Risks & Methods

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

HOW ILLICIT VALUE MOVES

Placement — Introduce proceeds → **Layering** — Obscure the trail → **Integration** — Apparent legitimacy

01 Money laundering and terrorist financing risks

The laundering cycle

- **Money laundering** conceals the criminal origin of property. A **predicate offense** generates the proceeds; examples include fraud, drug trafficking, corruption and criminal tax evasion.
- **Placement** introduces illicit proceeds into the financial system, such as cash deposits or purchases of monetary instruments. **Layering** obscures the trail through transfers, conversions and complex transactions.
- **Integration** returns apparently legitimate value to the offender through assets, investments or business income. Stages can overlap; classify the purpose of the activity rather than the payment instrument alone.
- **Tax evasion** involves unlawful nonpayment or concealment. **Tax avoidance** uses tax arrangements to reduce liability; its legality depends on applicable rules and substance.
- **Economic and social harm** includes distorted competition, weaker legitimate businesses, lost tax revenue, corruption and reduced financial confidence. Illicit capital flows can destabilize markets and discourage legitimate investment.

Terrorist and proliferation financing

- **Terrorist financing** can use legitimate income, donations or criminal proceeds. Small amounts may fund harmful activity; focus on destination, purpose, relationships and patterns as well as value.
- **Raise, move, store, use** describes a financing lifecycle. Cash couriers, informal transfers, trade, online fundraising and virtual assets can move value through different channels.
- **Proliferation financing** supports weapons of mass destruction and related delivery systems. Review sanctioned parties, procurement networks, end users and suspicious trade routes.
- **Dual-use goods** have civilian and military applications. Their presence calls for end-use and export-control analysis; an ordinary commercial description does not resolve the risk.

Risks & Methods

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

HOW ILLICIT VALUE MOVES

Placement — Introduce proceeds → **Layering** — Obscure the trail → **Integration** — Apparent legitimacy

Nonprofits and charitable fundraising

- **Nonprofit organizations (NPOs)** can be exploited through diverted donations, sham projects or compromised partners. Legitimate charities and humanitarian operations should be assessed individually rather than presumed high risk.
- **Risk indicators** include unexplained cash withdrawals, opaque beneficiaries, payments inconsistent with the mission and transfers to sanctioned parties. Conflict-zone operations require context and safeguards, not an automatic finding of wrongdoing.
- **Proportionate controls** establish governance, purpose, funding sources, delivery partners and intended beneficiaries. Review how funds reach their stated end use and investigate unexplained diversions.

Cash, structuring and funnel activity

- **Structuring** deliberately splits transactions to evade reporting or recordkeeping. Aggregate related activity across accounts, branches, people and time; a below-threshold amount alone does not prove evasion.
- **Smurfing** uses multiple people to fragment transactions. **Microstructuring** uses many small transactions, sometimes followed by foreign ATM withdrawals. Repeated monetary-instrument purchases can serve the same concealment purpose.
- **Funnel accounts** collect deposits from dispersed locations and rapidly move or withdraw funds elsewhere. Pass-through activity, low retained balances and unrelated counterparties warrant comparison with expected business.
- **Cash-intensive businesses** can mix illicit receipts with genuine sales. Privately owned ATMs can dispense illicit cash while settlement creates apparently legitimate bank credits; understand cash suppliers and replenishment.

Entities that obscure ownership

- **Shell companies** generally have little substantive business activity; **front companies** conduct legitimate business that can conceal or commingle criminal proceeds. Neither legal form alone proves wrongdoing.
- **Nominee directors or shareholders** act for someone else. Trace through nominees, holding companies and offshore structures to the natural persons who ultimately own or control the customer.
- **Bearer shares** allow ownership to follow possession, weakening transparency where permitted. Unexplained layers, secrecy, implausible wealth and refusal to identify controllers increase risk.
- **Private investment companies** and international business corporations may hold legitimate assets. Assess economic purpose, actual activity, beneficial ownership and funding rather than relying on a prestigious intermediary.

Risks & Methods

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

HOW ILLICIT VALUE MOVES

Placement — Introduce proceeds → **Layering** — Obscure the trail → **Integration** — Apparent legitimacy

Trade and the Black Market Peso Exchange

- **Trade-based money laundering** transfers value through manipulated trade. Methods include over- or under-invoicing, multiple invoicing, short or excess shipments, misdescription and **phantom shipping**.
- **Value direction:** over-invoicing moves extra value from buyer to seller; under-invoicing gives the buyer goods worth more than the payment. Compare price, quantity and quality together.
- **Trade red flags** include goods unrelated to the business, unexplained third-party payments, inconsistent invoices and shipping records, abrupt volume changes and uneconomic transshipment routes.
- **Black Market Peso Exchange (BMPE)** links criminal foreign-currency proceeds to importers needing that currency. Goods purchases and local-currency settlement can transfer value without a direct criminal-to-owner wire.

Payments, remittances and prepaid value

- **Money services businesses (MSBs)** may transmit money, exchange currencies, cash checks or issue monetary instruments. Agent networks, cash access and cross-border speed require suitable oversight and monitoring.
- **MSB indicators** include repeated visits to multiple agents, reused identity documents, unexplained same-value incoming and outgoing transfers, and reluctance to identify beneficiaries. Review sender-recipient networks.
- **Open-loop prepaid cards** work across participating merchants; reloadability, cash loading, transferability and ATM access can increase risk. Monitor linked cards, loading sources, users and redemption locations.
- **P2P and instant payments** combine fast movement with potentially limited counterparty information. Apply identity checks, sanctions controls, meaningful limits and monitoring before launch.
- **Crowdfunding and e-commerce** warrant review where projects open, fully fund and close rapidly, donors and beneficiaries are linked, prices are implausible, or refunds move value to different parties.
- **Hawala and other informal value transfer systems** rely on intermediaries and later settlement, potentially through trade. Value can move without the same funds crossing borders; assess licensing, records and actual activity.

Insurance and lending

- **Cash-value life insurance, annuities and investment-linked products** can store and transfer value. Examine premium sources, policy ownership, beneficiaries and the ability to borrow or withdraw funds.
- **Insurance indicators** include unexplained third-party premiums, overpayments followed by refunds, frequent policy switching, early surrender despite penalties and payouts to unrelated people.

Risks & Methods

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

HOW ILLICIT VALUE MOVES

Placement
Introduce proceeds

→

Layering
Obscure the trail

→

Integration
Apparent legitimacy

- **Free-look provisions** permit cancellation within a defined period. Criminals may seek an insurer-issued refund that disguises the original payment source; trace refunds to the actual funder.
- **Loan-back schemes** borrow against assets or deposits containing illicit wealth, then present loan proceeds as legitimate. Unexplained guarantors, opaque borrowers and repayments inconsistent with income warrant review.

Securities and capital markets

- **Securities markets** offer liquidity, speed, complex products and intermediated ownership. Review funding, securities transfers and withdrawals alongside trading, including account use inconsistent with investment goals.
- **Physical certificates** and **free-of-payment transfers** can move securities without a visible cash purchase. Establish provenance, beneficial ownership, transfer purpose and links between counterparties.
- **Matched or wash trades** may manufacture activity or disguise control. **Reverse-flip trades** can repeatedly allocate gains to one party and losses to another, transferring value despite little net position change.
- **Market abuse** includes insider dealing and price manipulation. Sudden promotion or price spikes in illiquid, low-priced securities, followed by sales and cash-out, warrant coordinated fraud and AML review.

Casinos, online gambling and gaming

- **Minimal-play laundering** converts cash or chips into casino checks or transfers after little genuine gambling. Look for pooled chips, third-party payouts and activity across tables, patrons or accounts.
- **Chip dumping** deliberately loses value to a cooperating player. Coordinated betting and player-to-player transfers can move funds while making the outcome resemble gambling proceeds.
- **Online gambling** adds remote identity and location risks. Review linked accounts, devices, IP addresses, payment sources and rapid deposit-withdrawal patterns; licensing does not eliminate criminal misuse.
- **Gaming assets** can carry financial crime risk when items or tokens can be transferred and converted into real money. Distinguish cash-out capability from purely recreational use.

Real estate and professional gatekeepers

- **Real estate** can store large amounts of value. Warning signs include hidden purchasers, nominees, unexplained third-party funds, rapid resale, implausible prices and wealth inconsistent with the purchase.
- **Gatekeepers** include lawyers, notaries, accountants and trust and company service providers. Company formation, asset management, client accounts and property transactions can give illicit funds professional legitimacy.

Risks & Methods

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

HOW ILLICIT VALUE MOVES

Placement — Introduce proceeds → **Layering** — Obscure the trail → **Integration** — Apparent legitimacy

- **Client or trust accounts** should match a genuine professional service. Unexplained pass-through transfers, cash withdrawals, unusual fees and payments unrelated to the engagement merit review.
- **Professional relationships** do not replace due diligence. Criminals may build trust through legitimate engagements before introducing questionable work; confirm authority, ownership, purpose and funding.

High-value goods and criminal supply chains

- **Precious metals and stones** concentrate value in portable, convertible form. Scrutinize unclear provenance, cash-heavy purchases, unknown payers and transactions inconsistent with the dealer or customer.
- **Art and antiquities** combine subjective valuation, intermediaries and private sales. Review beneficial owners, provenance, source of funds, storage in freeports and unexplained price changes or third-party payments.
- **Wildlife trafficking and illegal logging** may use legitimate trade firms, false documentation and corrupt officials. Compare goods, permits, routes, counterparties and financial flows with the stated business.
- **Synthetic opioid supply chains** may involve chemical importers, couriers and online sales. Unexplained changes in chemical trade, parcel activity and payments across unrelated firms are contextual indicators.
- **Human trafficking** involves exploitation; **migrant smuggling** facilitates unlawful entry. Trafficking indicators can include scattered cash deposits, rapid withdrawals, linked lodging or advertising payments and third-party control of accounts.

Cyber fraud, mules and virtual assets

- **Phishing** tricks users into revealing data or opening malicious links. **Spear phishing** targets specific people; **vishing** uses voice and **smishing** uses text messages. **Spoofing** falsifies an apparent sender or identity.
- **Business email compromise** redirects payments using impersonation or compromised accounts. Verify changed payment instructions through a trusted independent channel; coordinate fraud response with AML analysis.
- **Money mules** receive and forward criminal funds, knowingly or unknowingly. Look for rapid turnover, inconsistent purpose, shared devices or contact details and common beneficiaries across unrelated accounts.
- **Virtual assets** offer global, rapid transfers. Public blockchains can preserve traceable records, while pseudonyms, mixers, chain-hopping and self-hosted wallets can complicate attribution.
- **Virtual asset service providers (VASPs)** need risk-based identity, monitoring, sanctions and applicable transfer-information controls. A wallet address or crypto-to-fiat conversion alone does not establish illicit activity.

Standards & Frameworks

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

STANDARDS AND IMPLEMENTATION

- **FATF** — Global standards
- **FSRBs** — Regional support
- **National law** — Binding duties
- **FIUs** — Financial intelligence

02 International standards and legal frameworks

FATF standards and national systems

- **Financial Action Task Force (FATF)** sets international AML, counter-terrorist financing and counter-proliferation financing standards. Countries implement them through domestic legal and operational frameworks.
- **The 40 Recommendations** address risk assessment, criminalization, confiscation, preventive controls, beneficial ownership, supervision, financial intelligence and international cooperation.
- **Risk-based approach** means identifying, assessing and understanding exposure, then applying proportionate measures. Higher risk calls for stronger controls; simplified measures require a justified lower-risk basis.
- **FATF-style regional bodies (FSRBs)** support implementation through mutual evaluations, follow-up, regional typologies, training and technical assistance. They do not replace national supervisors or prosecutors.

Mutual evaluations and country risk

- **Mutual evaluations** are peer reviews of national systems. **Technical compliance** asks whether required laws and institutions exist; **effectiveness** asks whether the system achieves results.
- **The 11 Immediate Outcomes** cover risk understanding, cooperation, supervision, preventive measures, ownership transparency, financial intelligence, ML prosecution, confiscation, TF prosecution, TF prevention and proliferation sanctions.
- **Follow-up** tracks remediation of deficiencies. A technical re-rating does not itself demonstrate improved operational effectiveness; assess both implementation and outcomes.
- **Increased monitoring**, often called the grey list, identifies jurisdictions committed to action plans. FATF does not automatically call for EDD on all such relationships; incorporate the information into risk analysis.
- **High-risk jurisdictions subject to a call for action** attract FATF calls for EDD and, in the most serious cases, countermeasures. Distinguish these statements from sanctions and domestic legal requirements.

Standards & Frameworks

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

STANDARDS AND IMPLEMENTATION

- **FATF** — Global standards
- **FSRBs** — Regional support
- **National law** — Binding duties
- **FIUs** — Financial intelligence

FIUs, Egmont and public authorities

- **Financial intelligence units (FIUs)** receive suspicious reports and other relevant information, analyze it and disseminate financial intelligence to competent authorities. Institutional powers differ by country.
- **Egmont Group** connects FIUs for secure information exchange, capability development and cooperation. Operational autonomy, confidentiality, trust and reciprocity support effective exchange.
- **FIU requests** should explain the purpose and provide complete, factual context. Respect permitted use, dissemination restrictions and required consent; use authorized secure channels.
- **Supervisors** assess compliance and take regulatory action; **law enforcement** investigates crime; **prosecutors and courts** pursue and adjudicate cases. FATF standards and FIU intelligence do not themselves establish guilt.

Basel and Wolfsberg guidance

- **Basel KYC elements** are customer acceptance, customer identification, ongoing monitoring and risk management. Weak KYC creates legal, reputational, operational and concentration risks.
- **Wolfsberg Group** provides an industry perspective on financial crime controls, including private banking, correspondent banking, payment transparency and trade finance. Guidance complements applicable law.
- **Private banking principles** emphasize understood ownership, legitimate source of wealth and funds, appropriate independent approval and ongoing review. Relationship-manager familiarity does not replace verification.
- **Correspondent principles** call for risk-sensitive due diligence, assessment of ownership and controls, and scrutiny of downstream access. Geographic membership in a standard-setting body is not a low-risk guarantee.

USA PATRIOT Act: key distinctions

- **Section 311** authorizes special measures for designated primary money-laundering concerns. Measures may require extra records or restrict correspondent access; check the measure actually imposed.
- **Section 312** addresses due diligence for covered foreign correspondent and private banking accounts, with EDD in specified circumstances. Assess the account, institution, customers served and relevant jurisdiction.
- **Sections 313 and 319(b)** underpin foreign shell-bank restrictions and correspondent-account records, including foreign-bank ownership and a US agent for service of process, subject to applicable exceptions.
- **Section 319(a)** supports forfeiture from a foreign bank's US interbank account corresponding to illicit funds deposited abroad. **Section 319(b)** concerns records and subpoena powers; do not interchange them.

Standards & Frameworks

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

STANDARDS AND IMPLEMENTATION

- **FATF** — Global standards
- **FSRBs** — Regional support
- **National law** — Binding duties
- **FIUs** — Financial intelligence

Foreign correspondent safeguards

- **Foreign shell banks** lack physical presence in any country. Covered US institutions must prevent prohibited direct or indirect access; a regulated-affiliate exception has specific conditions.
- **Correspondent due diligence** examines the respondent's license, supervision, reputation, ownership, management, business and AML controls. Certain licenses, jurisdictions or access arrangements require extra scrutiny.
- **Payable-through accounts** allow a respondent's customers to transact directly. Understand who has access and whether the respondent identifies and monitors those users and can supply relevant information.
- **Foreign-bank record requests** can reach records outside the US when statutory conditions are met. Escalate subpoenas and noncompliance risks to counsel; US correspondent access can be affected.

European AML framework

- **EU directives** require national implementation. Local laws can add requirements; an **EU regulation** is directly applicable according to its terms. Determine which obligations apply to the entity and activity.
- **Fourth AML Directive** strengthened risk-based controls, beneficial ownership transparency and PEP measures. **Fifth AML Directive** extended coverage to specified virtual-currency services and strengthened transparency and high-risk-country controls.
- **EU criminal-law measures** harmonize aspects of money-laundering offenses and liability. The AML reform package separately combines a private-sector rulebook, national-system provisions and the **AMLA** supervisory authority.
- **High-risk third-country relationships** can require additional information, source-of-funds and wealth checks, transaction rationale, senior approval and enhanced monitoring. Apply the governing requirements and implementation timetable.

Sanctions scope and US nexus

- **Economic sanctions** pursue foreign-policy and national-security objectives by restricting dealings, assets or trade. Measures can target countries, persons, entities, sectors or specific activities.
- **OFAC** administers US sanctions. Coverage includes US citizens and permanent residents worldwide, persons within the US, US-incorporated entities and their foreign branches; some programs also cover foreign subsidiaries.
- **A US nexus**, including processing through a US bank, can create sanctions exposure for a cross-border transaction. Non-US parties can also face restrictions involving evasion or causing a US violation.

Standards & Frameworks / Programs & Controls

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

CONTROL THE CUSTOMER LIFECYCLE

Assess — Risk and appetite → **Identify** — Customer and owners → **Monitor** — Activity and changes → **Respond** — Mitigate and report

- **Secondary sanctions** can expose non-US parties to consequences for specified conduct even without a US nexus. Assess the particular program, activity and authorization rather than assuming currency alone determines scope.
- **UN sanctions** are implemented through member-state mechanisms. An arms embargo, asset freeze and travel ban have different effects; AML suspicion and sanctions designation are separate concepts.

03 AML compliance programs and controls

Governance and the three lines

- **The board** approves policy and oversees program effectiveness, risk appetite and remediation. **Senior management** implements the program and supplies authority, staff, systems and funding.
- **First line:** business teams own risks and operate controls. **Second line:** compliance and risk functions set standards, advise, challenge and monitor. **Third line:** independent audit provides assurance.
- **The AML officer or MLRO** coordinates day-to-day compliance and escalation with adequate stature and access to leadership. Outsourcing tasks does not transfer the institution's accountability.
- **Compliance culture** aligns incentives, information sharing and escalation with legal duties. Profit, customer prestige or personal relationships must not justify ignored concerns or undocumented exceptions.

Enterprise risk assessment and appetite

- **Enterprise-wide risk assessment (EWRA)** maps customers, products, services, transaction activity, delivery channels and geographies across all business lines and entities.
- **Inherent risk** exists before controls. Evaluate control design and operating effectiveness to estimate **residual risk**; a checklist or numerical score cannot substitute for reasoned judgment.
- **Risk appetite** defines acceptable exposure through qualitative boundaries and quantitative limits. Embed limits in onboarding, products, reporting and escalation; appetite cannot authorize prohibited conduct.
- **Refresh triggers** include mergers, acquisitions, new products, technologies, customer segments, geographic expansion, external threats and material control failures. Periodic review alone may miss change.
- **New-product approval** includes compliance early, before launch. Assess end users, counterparties, speed, anonymity, cross-border reach and control readiness; apply effective interim mitigation where appropriate.

Programs & Controls

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

CONTROL THE CUSTOMER LIFECYCLE

Assess — Risk and appetite → **Identify** — Customer and owners → **Monitor** — Activity and changes → **Respond** — Mitigate and report

Program design and group-wide controls

- **Core controls** include written policies, a responsible AML officer, risk-based CDD, monitoring and reporting, training, recordkeeping and independent testing. Translate laws into procedures, systems and assigned tasks.
- **Group-wide programs** establish a common baseline with local implementation. Apply home-country requirements to foreign branches and majority-owned subsidiaries where host-country law permits.
- **Conflicting local requirements** need documented legal analysis, escalation and additional risk mitigation. Headquarters policy does not override privacy, bank secrecy or other local law.
- **Cross-functional coordination** links AML, sanctions, fraud, cybersecurity, legal, HR and business teams through shared risk information, clear handoffs, common metrics and suitable access controls.

Customer identification and lifecycle

- **CDD** identifies and verifies the customer and beneficial owners, establishes purpose and intended activity, and supports ongoing monitoring. It applies throughout the relationship.
- **Customer acceptance** defines prohibited relationships, required information, risk categories and approvals. Verify persons acting for a customer and document their authority, including powers of attorney.
- **A useful profile** records occupation or business, expected amounts and frequency, funding sources, counterparties, jurisdictions and products. Compare actual activity with this profile and relevant peers.
- **Remote onboarding** needs reliable identity evidence and controls against impersonation or stolen documents. Device, address and IP inconsistencies are prompts for investigation, not conclusive proof.
- **Refresh CDD** periodically according to risk and when ownership, PEP status, business scope, geography or adverse information changes. If required CDD cannot be completed, consider refusal or exit and whether reporting is warranted.

Beneficial ownership, trusts and reliance

- **Beneficial owners** are the natural persons who ultimately own or control a customer or on whose behalf activity occurs. Legal title, signatory status and beneficial ownership are different roles.
- **Legal entities** require an understood ownership and control structure. Corroborate registries and customer declarations with reliable evidence; a nominee or opaque corporate chain does not resolve ownership.

Programs & Controls

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

CONTROL THE CUSTOMER LIFECYCLE

Assess — Risk and appetite → **Identify** — Customer and owners → **Monitor** — Activity and changes → **Respond** — Mitigate and report

- **Trusts** require identification of relevant settlors, trustees, protectors, beneficiaries or beneficiary classes, and other ultimate controllers. Understand purpose, authority and source of assets.
- **Third-party reliance** requires legally permitted arrangements and suitable access to identification and verification information. Introducers and regulated intermediaries do not automatically remove the bank's responsibilities.

Enhanced due diligence and PEPs

- **EDD** adds depth and scrutiny for higher risk: corroborated background, ownership and control, source of wealth and funds, transaction rationale, appropriate approval and more intensive monitoring.
- **Source of wealth** explains how overall wealth was accumulated. **Source of funds** explains the origin of the money used for a particular relationship or transaction; evidence should fit the explanation.
- **Politically exposed persons (PEPs)** hold or have held prominent public functions. Family members and close associates can share corruption exposure; screening must detect changes after onboarding.
- **Foreign PEP controls** include appropriate senior-management approval, reasonable measures to establish wealth and funds, and enhanced ongoing monitoring. Domestic and international-organization PEP treatment follows applicable risk-based rules.
- **PEP status** does not imply criminality or require automatic rejection. Leaving office does not automatically remove risk; reassess influence, role, connections and the applicable requirements.
- **Public procurement and defense contracts** can create corruption exposure through agents, commissions and opaque suppliers. Review unexplained wealth, disproportionate fees, unusual billing and ties to decision-makers.

Correspondent and private banking controls

- **Correspondent banking** supplies banking services to another institution, the respondent. The correspondent may have limited visibility into underlying customers, creating reliance and transparency risk.
- **Nested relationships** give downstream institutions access through the respondent. Understand the institutions served, their locations, business mix, volumes and controls; investigate activity outside the agreement.
- **Private banking** combines wealth, complex structures and close personal relationships. Independent approval, understood beneficial ownership, reliable funding evidence and periodic review reduce conflicts of interest.
- **Concentration accounts** aggregate funds for internal processing. Preserve a traceable link to customer-level transactions and prevent customer-directed use that obscures identity or the audit trail.

Programs & Controls

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

CONTROL THE CUSTOMER LIFECYCLE

- **Assess** — Risk and appetite
- → **Identify** — Customer and owners
- → **Monitor** — Activity and changes
- → **Respond** — Mitigate and report

Transaction monitoring and data quality

- **Transaction monitoring** compares activity with expected behavior, typologies and risk. Combine thresholds, velocity, historical trends, peer comparisons and linked-account analysis; persistent abnormal activity may evade change-only rules.
- **Data quality** is fundamental: reconcile feeds, amounts, currencies, identifiers and customer links. Missing products, rejected records or broken interfaces can create silent monitoring gaps.
- **Implementation testing** includes system integration and user acceptance before deployment. Validate scenarios against actual exposure and document configuration, approvals and changes.
- **Calibration** assesses both alert quality and missed risk. **Below-the-line testing** samples activity below thresholds to detect gaps; staffing pressure alone is not a sound reason to suppress alerts.
- **Machine learning** can recognize patterns and adapt as data changes. Validate accuracy, bias, explainability, drift and governance; models still need human oversight and reliable inputs.

Sanctions screening and disposition

- **Screening** covers relevant customers, owners, counterparties and transaction information against applicable lists. Rescreen promptly after list or customer changes; a fixed quarterly cycle can leave exposure.
- **A potential match** requires prompt review using identifiers, aliases, addresses and ownership. A similar name or country reference alone does not establish a true match; document release or escalation.
- **OFAC's 50 Percent Rule** can block entities owned directly or indirectly, 50% or more in aggregate, by blocked persons even when the entity is unlisted. Apply the ownership rules through relevant corporate chains.
- **Blocking** freezes property or interests subject to blocking rules; **rejecting** declines a prohibited transaction without freezing it under a blocking requirement. Determine the legal program and report as required.
- **General and specific licenses** can authorize defined activity subject to conditions. Internal approvals cannot replace legal authorization; verify scope before processing.

Programs & Controls

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

CONTROL THE CUSTOMER LIFECYCLE

Assess Risk and appetite → **Identify** Customer and owners → **Monitor** Activity and changes → **Respond** Mitigate and report

Payment transparency and sanctions evasion

- **Payment transparency** requires accurate, complete originator and beneficiary data under applicable rules. Request missing information and apply risk-based hold, escalation or rejection procedures.
- **Wire stripping** removes or alters payment information to hide parties or sanctioned interests. Compare incoming and outgoing messages and investigate instructions to omit identifying details.
- **Cover payments** separate settlement from the customer instruction and can reduce visibility if information is missing. Preserve required customer details across the payment chain.
- **Trade and vendor screening** should consider end users, ownership, services and destination. A vendor's low-risk registration address does not resolve sanctioned end-use or diversion risk.

Training, employees and escalation

- **Training** begins at onboarding or shortly afterward and continues through refreshers and change-driven updates. Tailor examples to tellers, lenders, private bankers, investigators, IT, management and the board.
- **Training effectiveness** considers knowledge checks, observed errors, audit findings and practical performance. Retain attendance and content records; completion counts alone do not demonstrate understanding.
- **Employee indicators** include unexplained wealth, avoided vacations, unauthorized overrides, unusual customer favoritism and repeated unresolved exceptions. Assess objective behavior rather than ethnicity, language or social familiarity.
- **Internal reporting** uses compliance or protected whistleblowing channels. Preserve confidentiality and use an independent escalation route where a manager or senior officer is implicated.
- **Willful blindness** is deliberate avoidance of knowledge of wrongdoing. Individuals as well as institutions may face civil or criminal consequences, subject to the legal standards and facts.

Independent testing, remediation and metrics

- **Independent AML testing** uses qualified internal or external reviewers who do not operate the controls tested. Report independently to the board or audit committee; risk and applicable rules determine scope and frequency.
- **Management owns remediation** through root-cause analysis, responsible owners, milestones and evidence. Audit assesses the finding and independently validates that corrective action works.
- **Useful metrics** include aged alerts, investigation timeliness, missed reviews, data failures, repeat findings and alert quality. True-to-false-positive ratios help assess productivity alongside coverage and missed-risk testing.
- **Program consequences** can include restrictions, fines, license loss, litigation and individual penalties. Reputational damage may also reduce customers, correspondent access, investment and market confidence.

Investigations

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

TURN SIGNALS INTO DECISIONS

Detect Alert or referral → **Investigate** Facts and flows → **Decide** Report and mitigate → **Preserve** Records and evidence

04 Investigations and information sharing

From an alert to an investigation

- **An alert is a lead.** Gather internal KYC and transaction records, establish expected activity and compare the observed pattern. Tips, adverse media and legal requests can also trigger review.
- **Follow the money:** identify sources, destinations, timing, intermediaries and ultimate beneficiaries. Link accounts through ownership, contacts, devices and counterparties; assess the full relationship across products.
- **Corroborate explanations** with invoices, contracts, financial statements and reliable external information. Evaluate source quality and identity matches; an allegation or unverified blog is not established fact.
- **Case records** should explain the concern, evidence, analysis, decisions and approvals. Clear a false positive only with a reasoned rationale; escalate unresolved indicators through authorized procedures.

SARs and STRs

- **Suspicious activity reports (SARs)** and **suspicious transaction reports (STRs)** communicate reasonable suspicion to the designated authority, commonly the FIU. Proof of the underlying crime is not required.
- **Report promptly** within applicable local deadlines when the reporting standard is met, including relevant attempted activity. A monitoring alert, PEP status or subpoena alone does not automatically establish suspicion.
- **A useful narrative** explains who, what, when, where, why and how: relevant parties, amounts, dates of activity, channels, fund flows and why conduct differs from expected behavior.
- **Authorized decision-making** follows internal responsibilities and escalation rules. Continue reviewing ongoing activity and make further reports where required; filing does not discharge monitoring duties.

Confidentiality and supporting records

- **No tipping off:** protect reports and information revealing their existence. Limit internal access to lawful, authorized needs; board reporting can use appropriate summaries and statistics.
- **Insider subjects** need special care: avoid disclosing a report to an implicated director or officer. Use independent governance and legal channels to manage conflicts.
- **Supporting documentation** includes the records used to reach the decision: KYC, statements, transaction data, communications and analysis. Retain a secure audit trail and make authorized retrieval practical.
- **FATF recordkeeping** generally calls for at least five years for transaction records and for CDD records following relationship termination or an occasional transaction. Apply longer domestic requirements and legal holds where relevant.

Investigations

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

TURN SIGNALS INTO DECISIONS

Detect
Alert or referral

→

Investigate
Facts and flows

→

Decide
Report and mitigate

→

Preserve
Records and evidence

Law enforcement and legal requests

- **Authenticate requests** independently and route them to the designated legal or compliance team. Confirm authority, legal basis, scope, deadline, confidentiality and permitted disclosure before releasing information.
- **A subpoena or production order** requires specified records or testimony. Preserve responsive material, review privilege with counsel, track requests centrally and respond completely and on time.
- **Overbroad requests** call for prompt clarification or lawful narrowing through counsel, rather than silence or unilateral omissions. Keep a record of what was produced, to whom and under which authority.
- **Search warrants** authorize a defined search or seizure. Obtain a copy, identify the agents, involve counsel promptly, preserve records and document seized items without obstructing lawful execution.
- **Freeze orders** restrict access to specified assets or persons under valid authority. Implement the defined scope promptly and preserve the assets; a general information request does not itself authorize freezing.

Keep-open requests and relationship exit

- **Keep-open requests** from law enforcement should be documented in writing with the authority and duration. Assess whether the institution can continue meeting its own obligations and managing the risk.
- **An open account** remains subject to monitoring, reporting and applicable sanctions. A request to keep it open does not eliminate AML duties or authorize prohibited transactions.
- **Exit decisions** consider unresolved CDD failures, unacceptable residual risk, persistent unexplained activity and legal restrictions. A single report, nationality or broad customer category should not substitute for assessment.
- **Controlled exit** records rationale and approvals, reviews outstanding activity, preserves records and coordinates lawful customer communication. Avoid tipping off and honor valid asset restraints or other legal directions.

Privacy and lawful information sharing

- **AML duties and privacy rules** operate together. Identify a legal basis, purpose, permitted recipients and applicable cross-border restrictions; headquarters ownership does not create unrestricted sharing rights.
- **Data minimization** limits sharing to necessary and proportionate information. Apply need-to-know access, secure transfer, retention controls and logs; consult legal and data-protection specialists on conflicts.

Investigations

Certified Anti-Money Laundering Specialist

KNOWLEDGE CHEATSHEET

TURN SIGNALS INTO DECISIONS

Detect
Alert or referral

→

Investigate
Facts and flows

→

Decide
Report and mitigate

→

Preserve
Records and evidence

- **SAR confidentiality** can differ from the treatment of underlying customer facts. Check the rules for the specific recipient, affiliate and jurisdiction before sharing either.
- **USA PATRIOT Act 314(a)** supports designated government-to-institution information requests. **314(b)** provides a conditional voluntary institution-to-institution sharing framework; it is not a universal cross-border authorization.

Cross-border cooperation and evidence

- **FIU-to-FIU channels** and Egmont mechanisms exchange intelligence under safeguards. Information may have use and onward-disclosure restrictions; intelligence is not automatically admissible courtroom evidence.
- **Mutual legal assistance treaties (MLATs)** and related formal requests obtain evidence through designated authorities. Specify the facts, legal basis, records sought and procedural requirements.
- **Letters rogatory**, liaison officers, police cooperation and joint investigation teams offer other lawful channels. Match the channel to urgency, jurisdiction, evidence needs and powers available.
- **Public-private partnerships** combine typologies, expertise and permitted case information. Agreements and secure systems support cooperation but do not create an exemption from privacy or reporting law.
- **Investigative interviews** require preparation, an appropriate setting and careful records. Establish facts with open questions, then test inconsistencies with focused follow-ups while respecting legal rights and avoiding unsupported accusations.