origin.

Related terms: placement, integration, transaction structuring.

Explanation: Layering often involves multiple jurisdictions, high-frequency trades, or use of virtual assets.

Example: A criminal transfers funds through three offshore accounts, each performing small currency conversions.

Challenge: Detecting subtle patterns amidst high volumes of legitimate activity.

Legal Entity Identifier (LEI) – A unique 20-character alphanumeric code that identifies a legal entity participating in financial transactions.

Related terms: global identifier, entity registration, risk analytics.

Explanation: LEIs facilitate transparency and help regulators trace relationships across the financial system.

Example: A multinational corporation's LEI appears on a trade finance transaction, linking it to its subsidiaries.

Challenge: Ensuring all counterparties maintain up-to-date LEI information.

Money Laundering Reporting Officer (MLRO) – The senior individual within an organization responsible for AML oversight and SAR filing.

Related terms: compliance officer, risk manager, regulatory liaison.

Explanation: The MLRO ensures policies are followed, reviews alerts, and communicates with the FIU.

Example: The MLRO signs off on a SAR after reviewing supporting documentation and approving the filing.

Challenge: Maintaining independence while integrating AML duties into broader risk functions.

Negative News Screening – The process of scanning public sources for adverse information about a client, often using automated tools.

Related terms: adverse media, reputation risk, screening engine.

Explanation: Negative news can indicate emerging risk and prompt re-assessment of a client's risk rating.

Example: An automated platform flags a client's involvement in a recent fraud case, prompting a manual review.

Challenge: Filtering out false positives from legitimate publications and handling language barriers.

Obligation to Report Suspicious Activity (SAR) – A legal requirement for financial institutions to notify the FIU of transactions that appear suspicious.

Related terms: STR, reporting threshold, confidentiality.

Explanation: SARs are the primary tool for law-enforcement agencies to receive early warnings of money-laundering schemes.

Example: A bank files a SAR after a customer makes an unusually large wire transfer to a high-risk jurisdiction without a clear business purpose.

Challenge: Determining when a transaction is truly suspicious versus merely unusual, and protecting reporting staff from retaliation.

Off-Shore Entity – A company incorporated in a jurisdiction different from where it conducts its primary business activities, often for tax or confidentiality purposes.

Related terms: tax haven, shell company, jurisdictional risk.

Explanation: Off-shore entities can be legitimate but are frequently used to conceal ownership or launder proceeds.

Example: A client uses an off-shore trust to hold shares in a domestic real-estate project.

Challenge: Tracing the true owners when documentation is limited or intentionally opaque.

Operational Risk – The risk of loss resulting from inadequate or failed internal processes, people, systems, or external events.

Related terms: process failure, technology risk, compliance breach.

Explanation: In AML investigations, operational risk includes errors in data entry, system outages, or inadequate training that compromise detection.

Example: A data migration error causes a batch of transactions to be excluded from monitoring, allowing a laundering scheme to go undetected.

Challenge: Implementing robust controls while maintaining efficiency.

Politically Exposed Person (PEP) – An individual who holds or has held a prominent public function, and their immediate family members or close associates.

Related terms: senior government official, risk factor, enhanced due diligence.

Explanation: PEPs are considered higher risk due to potential for corruption and abuse of office.

Example: A bank flags a newly opened account by a former minister for EDD, requiring source-of-wealth documentation.

Challenge: Keeping up-to-date with changing political positions and extended networks.

Risk Assessment – The systematic process of identifying, measuring, and prioritizing risks associated with customers, products, services, and geographies.

Related terms: risk matrix, risk appetite, control framework.

Explanation: A risk assessment informs the design of AML controls, monitoring thresholds, and resource allocation.

Example: An institution assigns a high-risk rating to a client dealing in cryptocurrencies from a high-risk jurisdiction.

Challenge: Balancing quantitative data with qualitative insights and avoiding over-reliance on static scoring models.

Sanctions List – A compilation of individuals, entities, and countries subject to trade, financial, or travel restrictions imposed by governments or international bodies.

Related terms: embargo, blocked party, watchlist.

Explanation: Screening against sanctions lists is mandatory to prevent prohibited transactions.

Example: A payment processor blocks a transfer to a bank flagged on the UN sanctions list.

Challenge: Managing frequent updates, reconciling conflicting lists, and handling false matches.

Source-of-Wealth (SOW) Verification – The process of confirming how a client accumulated the assets used in a transaction or held in an account.

Related terms: funds provenance, EDD, wealth statement.

Explanation: SOW verification helps distinguish legitimate wealth from illicit proceeds.

Example: A client provides audited financial statements, tax returns, and inheritance documents to justify a \$5 million deposit.

Challenge: Obtaining reliable documentation, especially from jurisdictions with limited transparency.

Suspicious Activity Report (SAR) Review – The internal analysis performed by the compliance team to decide whether a SAR should be filed.

Related terms: alert triage, MLRO approval, regulatory filing.

Explanation: Review involves assessing the facts, supporting evidence, and legal thresholds.

Example: An analyst compiles transaction logs, client profiles, and media excerpts before recommending SAR filing.

Challenge: Maintaining consistency across reviewers and avoiding bias.

Transaction Monitoring System (TMS) – Software that automatically screens financial transactions against predefined rules and risk scenarios.

Related terms: rule engine, real-time monitoring, alert generation.

Explanation: A TMS processes high volumes of data, applying thresholds, pattern detection, and machine-learning models to flag suspicious activity.

Example: The system raises an alert when a corporate client conducts a series of structured cash deposits just below the reporting limit.

Challenge: Tuning parameters to reduce false positives while preserving detection sensitivity.

Unusual Transaction Pattern – A behavior that deviates from a client’s normal activity profile or industry norms, potentially indicating money laundering.

Related terms: behavioral analytics, baseline profiling, anomaly detection.

Explanation: Detecting unusual patterns requires historical data and statistical modeling.

Example: A low-risk retail client suddenly initiates multiple large international wire transfers to unrelated third parties.

Challenge: Differentiating legitimate business changes from illicit activity, especially for dynamic enterprises.

Virtual Asset Service Provider (VASP) – An entity that conducts activities involving virtual assets, such as cryptocurrency exchanges, wallet providers, or custodians.

Related terms: digital currency, crypto AML, blockchain analysis.

Explanation: VASPs are subject to AML obligations, including KYC, transaction monitoring, and SAR filing.

Example: A crypto exchange implements blockchain tracing tools to detect mixing services used by customers.

Challenge: Rapidly evolving technology, pseudonymous transactions, and regulatory fragmentation.

Watchlist Screening – The process of comparing client and transaction data against curated lists of high-risk individuals or entities.

Related terms: sanctions screening, PEP list, adverse media database.

Explanation: Effective watchlist screening reduces the risk of facilitating illicit activity or breaching sanctions.

Example: A compliance platform automatically flags a new client whose name matches an entry on the OFAC list.

Challenge: Managing false positives caused by common names and ensuring timely updates.

Wire Transfer Monitoring – The surveillance of electronic funds transfers for signs of money laundering, such as rapid movement, layering, or destination to high-risk jurisdictions.

Related terms: SWIFT traffic, transaction tracing, fund flow analysis.

Explanation: Wire transfers are a common channel for moving large sums quickly; monitoring focuses on patterns and counterparties.

Example: A series of outbound wires from a corporate account to multiple offshore banks within a short period triggers an investigation.

Challenge: Balancing privacy concerns with the need for detailed transaction data, and coping with high transaction volumes.

Anti-Bribery and Corruption (ABC) Controls – Policies and procedures aimed at preventing bribery and corrupt practices, often overlapping with AML due to shared risk factors.

Related terms: FCPA, UK Bribery Act, integrity program.

Explanation: ABC controls complement AML by addressing the misuse of funds for illicit influence.

Example: A multinational firm conducts ABC training and integrates bribery risk into its AML risk assessment.

Challenge: Coordinating separate compliance functions and ensuring consistent enforcement across jurisdictions.

Beneficial Ownership Registry – A public or private database that records the natural persons who ultimately own or control legal entities.

Related terms: UBO, transparency initiative, corporate registry.

Explanation: Registries help regulators and businesses verify ownership and assess risk.

Example: A bank queries a national beneficial-ownership register to confirm the ultimate owners of a client corporation.

Challenge: Inconsistent data quality, limited coverage, and privacy restrictions.

Correspondent Banking – A banking relationship where one bank provides services to another, often across borders, facilitating international payments.

Related terms: payment corridor, risk of illicit flow, due diligence.

Explanation: Correspondent banks must assess the AML risk of their partners and monitor the flow of funds through the relationship.

Example: A domestic bank conducts enhanced due diligence on a foreign correspondent bank located in a high-risk jurisdiction.

Challenge: Managing complex networks of indirect exposure and ensuring all counterparties maintain adequate controls.

Customer Risk Rating – A score or classification that reflects the perceived AML risk associated with a client, based on factors such as geography, product usage, and transaction behavior.

Related terms: risk tier, risk matrix, risk profiling.

Explanation: The rating determines the level of monitoring, frequency of reviews, and escalation procedures.

Example: A high-risk rating for a client dealing in precious metals triggers daily transaction reviews.

Challenge: Maintaining dynamic ratings as client behavior changes and avoiding over-reliance on static models.

Data Privacy Compliance – Adherence to regulations governing the collection, storage, and processing of personal data, such as GDPR or CCPA.

Related terms: privacy impact assessment, data minimization, confidentiality.

Explanation: AML investigations must balance the need for detailed data with privacy obligations.

Example: An AML system anonymizes client identifiers when generating aggregate risk reports for senior management.

Challenge: Navigating conflicting requirements between AML (which often mandates extensive data) and privacy laws (which limit data usage).

Electronic Funds Transfer (EFT) – The movement of money between accounts using electronic systems, including ACH, SEPA, and SWIFT.

Related terms: payment network, transaction traceability, funds flow.

Explanation: EFTs are subject to AML monitoring due to their speed and cross-border nature.

Example: An ACH transaction from a small business to a supplier is flagged for unusual frequency.

Challenge: Integrating diverse EFT formats into a unified monitoring platform.

Financial Crime Typology – A classification of common methods and patterns used by criminals to launder money or finance illicit activities.

Related terms: scheme analysis, trend monitoring, risk scenario.

Explanation: Typologies help institutions design rules and controls that target known illicit behaviors.

Example: The “smurfing” typology describes the practice of breaking up large cash amounts into multiple small deposits to evade reporting thresholds.

Challenge: Keeping typologies current as criminals innovate and adapt to new technologies.

Geographic Risk – The assessment of AML risk based on the location of a client, transaction, or business activity, considering factors such as political stability, regulatory quality, and illicit activity prevalence.

Related terms: jurisdictional rating, high-risk country, regional compliance.

Explanation: Geographic risk informs both client onboarding and transaction monitoring thresholds.

Example: A client operating in a country identified as a FATF “high-risk jurisdiction” requires EDD and ongoing monitoring.

Challenge: Harmonizing geographic risk assessments across multiple regulatory frameworks.

High-Value Goods Trade – The movement of expensive commodities such as art, jewelry, precious metals, and luxury vehicles, which can be used to conceal illicit proceeds.

Related terms: trade-based money laundering (TBML), valuation risk, customs compliance.

Explanation: AML controls for high-value goods include verification of invoices, ownership, and shipping documents.

Example: A dealer purchases a rare painting for cash and resells it shortly thereafter, prompting a TBML investigation.

Challenge: Valuing unique items, detecting over- or under-invoicing, and coordinating with customs authorities.

Identity Verification – The process of confirming that a person presenting identification documents is indeed the rightful holder, often using biometric or electronic methods.

Related terms: KYC, document authentication, e-KYC.

Explanation: Accurate identity verification reduces the risk of synthetic identities being used for laundering.

Example: A bank uses facial recognition to match a selfie with the passport photo supplied during onboarding.

Challenge: Preventing deep-fake attacks and ensuring accessibility for customers lacking conventional ID.

International Sanctions Compliance – The adherence to sanctions regimes imposed by bodies such as the United Nations, European Union, or United States.

Related terms: export controls, blocked party, embargo.

Explanation: Institutions must screen customers, transactions, and assets against multiple sanction lists to avoid prohibited dealings.

Example: A trade finance department blocks a letter of credit where the beneficiary is listed on the EU sanctions list.

Challenge: Managing overlapping and sometimes contradictory sanctions, and dealing with secondary sanctions risk.

Joint Account Monitoring – The oversight of accounts owned by multiple individuals, which can increase complexity in assessing ownership and transaction intent.

Related terms: co-ownership, beneficial ownership, risk sharing.

Explanation: Joint accounts require additional scrutiny to ensure that all parties are vetted and that the account is not used to mask illicit activity.

Example: A joint checking account held by two unrelated individuals is examined when one party initiates a large outbound transfer.

Challenge: Determining the source of funds and the purpose of transactions when multiple owners are involved.

Know-Your-Customer (KYC) Refresh – The periodic updating of client information to ensure that records remain accurate and risk assessments stay current.

Related terms: re-verification, client review, data maintenance.

Explanation: KYC refreshes are triggered by regulatory timelines, material changes in client activity, or internal risk triggers.

Example: A bank conducts a KYC refresh for all high-risk corporate clients every twelve months, requesting updated board member lists and audited financials.

Challenge: Managing client fatigue and ensuring timely receipt of updated documentation.

Liquidity Risk – The danger that a financial institution cannot meet its short-term cash obligations, which can be exacerbated by illicit fund movements that obscure true cash flow.

Related terms: cash flow analysis, funds availability, stress testing.

Explanation: Money-laundering schemes can create artificial liquidity, masking underlying financial weakness.

Example: A bank experiences a sudden surge in cash deposits from a client later identified as a money-laundering conduit, leading to liquidity strain when the funds are withdrawn.

Challenge: Distinguishing legitimate liquidity spikes from laundering activity.

Money-Laundering Stages – The three-phase model of placement, layering, and integration that describes how illicit proceeds are introduced, concealed, and re-entered into the economy.

Related terms: placement, layering, integration.

Explanation: Understanding each stage helps investigators target controls and identify where a transaction fits within a laundering scheme.

Example: A cash-intensive retailer deposits large sums just under the reporting threshold (placement), then transfers the funds through multiple offshore accounts (layering), finally using the money to purchase real estate (integration).

Challenge: Detecting early-stage placement activities that are deliberately designed to blend with legitimate cash flows.

Non-Financial Transaction Reporting (NFTR) – The requirement for non-financial entities, such as real-estate agents or dealers in high-value goods, to report suspicious transactions.

Related terms: reporting obligation, DNFBP, SAR.

Explanation: NFTR extends AML obligations beyond banks, recognizing that money can be laundered through various channels.

Example: A jeweler files an SAR after a customer pays cash for a \$500,000 diamond with no clear source of funds.

Challenge: Providing adequate training and resources to non-financial businesses that may lack sophisticated compliance infrastructure.

Off-Shore Banking – Banking services provided by institutions located in jurisdictions that are typically outside the client's home country, often associated with tax advantages or secrecy.

Related terms: tax haven, secrecy jurisdiction, risk assessment.

Explanation: Off-shore banks can be used for legitimate international business but also for obscuring illicit proceeds.

Example: A client maintains an account with an off-shore bank in a jurisdiction flagged by FATF for weak AML controls.

Challenge: Conducting thorough due diligence on off-shore banks, especially when information is limited.

On-Boarding Risk Assessment – The initial evaluation of a prospective client's AML risk before establishing a business relationship.

Related terms: KYC, risk rating, client acceptance.

Explanation: The assessment considers factors such as industry, geography, transaction type, and ownership structure.

Example: A fintech platform uses an automated risk-scoring engine to decide whether to accept a high-frequency cryptocurrency trader.

Challenge: Balancing rapid onboarding for digital services with comprehensive risk evaluation.

Operational Red Flag – An indicator within an organization's processes that suggests a potential weakness or failure that could be exploited for money laundering.

Related terms: control deficiency, process audit, risk indicator.

Explanation: Red flags can be technical (e.g., system downtime) or procedural (e.g., lack of sign-off).

Example: An AML analyst discovers that a batch of alerts was automatically cleared due to a misconfigured rule, creating an operational red flag.

Challenge: Identifying and remediating red flags before they lead to regulatory breaches.

Payment Service Provider (PSP) – A company that enables merchants and consumers to make electronic payments, often through online platforms.

Related terms: e-money, gateway, AML controls.

Explanation: PSPs are subject to AML obligations, particularly when facilitating cross-border or high-value transactions.

Example: A PSP implements real-time monitoring for large transfers to jurisdictions with elevated money-laundering risk.

Challenge: Scaling AML controls while maintaining low friction for end-users.

Politically Exposed Entity (PEE) – A corporate or legal entity that is owned, controlled, or significantly

influenced by a PEP.

Related terms: PEP, beneficial ownership, risk factor.

Explanation: PEEs inherit the elevated risk associated with their politically exposed owners and therefore require enhanced scrutiny.

Example: A state-owned oil company is classified as a PEE, prompting mandatory EDD for any new banking relationship.

Challenge: Mapping complex ownership structures to identify indirect PEP influence.

Real-Time Transaction Monitoring – The immediate analysis of transactions as they occur, allowing for swift detection and response to suspicious activity.

Related terms: instant alerts, stream processing, risk engine.

Explanation: Real-time monitoring is essential for high-velocity environments such as payments, trading, and cryptocurrency exchanges.

Example: A system blocks a wire transfer in seconds when it matches a high-risk pattern involving a sanctioned country.

Challenge: Maintaining performance and accuracy at scale, and managing the operational impact of instant alerts.

Regulatory Examination – An inspection or audit conducted by a supervisory authority to assess an institution's compliance with AML laws.

Related terms: supervisory review, audit finding, corrective action.

Explanation: Examinations evaluate policies, procedures, training, and the effectiveness of monitoring systems.

Example: A central bank's AML examination uncovers gaps in the institution's PEP screening process, leading to a remediation plan.

Challenge: Preparing for examinations while maintaining day-to-day operations, and addressing findings promptly.

Risk-Based Approach (RBA) – A methodology that allocates resources and controls proportionate to the level of AML risk identified.

Related terms: risk assessment, risk matrix, control prioritization.

Explanation: The RBA enables institutions to focus on higher-risk customers, products, and geographies while applying lighter controls elsewhere.

Example: A bank applies stringent monitoring to private banking clients dealing in high-value assets, but adopts a simplified approach for low-risk retail accounts.

Challenge: Accurately quantifying risk and avoiding under-estimation that could lead to regulatory breaches.

Sanctions Evasion – The deliberate act of circumventing sanctions through indirect means, such as using third-party intermediaries or complex corporate structures.

Related terms: secondary sanctions, blocked party, re-routing.

Explanation: Detecting evasion requires deep analysis of transaction chains and ownership links.

Example: Funds are transferred through a non-sanctioned bank to ultimately reach a sanctioned entity,

concealed by multiple layers of intermediaries.

Challenge: Keeping abreast of evolving evasion tactics and ensuring that screening systems capture indirect connections.

Sector-Specific AML Controls – Tailored procedures and monitoring rules designed for particular industries, such as gambling, real estate, or precious metals.

Related terms: industry risk, customized monitoring, regulatory guidance.

Explanation: Different sectors face unique money-laundering threats that require specialized attention.

Example: A casino implements real-time monitoring of chip purchases and cashouts to detect structuring.

Challenge: Developing and maintaining sector-specific controls without over-complicating the compliance framework.

Suspicious Transaction Indicator (STI) – A factor or pattern that suggests a transaction may be linked to money laundering or other illicit activity.

Related terms: red flag, alert trigger, risk indicator.

Explanation: STIs are used to configure monitoring rules and to train analysts on what to look for.

Example: Repeated transfers just below the \$10,000 reporting threshold constitute an STI known as “smurfing.”

Challenge: Updating STIs in response to emerging typologies while avoiding excessive false alerts.

Third-Party Risk Management – The process of assessing and monitoring the AML compliance of vendors, agents, and other external partners.

Related terms: due diligence, contractual clause, ongoing monitoring.

Explanation: Institutions must ensure that third parties do not become conduits for laundering.

Example: A bank conducts a questionnaire on AML policies before engaging a correspondent bank in a new region.

Challenge: Gathering reliable information from third parties and maintaining oversight over long-term relationships.

Transaction Structuring – The practice of breaking up a large transaction into smaller amounts to avoid detection or reporting thresholds.

Related terms: smurfing, threshold evasion, pattern detection.

Explanation: Structuring is a common technique used during the placement stage of money laundering.

Example: A client makes multiple cash deposits of \$9,900 each over several days to stay below the \$10,000 reporting limit.

Challenge: Detecting dispersed patterns across accounts and time periods, especially when the client uses multiple branches.

Unclaimed Funds Investigation – The inquiry into dormant or abandoned accounts that may be linked to illicit activity.

Related terms: inactive account, escheatment, forensic review.

Explanation: Unclaimed funds can be a source of hidden money-laundering proceeds if the original owner is unknown.

Example: A bank reviews an old offshore account with large balances that have not been accessed for years,

uncovering a possible laundering scheme.

Challenge: Balancing the need for investigation with privacy considerations and regulatory reporting timelines.

Virtual Asset Transaction Monitoring – The surveillance of cryptocurrency and other digital-asset movements for signs of money-laundering, using blockchain analytics and pattern recognition.

Related terms: blockchain explorer, address clustering, crypto AML.

Explanation: Monitoring virtual assets requires understanding of on-chain data, wallet behavior, and exchange interactions.

Example: A transaction from a wallet associated with a known darknet marketplace to a fiat-off-ramp service raises an alert.

Challenge: De-anonymizing pseudonymous addresses, coping with rapid transaction speeds, and integrating on-chain data with traditional AML systems.

Watch-List Management – The ongoing process of maintaining, updating, and applying lists of high-risk individuals and entities for screening purposes.

Related terms: sanctions list, PEP database, adverse media feed.

Explanation: Effective watch-list management ensures that new risks are promptly incorporated and obsolete entries are removed.

Example: A compliance team schedules weekly updates to the OFAC list and validates matches through manual review.

Challenge: Managing data quality, handling name variations, and preventing over-blocking of legitimate customers.

Whistleblower Reporting – The submission of information by an insider regarding potential AML violations or misconduct.

Related terms: internal disclosure, confidential hotline, protective measures.

Explanation: Whistleblower programs can provide valuable leads for investigations and help uncover hidden schemes.

Example: An employee reports that a senior manager is authorizing suspicious cash deposits for a client with no legitimate business purpose.

Challenge: Ensuring anonymity, protecting reporters from retaliation, and investigating claims objectively.

Yield-Enhancement Schemes – Investment structures that promise high returns, often used to attract illicit funds that are then layered and integrated.

Related terms: investment fraud, high-return product, risk indicator.

Explanation: These schemes can be legitimate but are also attractive for laundering because of the rapid turnover of funds.

Example: A hedge fund offers a “guaranteed” 15