Center for Competitive Statecraft and Strategic Policy
WP-2026 Independent Policy Research Series

WP-2026-AML-01

AML/CFT/CPF Control Matrix

Illicit Finance Node Risk Framework — UNCLASSIFIED // OPEN SOURCE POLICY ANALYSIS

Author	Collin George
Contact	collin.george@protonmail.com
Date	March 2026
Version	Version 2.0 (Style Guide v3.0 / Editorial Directive Applied)
Repository	https://github.com/collingeorge/WP-2026
Institution	Center for Competitive Statecraft and Strategic Policy
Status	Unclassified // Open Source // Independent Policy Research
License	CC BY 4.0 — https://creativecommons.org/licenses/by/4.0/

ABSTRACT

This paper establishes the AML/CFT/CPF Control Matrix — a defensive compliance and policy-analysis reference supporting risk identification, control design, escalation review, and public-law alignment. It maps the principal node types through which illicit finance flows are reported, in the public record, to be routed, layered, and integrated across nine node categories and twenty node types. Each node is analyzed across eight dimensions: documented exposure pattern, risk indicators, institutional controls, escalation indicators, reporting pathways, and statutory authority basis. This matrix is illustrative, non-exhaustive, and intended for risk-based application rather than fixed-rule deployment. It is produced against Style Guide v3.0 and Verbiage Guide v2.2 standards. It reflects a full red-team audit pass covering statutory citation precision, escalation threshold language, and enforcement exposure framing. Cross-reference: WP-2026-SENI-02 provides the named-entity exposure index organized against this node architecture.

in a personal capacity. Nothing in this document reflects the views or positions of the University of Washington, UW Medical Center, or any other institution. All analysis is based entirely on open-source, publicly available information. No classified or controlled information was used or implied. This document does not constitute legal advice. This document is a defensive compliance and policy-analysis reference intended to support risk identification, control design, escalation review, and public-law alignment. It does not constitute legal advice.

METHODOLOGICAL NOTE

SCOPE AND ANALYTIC POSTURE

This matrix documents node categories and risk indicators as reflected in the public enforcement record — including official enforcement actions, regulatory findings, designation records, and FATF typology guidance. It does not assert current illicit activity by any named node type, institution, or geographic area. Escalation triggers are illustrative risk indicators and do not substitute for jurisdiction-specific legal review, institutional procedures, or case-specific evidentiary assessment. The matrix is illustrative, non-exhaustive, and intended for risk-based application rather than fixed-rule deployment. Certain entries reference enforcement typologies, civil findings, or designations that vary in evidentiary basis and procedural posture; these are distinguished from adjudicated criminal findings and should be interpreted accordingly. Attribution in this document reflects public enforcement, designation, or reporting records and does not constitute judicial determination unless explicitly stated. Certain entries reflect typology-level analysis rather than determinations regarding specific institutions. FATF Recommendations are international standards and are not legally binding unless implemented through domestic law. All findings are time-bound to the period specified and should not be interpreted as current conduct unless explicitly stated.

Source tier convention follows Style Guide v3.0: Tier 1 = U.S. Government, UN bodies, primary legal texts; Tier 2 = credible policy institutions and commercial data providers; Tier 3 = named news media and trade publications. Confidence labels follow ODNI analytic standards and the dual-axis framework (probability × evidence quality). All quantitative claims are sourced at point of use.

The matrix was produced in two phases. Phase 1 established the node architecture and eight-column control structure drawing on BSA/FinCEN regulations, FATF Recommendations (2012, updated 2023), OFAC compliance frameworks, BIS/EAR export control guidance, AMLA 2020, EU AMLD6, UN Security Council Resolutions, and the DOJ Crypto Enforcement Framework. Phase 2 applied a systematic red-team audit across all 20 nodes covering: (1) statutory citation precision and scope clarity; (2) escalation threshold language — replacing hard numerical triggers with risk-based behavioral pattern language; (3) enforcement exposure framing — removing outcome-assumptive language, time-bounding claims, and clearly separating indicators from conclusions.

KEY JUDGMENTS

1

MODERATE CONFIDENCE · ANALYTICALLY INFERRED — CONSISTENT WITH FATF MUTUAL EVALUATION FINDINGS AND FINCEN TYPOLOGY REPORTS

The principal vulnerability in illicit finance architecture is assessed with moderate confidence to reside at transition points between node categories, where AML/CFT detection coverage degrades across jurisdictional and institutional boundaries. The public record supports this judgment through multiple documented cases in which layering sequences traversed two or more node categories before generating SAR or enforcement activity.

2

HIGH CONFIDENCE · DIRECTLY SUPPORTED — BASED ON DOJ, FINCEN, OFAC ENFORCEMENT RECORD 2017–2025

Virtual asset infrastructure — in particular unregistered OTC desks and privacy coin or mixer services operating outside FATF-compliant jurisdictions — is assessed with high confidence to constitute the highest-velocity layering mechanism for state-linked threat actors and organized crime, based on the public enforcement record from DOJ, FinCEN, and OFAC actions between 2017 and 2025.

3

HIGH CONFIDENCE · DIRECTLY SUPPORTED — FATF TBML GUIDANCE; BIS/OEE ENFORCEMENT RECORD; UN PANEL OF EXPERTS REPORTS

Trade-based money laundering and free trade zone transshipment are assessed with high confidence to represent the primary mechanism for proliferation finance and sanctions evasion by state actors, because they exploit the structural gap between financial sector AML controls and customs/export control enforcement operating under different legal frameworks and information-sharing authorities.

4

HIGH CONFIDENCE · DIRECTLY SUPPORTED — FINCEN RULEMAKING RECORD; AMLA 2020 MANDATE; FATF 2022 U.S. MUTUAL EVALUATION

The insurance sector and luxury goods/art market are assessed with high confidence to represent the most under-regulated node categories in the U.S. AML/CFT architecture as of March 2026, with FinCEN rulemakings for both sectors not finalized, creating a documented and persistent coverage gap. The public record does not establish whether this gap has been exploited in specific adjudicated cases at scale.

5

MODERATE CONFIDENCE · ANALYTICALLY INFERRED — DERIVED FROM RED-TEAM AUDIT OF INSTITUTIONAL COMPLIANCE PROGRAM LANGUAGE AND FINCEN SAR ANALYSIS

Escalation trigger language in institutional AML compliance programs is assessed with moderate confidence to over-rely on hard numerical thresholds that are both gameable by sophisticated actors and operationally brittle. Risk-based language calibrated to behavioral pattern consistency with documented typology indicators provides more defensible and institutionally resilient escalation architecture.

SERIES INTEGRATION

AML-01 occupies the methodology layer for financial enforcement within the WP-2026 series. It provides the control architecture that the applied enforcement papers presuppose.

READS INTO

SIEGE-01 · CTF-01 · CPF-02 · SHIELD-01 · MAXPRESS-01 · SENI-01 · SENI-02

READS UPSTREAM FROM

ATTRIBUTION-01 / CSE-01 (nexus attribution framework) · PERSIST-01 (competitive statecraft architecture)

The matrix continues on the following pages in landscape orientation. Three appendices follow the matrix: Appendix A — Analytic Posture Framework; Appendix B — Control Typology Classification; Appendix C — False-Positive Discipline Reference.

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
I. BANKING & CORRESPONDENT NETWORKS							
Correspondent Banking / Nostro Accounts	ML / TF / Sanctions Evasion	The public record reflects correspondent relationships in which nested shell company beneficiaries transit USD/EUR clearing; payable-through accounts may obscure originator identity; and structuring patterns are reported below CTR thresholds. These patterns appear in FATF typology reporting and FinCEN advisories as consistent with layering risk.	No end-beneficiary transparency in payable-through structures Respondent bank domiciled in FATF grey or black list jurisdiction at time of review Same-day inbound/outbound flows lacking apparent commercial rationale Inconsistent LEI data across SWIFT messaging Volume increase materially exceeding established customer baseline, consistent with known AML typology indicators	Enhanced Due Diligence (EDD) on respondent institution Automated wire screening against OFAC, UN, EU, and FATF designation lists CDD refresh at intervals not exceeding 12 months for designated high-risk corridors Payable-through account controls requiring sub-account beneficiary mapping	Match against SDN or designated entity list Pattern consistent with known AML typology indicators — may prompt jurisdictional risk reassessment or de-risking review, evaluated against institutional risk appetite and applicable obligations SAR filing threshold met (generally ≥$5K where suspicion is present under BSA; based on suspicion, not solely monetary amount) Peer institution information-sharing channels, where lawful and appropriate	SAR → FinCEN (BSA/AML) UNSCR 1267 Committee referral pathway via OFAC — ISIL/Al-Qaeda nexus UNSCR 1373 — general TF scenarios UNSCR 2231 — Iran-specific scenarios Egmont FIU-to-FIU channel	BSA 31 USC §5318 · OFAC SDN List; CAATSA authorities (where applicable) · UN SCRs 1267/1373/2231 (scenario-specific, where applicable to UN-designated entities under relevant sanctions regimes) · FATF Rec. 13
Private Banking / Wealth Management	ML / Grand Corruption / CPF	The public record reflects that PEP-linked layering through numbered accounts,	PEP designation with unexplained wealth quantum, as identified through public reporting or	PEP-mandatory EDD including adverse media screening Source-of-wealth verification	Match against HM Treasury, OFAC, or EU designation list Adverse media indicating	SAR → FinCEN, FCA, or FINMA depending on booking center FATF mutual evaluation	BSA/USA PATRIOT Act §312 (applies to correspondent and private banking

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		discretionary trusts, and fiduciary nominee structures has been cited in enforcement actions. Concealment of assets associated with sanctioned individuals and family-office opacity have appeared in regulatory findings and Senate investigative reports.	screening results Nominee beneficial owner inconsistent with documented economic rationale Booking center jurisdiction with elevated secrecy index Refusal to disclose source of wealth Trust or foundation structure with no apparent purpose	(documentary) Annual BO re-certification Politically exposed family member (RPEP) screening Sanctions review and potential blocking obligations where applicable — not a fixed freeze protocol absent legal predicate	corruption, bribery, or WMD nexus Incoming from recently sanctioned jurisdiction without apparent lawful purpose or licensing basis	referral DOJ/FBI financial crimes task force referral, where nexus is established	accounts maintained for non-U.S. persons and foreign financial institutions) · FCPA 15 USC §§78dd-1, 78dd-2, 78dd-3 (as applicable; where corruption nexus is explicit) · UK POCA 2002 §330 (UK jurisdiction only) · EU AMLD6 Art. 3 (EU jurisdiction only)
Retail / Commercial Bank Accounts	Narco-trafficking / TF / ML	Structuring patterns, third-party deposit schemes, and funnel account architectures are reflected in FinCEN typology reporting and DOJ enforcement actions as consistent with drug-trafficking-related ML and TF risks. Cash-intensive business front account typologies appear in multiple	Multiple sub-$10K deposits at same branch or on same day Rapid depletion of account balance within 24–48 hours of deposit Account holder profile inconsistent with transaction volume Multiple third-party depositors with no apparent commercial rationale Geographic anomaly: deposits in locations inconsistent with account holder	Automated structuring detection (velocity-based rules) Cash-intensive business EDD Beneficial ownership CDD (FinCEN CDD Rule 2018) Geographic clustering analysis Account behavior baseline deviation alerts	Repeated structuring patterns within a defined monitoring period, consistent with typology indicators Funnel account signature identified through behavioral analysis Documented nexus to jurisdictions associated with heightened narcotics-trafficking risk	CTR → FinCEN (>$10K cash) SAR → FinCEN DEA/FBI referral via law enforcement liaison, where appropriate based on nexus to narcotics or criminal investigation	BSA 31 USC §5324 (structuring) · FinCEN CDD Rule 31 CFR §1010.230 · 18 USC §1956

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		enforcement records.	address				
Shell Company / SPV Bank Accounts	Sanctions Evasion / CPF / ML	Multi-jurisdictional SPV chain layering, nominee director structures, and round-trip financing patterns are reflected in FATF guidance, FinCEN advisories, and DOJ enforcement records as consistent with sanctions evasion and proliferation finance risk. The public record reflects that non-US dollar clearing avoidance has been identified in IEEPA-related enforcement.	No identifiable economic purpose for the account structure Beneficial owner domiciled in sanctioned jurisdiction Incorporation in secrecy jurisdiction within 90 days of account opening Professional nominee director serving multiple unrelated entities Inbound funds immediately disbursed to opaque counterparties	BO verification to natural person level (≥25% ownership threshold) Negative-news screening on all linked entities GLEIF LEI cross-check Corporate registry verification against declared ownership structure Periodic dormancy review	BO linked to SDN or associated with sanctioned jurisdiction Multi-layered ownership structure lacking economic or operational rationale — consistent with potential round-tripping typology Pattern consistent with indicators documented in IEEPA-related enforcement records	SAR → FinCEN OFAC administrative subpoena cooperation DOJ NSD referral where IEEPA potential violations are identified	IEEPA 50 USC §1701 (applicable where sanctions-evasion nexus is established) · FinCEN CDD Rule · EU 5th AMLD BO register (EU jurisdiction only) · FATF Rec. 24/25 (international standards — not legally binding unless implemented through domestic law)
II. CAPITAL MARKETS & SECURITIES							
Brokerage / Securities Accounts	ML / Sanctions Evasion / CPF	Wash-trade patterns between related accounts, nominee share parking, and layering through secondary	Circular trading patterns with no net position change, inconsistent with stated investment mandate BO inconsistency	SEC/FINRA AML program compliance OFAC screening at account opening and on a periodic basis Securities-specific	SDN match on account holder or beneficial owner Wash trade detection threshold exceeded, based on surveillance	SAR-SF → FinCEN SEC Enforcement referral FINRA regulatory referral	Securities Exchange Act §17(a) (recordkeeping and reporting authority; note: not a direct AML mandate

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		market bond transactions are reflected in SEC enforcement records and FinCEN SAR typologies. Short-selling patterns preceding sanctions designations have appeared in public reporting.	between custodian and issuer records Account linked to IP address associated with sanctioned jurisdiction High-frequency inbound/outbound activity in low-liquidity instruments Trades inconsistent with stated investment mandate or customer risk profile	SAR filing (SAR-SF) Cross-account wash trade surveillance DVP/RVP delivery anomaly monitoring	models calibrated to market norms Coordinated account activity, absent documented legitimate trading rationale, may warrant escalation	OFAC reporting per 31 CFR §501.604	— AML obligations arise through FinCEN/BSA) · FinCEN SAR rules 31 CFR §1023.320 · OFAC 31 CFR Parts 500-598 · FATF Rec. 26 (regulation and supervision of financial institutions)
OTC Derivatives / Structured Notes	CPF / Sanctions Evasion	The public record reflects that structured note issuance in offshore jurisdictions for designated entity affiliates, swap counterparty opacity, and instruments referencing sanctioned sovereign debt have appeared in CFTC, OFAC, and FATF CPF enforcement and guidance. Certain structures may also reflect lawful	Counterparty domiciled in sanctioned jurisdiction or FATF non-cooperative territory Notional value disproportionate to counterparty balance sheet, without documented hedging or risk management rationale Instrument appears designed to reduce exposure to U.S. financial system controls Exotic structure with no apparent hedging rationale and sanctioned-	ISDA counterparty KYC with BO penetration Derivative booking jurisdiction controls CFTC swap data repository (SDR) reporting Sanctions clause in ISDA Master Agreement	Counterparty linked to OFAC/EU-designated entity Instrument appears to provide economic benefit to SDN-listed party Instrument appears designed to reduce exposure to U.S. financial system controls — evaluated in context of counterparty, jurisdiction, and transaction purpose	SAR → FinCEN CFTC Division of Enforcement referral OFAC ISDA-specific disclosure protocol	CEA §4s(j) (applies to swap dealers and major swap participants) · OFAC GL/FAQ for derivatives (where SDN exposure exists) · FATF Proliferation Finance Guidance (2021) · EU Dual-Use Reg. 2021/821 (CPF context only)

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		jurisdictional, tax, or hedging preferences; review should focus on context, counterparties, and sanctions exposure.	jurisdiction counterparty				
III. VIRTUAL ASSETS & CRYPTO INFRASTRUCTURE							
Centralized VASP / Exchange	ML / TF / Sanctions Evasion / Narco	The public record — including DOJ enforcement actions, FinCEN civil penalties, and OFAC designations — reflects that certain VASPs have been cited for processing transactions associated with sanctioned jurisdictions, darknet markets, and ransomware actors. Blockchain analytics indicators consistent with typologies publicly attributed to DPRK-linked actors have been identified in multiple enforcement records.	Deposits from OFAC-designated wallet address Transaction volume inconsistent with stated income or stated purpose Rapid conversion to privacy coin or cross-chain bridge following deposit IP address associated with sanctioned jurisdiction On-chain cluster analysis links to darknet marketplace or ransomware wallet	Travel Rule compliance (FATF Rec. 16 for VASPs) On-chain blockchain analytics (Chainalysis, Elliptic, TRM Labs or equivalent) OFAC virtual currency compliance framework Address screening against OFAC SDN virtual currency list KYC at onboarding and enhanced review for high-value withdrawals	Exposure consistent with publicly designated wallet clusters, when evaluated in combination with other indicators — note: blockchain attribution is probabilistic, not determinative; on-chain analytics indicators support, but do not alone constitute, a finding of sanctions nexus Funds received from darknet marketplace address per blockchain analytics Blockchain analytics indicators consistent with typologies publicly attributed	SAR → FinCEN (VASPs are MSBs under BSA) OFAC reporting obligation 31 CFR §501.604 FBI/CISA referral for state-actor cyber-enabled theft DOJ CCIPS referral	BSA 31 USC §5330 (VASP as MSB) · OFAC VA Sanctions Compliance Guidance (2021) · FATF Updated Guidance on VAs (2021) · 18 USC §1960

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
					to DPRK-linked actors — in combination with other risk indicators; attribution derives from FBI/OFAC public statements, not judicial determination Rapid chain-hop pattern post-deposit, in combination with other risk indicators		
Privacy Coins / Mixers / Tumblers	TF / Narco / ML / CPF	The public record reflects that certain privacy coin technologies, mixing services, and tumbler architectures have been cited in enforcement actions and OFAC designations in connection with darknet market settlement, ransomware proceeds, and sanctions evasion. Certain technologies may have legitimate privacy uses; escalation should turn on totality of	Inbound funds from exchange followed by immediate mixer deposit Receipt of privacy coin at onboarding inconsistent with customer profile NFT self-purchase at inflated value Mixer service deposit without documented business explanation Output wallet address associated with ransomware cluster in public reporting	Mixer or tumbler service exposure triggers enhanced review under institutional policy Reject privacy coin deposits where blockchain tracing is not operationally possible, per institutional policy NFT platform KYC and transaction monitoring OFAC designation compliance — Tornado Cash (Aug 2022), Blender.io — where designation applies	Interaction with OFAC-designated mixer where designation is confirmed applicable (e.g., Tornado Cash, Blender.io) Privacy coin receipt, in combination with other indicators, presents elevated risk requiring enhanced review Ransomware cluster linkage identified through on-chain analytics	SAR → FinCEN OFAC mandatory blocking and reporting FBI Cyber Division referral CISA ransomware reporting portal	OFAC Tornado Cash designation (OFAC-2022-0831) — note: subject to ongoing constitutional litigation regarding smart contract designation authority (Van Loon v. Dep't of Treasury, 5th Cir. 2024) · BSA 31 USC §5318(g) · 18 USC §1956(a)(1) (requires proof of intent) · FATF Recommendation 15

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		indicators, sanctions exposure, and institutional policy — not on use of privacy-enhancing technology alone.					
Crypto OTC Desk (Unregistered)	ML / Sanctions Evasion / Narco	The public record reflects that unregistered crypto OTC desks operating without MSB registration have been cited in DOJ and FinCEN enforcement actions. These entities are functionally analogous to informal value transfer systems and have been identified in public reporting as facilitating conversion of illicitly obtained crypto assets.	No FinCEN MSB registration on record Transaction volume incompatible with declared business purpose Counterparties associated with sanctioned jurisdiction (Iran, Russia, DPRK) per public screening indicators Cash-to-crypto transactions without KYC documentation Operation through messaging platforms (Telegram, WeChat) without formal business infrastructure	MSB registration verification at onboarding for institutional OTC counterparties Correspondent crypto-bank due diligence on OTC desk clients On-chain analytics for settlement addresses Travel Rule enforcement at settlement leg	Unregistered MSB status confirmed through FinCEN registry check Sanctions-nexus counterparty identified through screening Transaction volume exceeding $25K with no KYC documentation, or otherwise inconsistent with risk-based KYC expectations	SAR → FinCEN FinCEN enforcement referral for unlicensed MSB DOJ MLARS referral OFAC penalty process	18 USC §1960 · BSA 31 USC §5330 · OFAC 31 CFR §501 · DOJ Crypto Enforcement Framework (2020)
IV. REAL ESTATE & HIGH-VALUE ASSETS							
Residential / Commercial Real Estate	ML / Grand Corruption / Sanctions Evasion	The public record — including FinCEN Geographic	All-cash LLC purchaser with no identifiable beneficial owner Property value	FinCEN GTO compliance — mandatory BO disclosure for qualifying all-cash	BO matches or is publicly associated with a designated individual	SAR → FinCEN (covered institutions) FinCEN GTO mandatory	BSA / FinCEN GTO (31 USC §5326) · IEEPA / OFAC for sanctioned

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		Targeting Orders, congressional reports, and DOJ civil forfeiture actions — reflects that all-cash LLC-veil purchases, multi-tier corporate title structures, and serial property acquisitions have been cited as consistent with ML and sanctions evasion risk. Note: GTO applicability is jurisdiction-specific and time-sensitive; obligations should be verified against current FinCEN directives.	materially above comparable market / no arm's-length negotiation documented BO domiciled in high-corruption or sanctioned-state jurisdiction Serial purchases in FinCEN GTO-covered markets — verify current GTO for applicable jurisdictions Rapid re-sale at same or lower value without apparent commercial rationale	purchases in covered markets; verify current GTO for applicable jurisdictions and thresholds Title company AML program Deed-of-trust / mortgage lender BSA compliance Real estate attorney and agent SAR filing obligation — note: proposed FinCEN rule (2024 ANPRM) not yet final; proposed obligations are not yet universally applicable	GTO threshold met with LLC purchaser and no BO disclosure, in applicable jurisdiction Documented nexus to known narco proceeds or corruption proceeds investigation	reporting DOJ/FBI task force referral IRS-CI referral where tax evasion nexus is identified	BO · 18 USC §1956 · Proposed FinCEN real estate AML rule (2024 ANPRM — not yet final)
Luxury Goods / Art / Collectibles	ML / Sanctions Evasion / CPF	The public record — including AMLA 2020 legislative findings, DOJ civil forfeiture records, and FATF guidance — reflects that high-value art, anonymous auction transactions, shell company	Freeport-domiciled sale or purchase with no identifiable title chain — may present elevated opacity risk Auction purchase by anonymous shell-company bidder Rapid re-sale post-acquisition at comparable value, without market-	Art dealer and auction house AML program (AMLA 2020 — coverage established; FinCEN rulemaking ongoing) BO disclosure for purchases over applicable threshold (pending FinCEN rulemaking) Provenance	Sanctioned consignor or buyer identified through screening CITES violation identified (antiquities) Freeport-stored asset linked to active forfeiture investigation per public record	SAR → FinCEN (post-AMLA 2020 coverage of art market) OFAC voluntary self-disclosure for sanctions exposure HSI referral for cultural property or antiquities trafficking	AMLA 2020 (31 USC §5312 expanded) · IEEPA / OFAC SDN list · National Stolen Property Act 18 USC §2314 · UNESCO 1970 Convention / CPIA

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		acquisitions of luxury assets, and freeport storage arrangements have been cited as consistent with ML and sanctions evasion risk. Freeport use may present elevated opacity risk; not all freeport use is indicative of illicit activity.	based justification Consignor associated with sanctioned jurisdiction per public screening Artwork origin documentation absent or inconsistent	verification requirement Freeport operator due diligence protocols			
V. TRADE-BASED ML (TBML) & PROLIFERATION FINANCE							
Trade Finance / Letters of Credit	TBML / CPF / Sanctions Evasion	The public record — including FATF TBML guidance, BIS/OEE enforcement actions, and UN Panel of Experts reports — reflects that over- and under-invoicing, phantom shipments, and multiple-invoicing of single shipments have been identified as consistent with value-transfer and proliferation finance risk. Transshipment	Material deviation from established commodity pricing benchmarks (cross-referenced against Panjiva, UN Comtrade, or equivalent) Country of origin inconsistent with commodity type or stated routing Consignee identified as known front company or newly established entity with no operational history Payment terms materially favorable to high-risk jurisdiction counterparty (e.g., unsecured	Trade-Based ML Risk Assessment per FATF Guidance Dual invoice cross-check (shipping documents vs. L/C vs. buyer invoice) Commodity pricing database verification End-User Certificate (EUC) verification for dual-use exports SWIFT MT700 screening for sanctioned entity or jurisdiction	Shipment routed through transshipment hub associated with sanctioned-jurisdiction nexus, as identified through public reporting or screening indicators Dual-use goods identified without export license documentation Invoice variance materially inconsistent with pricing benchmark — consistent with potential diversion typology	SAR → FinCEN BIS Office of Export Enforcement (OEE) referral OFAC referral where sanctions nexus is identified DOJ NSD Counterproliferation Section referral	AECA 22 USC §2778 · EAR 15 CFR §730-774 (dual-use goods — Commerce/BIS jurisdiction; note: defense articles subject to ITAR/AECA, not EAR) · IEEPA 50 USC §1705 · FATF TBML Guidance (2020) · UN SC Resolution 2094 (DPRK-specific regime)

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		patterns consistent with potential diversion typology have appeared in enforcement actions.	advance payment) Dual-use goods with civil stated end-use but specifications consistent with military-grade application				
Free Trade Zones (FTZs)	Sanctions Evasion / TBML / CPF	The public record reflects that certain FTZ arrangements have been cited in BIS enforcement actions, FinCEN advisories, and UN Panel of Experts reports as consistent with transshipment and sanctions evasion risk. Certain FTZ arrangements may elevate risk where transparency, licensing, and end-use verification are limited; FTZ status itself does not establish illicit activity.	Consignee identified as FTZ-based trading company with no documented operational history Final destination country not disclosed or inconsistent with shipping manifest Cargo type inconsistent with declared end-user industry Rapid re-export within 48–72 hours of FTZ arrival, without documented commercial justification	FTZ operator AML/CFT controls (FATF Rec. 25 for FTZs) Customs authority AIS/AES data analytics for transshipment anomaly detection Financial institution refusal to finance FTZ-based transactions absent full supply chain transparency Coordinated Customs-FIU information sharing	Cargo destined for sanctioned jurisdiction, as identified through public reporting or screening indicators Dual-use goods identified without export license documentation transiting FTZ FTZ operator linked to prior enforcement action per public record	SAR → FinCEN for financial institutions financing the transaction BIS/OEE referral CBP / HSI referral FinCEN advisory engagement	EAR 15 CFR Part 736 · IEEPA · 19 USC §1595a (CBP seizure authority) · FATF Guidance on FTZ risks (international standard — not legally binding unless implemented through domestic law)
VI. INFORMAL VALUE TRANSFER & HAWALA							
Hawala / IVTS / Hundi	TF / Narco / ML	The public record — including FinCEN	Customer receiving large IVTS transfers with no documented	MSB KYC and registration verification Risk-tiered	Operator associated with TF nexus through public	SAR → FinCEN FBI JTTF / TFOS referral where TF nexus is	BSA 31 USC §5330 (MSB registration) · 18 USC §1960

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		guidance, DOJ enforcement records, and FATF typology reports — reflects that informal value transfer system architectures have been cited in connection with terrorism financing, narcotics proceeds repatriation, and sanctions evasion. Escalation analysis should be pattern-based and documentation-based, not premised on geography alone.	income source Correspondent MSB lacks FinCEN registration Transactions involving corridors commonly cited in public IVTS typologies, when combined with documentation and registration deficiencies No paper trail beyond informal ledger Settlement through gold, real property, or commodity exchange	geographic destination monitoring based on documented public typology indicators Cross-border wire monitoring for IVTS-equivalent patterns CTR and SAR obligations for registered hawala operators FinCEN Guidance FIN-2010-G004 on IVTS compliance	enforcement record Transfers to OFAC-designated jurisdiction without documented license basis Pattern consistent with narco repatriation typology, based on documented indicators	established DEA referral for narco proceeds repatriation, where nexus is documented OFAC referral where designated-entity funding is suspected	(unlicensed MSB) · 18 USC §2339B (material support to FTO — requires nexus to a designated Foreign Terrorist Organization; not applicable to IVTS activity absent that nexus) · FATF Recommendation 14
VII. CASINOS & GAMING							
Land-Based Casino	ML / Narco / Corruption	The public record — including AUSTRAC enforcement actions, FinCEN advisories, and state gaming commission findings — reflects that chip-washing patterns, VIP junket arrangements,	Large cash buy-in followed by minimal play relative to buy-in size, then cash-out Third-party chip purchase on behalf of undisclosed principal Customer travels internationally for single casino visit with no apparent commercial rationale	Casino BSA AML program (31 CFR §1021) CTR for cash transactions exceeding $10K SAR filing threshold (generally ≥$5K where suspicion is present under BSA) Player due diligence (PDC) for	Chip-washing pattern confirmed through surveillance and play analysis Structuring pattern below CTR threshold identified Customer associated with organized criminal network per public enforcement	CTR → FinCEN SAR → FinCEN FBI/DEA referral, where appropriate State gaming commission referral	BSA 31 CFR §1021 · 18 USC §1956 · FinCEN Casino Advisory FIN-2014-A002

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		and structured cash transactions have been cited as consistent with ML risk. Organized criminal typologies involving casino operations have been documented in multiple public enforcement proceedings.	Multiple cash transactions below $10K CTR threshold VIP junket operator with opaque BO structure — may warrant enhanced due diligence	high-value players Junket operator EDD with BO penetration	record		
Online Gaming / iGaming Platform	ML / TF	The public record reflects that account-to-account credit transfer patterns, bonus cycling, and unlicensed offshore platforms have been cited in enforcement and regulatory proceedings as consistent with ML and TF risk. Offshore status alone does not establish illicit activity; escalation analysis should be anchored in licensing status, KYC absence, payment method anomalies, and	Account funded then immediately withdrawn without meaningful play — inconsistent with expected gaming behavior Multiple accounts linked to same BO with cross-account transfers Jurisdictional anomaly between player IP address and payment method origin High-value in-game items converted to fiat outside platform No KYC at onboarding on platform lacking regulatory license	KYC at onboarding and for withdrawals exceeding applicable threshold Payment method verification and origin matching Play pattern behavioral analytics AML compliance with applicable licensing jurisdiction requirements Correspondent banking restrictions on unlicensed gaming platforms, per institutional policy	Platform not registered in any FATF-compliant jurisdiction Transfer pattern inconsistent with documented gaming behavior Player associated with TF investigation per public record	SAR → FinCEN for US-licensed platforms FBI Cyber Division referral for offshore unlicensed platforms FinCEN referral for unlicensed gaming MSB	UIGEA 31 USC §5362 (definitions) and §5363 (prohibited transactions) · 18 USC §1955 (illegal gambling) · BSA for licensed platforms · FATF Recommendation 22

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
		transaction behavior.					
VIII. INSURANCE & FINANCIAL PRODUCTS							
Life Insurance / Annuities	ML / Sanctions Evasion	The public record — including OFAC enforcement actions and FATF guidance — reflects that early-surrender premium schemes, policy assignment to undisclosed third parties, and variable annuity churning have been cited as consistent with ML and sanctions evasion risk. Note: BSA AML requirements for insurance companies reflect a proposed and evolving regulatory framework; the FinCEN insurance AML rule was proposed in 2014 and re-proposed in 2024 and had not been finalized as of March 2026.	Single large premium payment followed by early surrender within 12 months Premium funded by third party with no documented insurable interest Policy assigned to undisclosed third party shortly after issuance Beneficiary domiciled in sanctioned jurisdiction Customer resistance to source-of-funds disclosure	AML program for insurance companies — proposed/evolving regulatory framework; verify current status of FinCEN rulemaking before applying as binding obligation SAR filing obligation for suspicious transactions (where applicable to covered entities) Beneficiary screening against OFAC SDN list Source-of-funds verification for single premium over applicable threshold Early surrender pattern monitoring	Beneficiary match against SDN list Early surrender within 6 months of single premium, without legitimate financial explanation Policy assignment to unknown third party without documented rationale	SAR → FinCEN (for covered insurance companies under applicable rules) OFAC blocking and reporting for SDN beneficiary State insurance regulator referral	BSA (proposed insurance AML rule — not yet final as of March 2026) · OFAC 31 CFR §501 · 18 USC §1956 · FATF Rec. 26 (supervision); Rec. 22 (DNFBPs); Rec. 1 (risk-based approach)

NODE TYPE	THREAT VECTOR(S)	DOCUMENTED OR REPORTED EXPOSURE PATTERN	RISK INDICATORS	CONTROLS	ESCALATION INDICATORS	REPORTING PATHWAY	AUTHORITY BASIS
IX. MONEY SERVICES BUSINESSES & REMITTANCE							
MSB / Currency Exchange / Remittance	Narco / TF / ML / Sanctions Evasion	The public record — including DOJ enforcement actions, FinCEN civil penalties, and OFAC designations — reflects that bulk cash remittance, structuring across agent networks, and unlicensed remittance to sanctioned jurisdictions have been cited as consistent with ML and narcotics-proceeds-related risk.	High-volume remittance to single high-risk destination Multiple senders, single recipient — inconsistent with expected remittance behavior MSB agent operating without state license Exchange rate materially outside market rate without documented commercial rationale Customer conducting multiple transactions in single day across multiple agents	FinCEN MSB registration and state licensing verification Agent monitoring program CTR for cash transactions exceeding $10K SAR for transactions ≥$2K (31 CFR §1022.320) Destination country risk-tiering with enhanced monitoring, based on documented public typology indicators	Remittance to OFAC-sanctioned jurisdiction without license basis Structuring pattern identified across agent network MSB agent confirmed unlicensed in operating state	CTR and SAR → FinCEN FinCEN enforcement for unlicensed MSB DEA referral for remittance patterns associated with jurisdictions presenting heightened narcotics-trafficking risk, subject to institutional protocol and nexus assessment OFAC for sanctioned-destination transactions	BSA 31 USC §5330 · 18 USC §1960 · 31 CFR §1022 · OFAC MSB Guidance · FATF Recommendation 14

ESCALATION INDICATORS NOTE: *Escalation indicators listed above are illustrative risk indicators derived from the public enforcement record. They do not substitute for jurisdiction-specific legal review, institutional procedures, or case-specific evidentiary assessment. No indicator is conclusive absent contextual review.*

GTO NOTE: *Geographic Targeting Orders and related reporting obligations are jurisdiction- and time-specific and should be verified against current FinCEN directives before application.*

SOURCE BASIS: *BSA/FinCEN regulations; FATF Recommendations (2012, updated 2023) — international standards, not legally binding unless implemented through domestic law; OFAC compliance frameworks; BIS/EAR export control guidance; AMLA 2020; EU AMLD6; UN Security Council Resolutions; DOJ Crypto Enforcement Framework. All findings are time-bound to the period specified. Attribution reflects public enforcement records and does not constitute judicial determination unless stated. WP-2026-AML-01 v2.2 — George (2026) — CC BY 4.0. Defensive compliance and policy-analysis reference. Does not constitute legal advice.*

APPENDIX A — ANALYTIC POSTURE FRAMEWORK

This appendix defines the four-component analytic posture applied throughout this matrix, consistent with Style Guide v3.0 and ODNI analytic standards. Each component should be applied explicitly in extended analysis derived from matrix entries.

COMPONENT	DEFINITION	APPROVED LANGUAGE PATTERNS
Observed / Reported	What the public record establishes through Tier 1–2 sources: enforcement actions, designations, regulatory findings, or investigative reporting with named institutional attribution.	The public record reflects…; Official reporting indicates…; The enforcement record documents…
Assessment	Synthesized judgment derived from the reporting, with explicit probability and confidence labels per ODNI analytic standards.	We assess with [confidence] that [subject] is [probability] to…; The available evidence is consistent with…
Key Unknowns	What the record does not establish; limits on the analytic inference; principal uncertainties that constrain confidence.	The public record does not establish…; The available reporting does not permit a firm conclusion about…; Principal uncertainty concerns…
Confidence	Dual-axis confidence label (HIGH / MODERATE / LOW) calibrated against source tier and evidence completeness. Separate from probability.	HIGH CONFIDENCE — directly supported by multiple independent Tier 1 sources; MODERATE CONFIDENCE — credible Tier 1/2 sourcing with meaningful inference; LOW CONFIDENCE — primarily analytic inference from limited evidence.

APPENDIX B — CONTROL TYPOLOGY CLASSIFICATION

This appendix classifies the controls listed in the matrix into three functional categories. Classification supports program design, gap analysis, and regulatory examination preparation.

CONTROL TYPE	FUNCTION	REPRESENTATIVE EXAMPLES FROM MATRIX
Preventive	Controls that reduce the probability of illicit activity occurring or entering the institution's exposure perimeter.	KYC/CDD at onboarding; beneficial ownership verification; negative-news screening; sanctions list screening; export license verification; GTO compliance.
Detective	Controls that identify suspicious activity within the institution's transaction and account population after it has occurred or is occurring.	Transaction monitoring and velocity rules; behavioral baseline deviation alerts; wash-trade surveillance; on-chain blockchain analytics; audit trail review.
Reactive	Controls and protocols that respond to identified suspicious activity, including escalation, reporting, and referral.	SAR filing; CTR filing; account restriction; OFAC blocking; law enforcement referral; voluntary self-disclosure; EDD escalation.

APPENDIX C — FALSE-POSITIVE DISCIPLINE REFERENCE

This appendix documents plausible non-illicit explanations for patterns listed as risk indicators in the matrix. Awareness of these explanations is required for defensible escalation decisions, SAR quality, and institutional risk-appetite calibration. Escalation absent consideration of these alternatives produces over-filing, regulatory friction, and analytic degradation.

INDICATOR PATTERN	PLAUSIBLE NON-ILLICIT EXPLANATION	ESCALATION CAVEAT / CONTEXTUAL REVIEW REQUIREMENT
Cash-Intensive Business Accounts	High transaction volume may reflect legitimate business operations (restaurant, laundromat, retail) rather than structuring. Review against industry norms and documented business purpose before escalating.	Document business type and revenue model; compare transaction patterns to industry benchmarks; require supporting commercial documentation before SAR.
Privacy Coin or Mixer Use	Certain privacy-enhancing technologies have legitimate personal privacy uses. Not all privacy coin use or mixer interaction reflects illicit activity.	Escalation should turn on totality of indicators, confirmed sanctions exposure, and institutional policy — not on use of privacy-enhancing technology alone.
FTZ Rapid Re-Export	Short transit times in FTZs may reflect legitimate commercial logistics and supply chain operations.	Assess against documented commercial purpose, licensing status, end-use certification, and known typology indicators before referral.
Large Single Insurance Premium	Lump-sum premium payments may reflect legitimate estate planning, inheritance, or corporate treasury management.	Verify source of funds through documentation; assess customer profile and stated purpose; evaluate early surrender patterns over time.
Multi-Jurisdiction Shell Structure	Multi-layer corporate structures may reflect legitimate tax planning, asset protection, or operational complexity.	Assess whether economic or operational rationale is documented and consistent; evaluate BO transparency against applicable threshold; escalate where rationale is absent or inconsistent.
High-Volume Remittance	High remittance volumes to a single destination may reflect diaspora community patterns, legitimate family support, or business payroll.	Assess against destination risk tier, customer profile, and documented purpose; require supporting documentation for volume outliers before SAR.
