

Practical AI in Financial Crime Prevention, Participant FAQ

Reference handout for attendees of the Center of Excellence in Anti-Money Laundering webinar, 7 May 2026

Prepared by: Evaldas Kazlauskas, Product Owner, AMLYZE

Website: amlyze.com

Format: ~29 questions across 8 sections, plus glossary and source bibliography

Author note: I work as Product Owner at Amlyze, a Lithuanian AML/CFT technology company. My role sits between product, compliance practice, and implementation, so this FAQ is written from a practitioner-observer perspective.

Important note: This material is for education and discussion only. It is not legal advice. Please do your own legal research before relying on it for compliance decisions.

Table of Contents

Practical AI in Financial Crime Prevention, Participant FAQ	1
How to use this document.....	2
Section 1. The Frame	2
Section 2. AI as a Toolbox	2
Section 3. The Baseline Comparison Problem	4
Section 4. Use Cases	5
Section 5. The Four Common Mistakes.....	7
Section 6. The Regulatory Landscape	8
Section 7. Lithuanian Context	10
Section 8. Practical Next Steps	11
Glossary	12
Source bibliography (primary sources cited in the talk).....	13

How to use this document

This FAQ revisits the questions covered (or adjacent to) the talk. It is a reference, not a substitute for the slides. Each answer is short by design. Cross-references to other answers are marked *See also: Q##*. Primary sources are listed at the end.

If something here disagrees with what you heard live, the live talk takes precedence. This document is a snapshot from the day of delivery.

Section 1. The Frame

Q1. What does “practical AI in financial crime prevention” mean?

It means observable use cases, observable limits, and operational good practice. Not vendor case studies or strategic vision. The talk covers what AI is doing today inside AML programmes, where it fails when deployed casually, and what an institution needs to do before its next AI vendor meeting.

Q2. Why anchor the talk on TMNL, the Digital Euro, and the Central Bank of Ireland Innovation Sandbox?

Each of the three is a real, dated, primary-sourced European event. Together they bracket the actual frontier. TMNL (wound down July 2024) shows that cross-bank monitoring runs into a privacy boundary. The Digital Euro architecture (October 2025) shows what regulators centralise when policy aligns. The CBI Innovation Sandbox cohort 1 (December 2024 to June 2025) is one place where structured financial-crime knowledge, AI and privacy enhancing technologies are being tested in a regulatory sandbox.

Q3. What is the central thesis of the talk?

Fix the foundation before adding AI. AI on top of broken data, fragmented systems, unclear ownership, and weak measurement does not solve AML problems. It can scale a poor process. The institutions that get value from AI tend to have measurement, data quality, governance, and integration in place *before* they deploy a model.

Section 2. AI as a Toolbox

Q4. What is the difference between predictive, relational, language, and agentic AI?

These are four overlapping families:

- **Predictive AI.** Supervised and unsupervised machine learning that asks “is this suspicious?” Used in transaction monitoring, alert prioritisation, sanctions screening enhancement, anomaly detection, customer risk scoring.

- **Relational / graph AI.** Graph neural networks and graph analytics that ask “who is connected to whom in a way that matters?” Used in network analysis, beneficial ownership traversal, mule ring detection.
- **Language AI.** NLP and large language models (LLMs) that read and generate text. Used in adverse media triage, SAR drafting, case summarisation, policy retrieval.
- **Agentic AI.** Multi-step workflows that chain detection, retrieval, and drafting across systems. Emerging.

The categories overlap. A graph neural network is predictive AI applied to relational data. Graph *visualisation* on its own is analytics, not AI. *See also: Q5, Q6.*

Q5. Why does it matter that LLMs are not detection engines?

Because vendors and internal teams sometimes assume that “deploying an LLM” near a compliance pipeline improves detection. It does not, by default. LLMs are excellent at text: summarising, drafting, retrieving. They are not designed to score whether a transaction is suspicious. If you use an LLM to draft a SAR narrative, that is genuine value. If you use an LLM to decide whether to file the SAR, you have replaced a probabilistic model with one that has worse calibration on the specific question.

Q6. When is graph analysis “AI” and when is it just analytics?

Graph analytics (community detection, centrality, shortest paths, entity linking) is computational analysis, not AI. It can be powerful without involving any model. Graph *neural networks*, where a model learns to predict labels or anomalies on graph-structured data, are AI. Both are useful in AML. The distinction also matters for AI Act classification and for governance. A graph view that helps an investigator see existing relationships does not need the same documentation overhead as a predictive model.

Q7. What’s actually different across the three eras of AML monitoring (rules, ML, agentic)?

The era names refer to *who designs the pattern*:

- **Rules era.** A human designs the pattern. The pattern can be sophisticated: dynamic thresholds per customer segment, comparisons against the customer’s own past or peer group, transaction sequences over time, suppression of repeat alerts after prior dispositions. Real rule engines are not just static thresholds.
- **ML era.** A model learns patterns from data, including patterns the rule designer did not pre-specify. Requires clean labels, stable feature pipelines, and retraining as criminals adapt, behaviors change.
- **AI / agentic era.** Language models drafting narratives; multi-step workflows; real-time scoring. The machine has not solved the problem. It has reshaped it.

False-positive rates drop across the eras *as a direction*, but the headline 90 to 95% figure for rules (industry and vendor practitioner consensus; specific rates vary materially by institution and configuration) describes legacy or unmaintained installations, not what a well-tuned rule engine can do. *See also: Q9, Q10.*

Section 3. The Baseline Comparison Problem

Q8. What is the baseline comparison problem in AI procurement?

It is the framing pattern in vendor pitches: *“AI does X that legacy systems cannot do.”* The implicit comparison is almost never to a well-tuned, segmented, suppression-aware rule engine. It is to an unmaintained legacy stack. That unfair baseline comparison overstates the marginal benefit of AI, sometimes by a lot.

Q9. What single question should I ask every AI vendor?

“What’s the comparison? Your AI versus an untuned legacy baseline, or your AI versus a well-tuned, segmented, suppression-aware rule engine?”

If the case studies don’t disclose the baseline, the headline magnitude is unreliable. Most published AML case studies compare ML to the bank’s incumbent process, not to a separately optimised classical alternative. *See also: Q10.*

Q10. Why are independent benchmarks of AI vs classical AML scarce?

Because almost all published case studies use the institution’s existing rule engine as the baseline, not a fresh well-tuned classical engine. That is not malicious (it is the only baseline the bank can produce), but it overstates AI’s contribution.

One clean independent benchmark in the public literature is a US Federal Reserve staff working paper (FEDS 2025-092, Allen and Hatfield). Comparing LLMs against four classical fuzzy algorithms plus a weighted-composite baseline on OFAC organisation-name and address data, it reported a 92% reduction in false positives and 11% higher detection vs the best classical baseline. Two scope caveats apply: the dataset is Roman-alphabet only (the paper itself excludes Russian, Arabic, Chinese, Farsi transliterations), and it is a limited pairwise matching, not full production filtering at scale. A complementary 2026 pre-print (OpenSanctions Pairs, arXiv 2603.11051) covers 31 countries with multilingual names and reports similar direction.

For AML transaction monitoring specifically, no equivalent independent benchmark exists. Treat headline numbers cautiously.

Section 4. Use Cases

Q11. Where does AI add the most value in AML today?

Three use cases stand out for the EU mid-market:

1. **Sanctions screening enhancement** on top of a tuned classical engine. Handles cross-script variants, contextual disambiguation, indirect-ownership traversal that classical fuzzy matching misses.
2. **Alert prioritisation** on existing rule output. Orders the queue by likely true-positive probability, reducing analyst dwell on low-value cases.
3. **Investigation reasoning**. Case summarisation, evidence retrieval, typology mapping, narrative drafting. *See also: Q14.*

Less mature: behavioural baselining, network analysis, liveness/deepfake detection, synthetic identity detection. Each has a path but each requires the foundation in place first.

Q12. Sanctions screening, what's practical?

The classical layer is not a strawman. Sophisticated rule-based screening can do this without AI: multi-script normalisation (Cyrillic, Greek romanisation), configurable similarity scoring, alias and birthdate handling, segmented thresholds per screening type, dynamic filters.

AI adds value at the edges:

- Cross-script and cross-cultural name variants where transliteration fails
- Tailoring algorithm to specific languages and cultures
- Contextual disambiguation (combining name match with profile, transaction context, history)
- Graph-based ownership traversal at scale
- Sanctions-evasion typologies, including luxury-goods routing through third countries, dual-use goods through new shell companies, transit payments through home-jurisdiction institutions

The Lithuanian FCIS 2024 annual report records a notable rise in sanctions-related STRs received via the external reporting portal, including reports related to EU sanctions on entities, restrictions on goods exports to Russia or Belarus, and possible attempts to circumvent EU sanctions. *See also: Q9, Q25.*

Q13. Deepfakes in KYC, how real is the threat, and what works against it?

Real and increasing. Documented cases include the ABN AMRO onboarding case under prosecution in the Netherlands (2025 to 2026): deepfake-manipulated identity documents bypassed onboarding; 46 to 47 fraudulent accounts opened; prosecutor sought a 30-month sentence; Amsterdam court issued an interim ruling 31 March 2026 ordering further investigation. The Lithuanian FCIS 2024 report documents a related but distinct typology: fraudsters created a website mimicking the legitimate e-sveikata.lt portal and harvested Smart-ID PIN credentials.

What works against it: layered controls. Presentation-attack detection (PAD) plus injection-attack detection plus document authenticity checks plus NFC and registry checks plus device and behavioural signals plus post-onboarding monitoring. Liveness certification proves PAD conformance. It does not certify end-to-end onboarding resilience. The European supervisors (ENISA Threat Landscape, ESAs joint AI-fraud factsheet, FATF Horizon Scan on AI and Deepfakes) all signal intensified scrutiny in this area. *See also: Q14.*

Q14. Where do LLMs belong in investigation work?

Across the whole investigation cycle, not just SAR drafting at the end. Concretely:

- **Case summarisation.** Pulling alert metadata, transactions, customer profile, prior dispositions into one investigator-readable brief.
- **Evidence retrieval.** Surfacing relevant prior cases, internal policy, applicable typology, screening hits.
- **Typology mapping.** Comparing the case pattern to known red-flag indicators.
- **Narrative drafting.** Turning notes into a coherent SAR narrative; eliminating the blank-page problem.
- **Consistency checks.** Flagging inconsistencies between the current draft and prior dispositions on similar cases.

Non-negotiables: LLMs “hallucinate”. Human review before any decision (escalation, account action, FIU submission) stays the rule. AI drafts and surfaces; investigators decide and sign off. *See also: Q5.*

Q15. How should we think about transaction monitoring AI?

Start with the rule engine, not the model. A well-tuned rule engine, with dynamic thresholds per customer segment, behavioural baselines against the customer’s own past or peer group, sequence-aware patterns, suppression of repeat alerts after prior dispositions, and alert consolidation, operates well below the headline 90 to 95% false-positive figure. AI augmentation makes sense *on top of* this kind of foundation. AI on top of an untuned engine can scale a poor process.

The HSBC and Google Cloud AML AI deployment (June 2023) reported a 60% reduction in alert volume, 2 to 4 times more suspicious activity surfaced, at over 1 billion transactions per month. That is tier-1 global bank scale. The direction translates; the magnitude is institution-specific. *See also: Q9.*

Section 5. The Four Common Mistakes

Q16. Why do AI programmes in AML fail?

Per the EBA's 2025 ML/TF Opinion, more than half of serious compliance failures reported to the EuReCA database involved improper use of RegTech tools. The failure pattern is rarely "the model didn't work." It is "the institution wasn't designed to use it." Four common organisational mistakes follow.

Q17. What is "AI on top of a broken process"?

You train a model on historical analyst dismissals. Analysts had been working with rules where 95%+ of alerts were false. Their dismissal patterns trained the model to replicate those dismissals, automated. The true-positive rate did not improve. The risk increased: dismissals now happen faster, without human eyes.

The fix is unglamorous: before adding AI, optimise rule performance. Three independent voices say the same thing. The FCA's 2017 New Technologies report, the Wolfsberg Group's August 2025 *Statement on Effective Monitoring for Suspicious Activity, Part II*, and PwC's EMEA AML Survey 2026, which reports only 28 to 38% of EU firms are fully confident their TM is fit for purpose, with sector variation: 23% of insurers, 28% of AWM firms, 30% of banks, and 38% of e-money and payments firms (PwC EMEA AML Survey 2026, select interview sample).

Q18. Analytics gap vs AI gap, how do I tell the difference?

If you cannot answer your own rule true-positive rate, alert-to-SAR conversion, average time-to-investigate, or which typologies your rules are designed to detect, you do not have an AI problem. You have a measurement problem.

The Lithuanian FCIS 2024 report publishes the full STR funnel at unusually granular detail: 82,337 STRs received from obliged entities and foreign FIUs; 72,070 auto-closed via automated risk assessment (87.5%); 1,477 referred onwards (1,119 to foreign FIUs, 245 to other Lithuanian law-enforcement and state authorities, 63 to the State Tax Inspectorate, 50 to FCIS investigation units); 16 pre-trial criminal investigations initiated by FCIS based on STR analyses. The volume-to-effectiveness pattern is structural across EU FIUs (UK 2023 to 24: 872,048 SARs to 2,881 actionable DAML refusals; Netherlands 2022: 1.8M unusual transactions to 91,893 declared suspicious). FCIS publishing the funnel at this granularity is itself a strength. *See also: Q25.*

Q19. What is the “individual not institutional” failure mode?

One analyst drafts SARs in 10 minutes using a personal LLM workflow. The team still budgets four hours per SAR. One investigator has a Python script enriching alerts on her laptop; the script is not in any system. One MLRO has a private prompt library that turns case notes into clean summaries. When she leaves, the capability leaves.

These individuals are usually the most capable people in the institution. The failure is that the institution does not capture the improvement as process change. Public Lithuanian regulator-enforcement cases illustrate adjacent versions of the same pattern: UAB Foxpay’s licence was revoked in November 2024 after the Bank of Lithuania found that staff and board members not directly responsible for AML were performing AML functions; UAB Verse Payments was fined EUR 280K in March 2023 with the director personally fined because the AML compliance function was not independent of business interests.

The fix is to turn useful patterns into institutional workflows: approved tools, audit trails, shared prompts where appropriate, model-owner accountability, training, measurement.

Section 6. The Regulatory Landscape

Q20. What is the EU AI Act, and how does it apply to AML?

Regulation (EU) 2024/1689. It classifies AI systems by risk: prohibited (Article 5), high-risk (Annex III categories), limited-risk (transparency obligations), and minimal-risk. Annex III categories that touch AML use cases include points 1 (biometrics, relevant for KYC liveness if the system identifies rather than verifies), 5 (essential services, credit scoring crossover, with a narrow “detecting financial fraud” exception), and 6 (law enforcement, applicable when the deployer is a law enforcement body).

Whether a particular AML AI system is high-risk is a *deployer responsibility* to document. The European Commission’s Article 6(4) classification guidelines were due 2 February 2026 and have been signalled to publish “during 2026”; until they are published, classification analysis runs on the regulation text plus EBA, ECB, national guidance. From 2 August 2026, high-risk AI systems enter the main AI Act regime: providers carry the system-side requirements (Articles 9 to 15), and deployers carry their own operational duties (Article 26), including use according to instructions, human oversight where applicable, logs and monitoring, and documenting classification. *See also: Q21.*

Q21. Article 14(5), does my biometric KYC trigger the two-person verification rule?

Article 14(5) applies to high-risk AI systems under Annex III point 1(a), biometric *identification*. The verification-vs-identification distinction matters operationally:

- **Verification** (“is this the person they claim to be?”, face match to the document the user just presented) is typically excluded from Annex III via the verification exclusion. Article 14(5) does not trigger.
- **Identification** (“who is this?”, biometric match against a database to determine identity) falls under Annex III 1(a). Article 14(5) triggers. At least two competent persons must separately verify and confirm the identification before any action or decision.

Either way, the general Article 14 oversight obligation applies to all high-risk AI: persons assigned to oversight need “necessary competence, training and authority” (verbatim from the regulation). *See also: Q20.*

Q22. AMLR Article 75, what does it actually permit?

Regulation (EU) 2024/1624 (AMLR) Article 75, “*Exchange of information in the framework of partnerships for information sharing*,” applies from 10 July 2027.

What it permits: members of partnerships for information sharing may share information among each other where *strictly necessary* for compliance with Chapter III (CDD) and Article 69 (STR) obligations.

What is required: supervisory authority notification before joining a partnership; a Data Protection Impact Assessment (GDPR Article 35); pseudonymisation; no further sharing outside the partnership; ultimate compliance responsibility remains with each participant.

It is not a TMNL-style broad-pooling vehicle. It is a narrow, supervised, purpose-limited mechanism. AMLR Article 6(5)(b) pairs with this: meaningful human intervention is mandatory for business-relationship enter, refuse, or maintain decisions.

Q23. When does AMLA become operational, and what does that mean?

The Anti-Money Laundering Authority (AMLA) was established by Regulation (EU) 2024/1620 in June 2024. It is expected to reach full operational capability during 2028 (national-supervisor and legal summaries often shorthand this as 1 January 2028). Direct supervision of selected high-risk cross-border financial institutions follows. Selection criteria via Regulatory Technical Standards (RTS) are still being defined; until they are published, institutions cannot self-assess with certainty.

AMLA’s published outputs to date are draft RTS, ITS, and consultations on CDD, beneficial ownership, sanctions, and pecuniary sanctions. AMLA has not yet published an AI-in-AML thematic supervisory expectation document. Per AMLA’s Single Programming Document 2026 to 2028, AMLA itself plans to integrate AI into operations. The supervisor will be AI-equipped from 2028 onward.

Q24. How do AI Act, AMLR, and GDPR Article 22 fit together?

They are complementary regimes, not alternatives:

- **AI Act** governs the AI system itself: classification, risk management, documentation, oversight, transparency.
- **AMLR** governs the AML/CFT process: CDD, ongoing monitoring, STR filing, information sharing under Article 75, mandatory human intervention under Article 6(5)(b).
- **GDPR** governs the personal data: lawful basis (Article 6(1)(c) for AML), data minimisation, the Article 22 prohibition on solely-automated decisions with legal or similarly significant effect.

Meeting Article 14 (AI Act human oversight) does not satisfy Article 22 (GDPR data subject rights) by itself. Documentation must address all three regimes. Strong reliance on third-party scores can also create GDPR Article 22 questions. DPO review is recommended for any AML AI producing decisions or strongly-relied-upon scores affecting natural persons. *See also: Q21, Q22.*

Section 7. Lithuanian Context

Q25. What does the FCIS STR funnel actually look like?

Lithuanian FCIS *Veiklos rezultatai 2024* (Activity Results 2024), Lithuanian-language annual report, sections 01 and 04:

- **82,337** STRs received from obliged entities and foreign FIUs (down from 98,588 in 2023)
- **72,070** auto-closed via automated risk assessment (~87.5%)
- ~10,267 went to human analysis
- **1,477** referred onwards: 1,119 to foreign FIUs (XBR via FIU.net), 245 to other Lithuanian law-enforcement and state authorities, 63 to State Tax Inspectorate, 50 to FCIS investigation units
- **16** pre-trial criminal investigations initiated by FCIS based on STR analyses (up from 12 in 2023)

Cross-border STR sharing through FIU.net grew sharply: 5,291 outgoing reports in 2023 to 37,210 in 2024.

Cross-jurisdictional context: UK NCA Annual Report 2023 to 24 reports 872,048 SARs received with 2,881 DAML refusals (~0.33%); FIU-Nederland 2022 reports 1.8M unusual transactions to 91,893 declared suspicious (~5.1%). FCIS publishes the funnel at sector-and-outcome granularity that most EU FIUs do not. *See also: Q18.*

Q26. What is STRIX AML, and what does the Bank of Lithuania's 2026 inspection plan mean?

STRIX AML is a tool the FCIS has used since December 2023 for risk-based supervision of obliged entities. It enables AML/TF risk assessment based on targeted-survey data collected from supervised entities. First major deployment: February 2024, surveying 547 VASP-sector companies. (*FCIS Veiklos rezultatai 2024, § 05, page 24.*)

Separately, the Bank of Lithuania approved its **2026 AML inspection plan** by Decision No 2026/441-12 on 20 January 2026 (publicly surfaced 22 January 2026). Named institutions in scope: **Luminor, Saldo Bank, Lietuvos centrinė kredito unija, RIA Lithuania, B4B Payments Europe, Bendras finansavimas**. The plan is published on the Bank of Lithuania website.

Lithuania has unusually transparent FCIS funnel data and active AML supervision. No Baltic FIU has yet published a dedicated AI-in-AML supervisory expectation document.

Section 8. Practical Next Steps

Q27. What is the Monday-morning action?

Run one query: alert-to-SAR conversion rate, last quarter, by rule family. If you can run it, you have a baseline you can improve. If you cannot run it, you have your answer about where to start.

Q28. How do I assess my institution's AI readiness?

Five questions to answer before the next AI vendor meeting:

1. **Can you measure your current state?** Rule true-positive rate; alert yield; investigation time; SAR conversion; portfolio risk-review coverage; typology coverage.
2. **Is your data pipeline healthy?** Customer, transaction, screening, KYC, adverse media, and case data must connect.
3. **Do you have a named model owner inside the institution?** The vendor can own the model artefact; the institution must own deployer-side accountability — AI Act Article 14 human oversight (necessary competence, training, authority), Article 26 use-per-instructions, classification documentation under Article 6(3)/(4), and regulator liaison. A vendor contact alone cannot discharge those duties.
4. **Where is the human review point?** For high-risk AI outputs used in decisions with legal or similarly significant effects, define the human review point. For SAR filing and escalation, keep human accountability and audit-trail discipline under AML governance.
5. **Are you looking at the whole?** TM, KYC, Screening, Adverse media, Case management, and Risk scoring is the programme. AI in one silo helps one silo.

If you can do only one of these next week, do #1. *See also: Q9, Q27.*

Q29. Where should small institutions actually start?

The sequence that fits most EU mid-market institutions:

1. **Measurement:** rule yield, alert-to-SAR conversion, segmented performance.
2. **Rule optimisation** and threshold tuning, because many institutions can reduce noise before adding ML.
3. **Sanctions screening enhancement.** High value, low risk, mature technology.
4. **Alert prioritisation** on existing rule output. Same risk profile as #3.
5. **Behavioural baselining.** When measurement supports it.
6. **Network analysis, SAR drafting, other** layers. When foundation supports them.

The common mistake is “we deployed AI without measuring our current state first.”

Glossary

- **Alert.** Automated notification that a transaction or customer pattern may be suspicious and should be reviewed by an analyst.
- **Behavioural baseline.** Expected pattern of activity for a customer or peer group, used to detect deviations. Can be built with rule logic or with machine learning.
- **CDD (Customer Due Diligence).** Process of verifying a customer’s identity, business purpose, and source of funds, with ongoing monitoring.
- **Deployer.** Under the AI Act, the entity using an AI system for its own purposes. Distinct from “provider” (who builds it).
- **Dynamic threshold.** An alert threshold that varies based on customer segment, product, geography, or risk band. Different from a static threshold.
- **EDD (Enhanced Due Diligence).** Deeper diligence applied to higher-risk customers.
- **False positive.** An alert that turns out not to indicate a crime.
- **High-risk AI.** Under the EU AI Act, AI systems falling under Annex III categories (or Article 6(2)) that face the most stringent compliance obligations.
- **Identification (biometric).** Determining who a person is by matching their biometrics against a database. Distinct from verification.
- **KYC (Know Your Customer).** Onboarding process to identify and verify a customer.
- **MLRO (Money Laundering Reporting Officer).** Institution’s designated AML compliance lead.
- **PAD (Presentation Attack Detection).** Technical countermeasure against fake faces, masks, and spoofs in biometric systems.
- **Profiling.** Processing personal data to evaluate aspects of a person’s behaviour or characteristics.
- **RegTech.** Regulatory technology; software used to support compliance.

- **SAR / STR.** Suspicious Activity Report (US) / Suspicious Transaction Report (EU). Filed with the Financial Intelligence Unit.
- **Suppression logic.** Rule mechanism that mutes repeat alerts after prior dispositions, to reduce noise.
- **Transaction monitoring (TM).** Automated review of transactions for suspicious patterns.
- **Verification (biometric).** Confirming that a person is who they claim to be by matching their biometrics to a presented document. Distinct from identification.

Source bibliography (primary sources cited in the talk)

Regulation

- Regulation (EU) 2024/1624, Anti-Money Laundering Regulation (AMLR), particularly Articles 6(1)(c), 6(5)(b), 75. *Applies from 10 July 2027.* <https://eur-lex.europa.eu/eli/reg/2024/1624/oj/eng>
- Regulation (EU) 2024/1640, AML Directive 6 (AMLD6). <https://eur-lex.europa.eu/eli/dir/2024/1640/oj/eng>
- Regulation (EU) 2024/1620, establishing AMLA. <https://eur-lex.europa.eu/eli/reg/2024/1620/oj/eng>
- Regulation (EU) 2024/1689, EU AI Act, particularly Articles 5, 6(2), 6(3), 9, 10, 11, 13, 14, 14(5), 15, 26, 50, 86, 113. *High-risk obligations apply from 2 August 2026.* <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- Regulation (EU) 2024/886, SEPA Instant Regulation. <https://eur-lex.europa.eu/eli/reg/2024/886/oj/eng>
- Regulation (EU) 2016/679, GDPR, particularly Article 22. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Regulation (EU) 2024/1183, EU Digital Identity Wallet (eIDAS 2). *Each Member State must provide at least one certified EUDI Wallet by end of 2026.* <https://eur-lex.europa.eu/eli/reg/2024/1183/oj>
- ECB digital euro framework-agreement procurement notice (Risk-and-fraud-management lot; Feedzai S.A. ranked first, Capgemini Deutschland GmbH ranked second; max EUR 237.3M; re-estimated EUR 79.1M; up to 15 years). PDF: <https://www.ecb.europa.eu/ecb/jobsproc/proc/pdf/2025-ojs189-00646738-en-ts.pdf> · ECB MIP news announcement 2 October 2025: <https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews251002.fr.html>
- Regulation (EU) 2023/1113, Funds Transfer Regulation (TFR). *Recital 11 information-availability principle relevant to AMLA RTS Article 3.* <https://eur-lex.europa.eu/eli/reg/2023/1113/oj>
- AMLA draft Regulatory Technical Standards on business relationships and linked transactions (consultation 9 February to 8 May 2026; final draft to European Commission by 10 July 2026; AMLR Article 19(9) empowerment).

<https://www.aml.europa.eu/consultation-on-amlas-first-set-of-regulatory-technical-standards>

Court of Justice

- CJEU C-634/21 SCHUFA Holding (Scoring), 7 December 2023. <https://curia.europa.eu/juris/document/document.jsf?docid=280649>

EU supervisors

- European Banking Authority. *Opinion and Report on ML/TF Risks* (EBA/Op/2025/10), 28 July 2025. <https://www.eba.europa.eu/sites/default/files/2025-07/13ae2f94-dc04-4a50-9f24-af2808e78944/Opinion%20and%20Report%20on%20ML%20TF%20risks.pdf>
- European Banking Authority. *Report on the Use of AML/CFT SupTech Tools* (EBA/Rep/2025/23), 12 August 2025. <https://www.eba.europa.eu/sites/default/files/2025-08/2ed3b67d-880b-428d-8282-15689f65b12f/Report%20on%20the%20use%20of%20AMLCFT%20SupTech%20tools.pdf>
- European Banking Authority. *AI Act: Implications for the EU Banking and Payments Sector* (factsheet), 21 November 2025. <https://www.eba.europa.eu/sites/default/files/2025-11/d8b999ce-a1d9-4964-9606-971bbc2aaf89/AI%20Act%20implications%20for%20the%20EU%20banking%20sector.pdf>
- ECB Banking Supervision. *From data to decisions: AI and supervision* (interview), 26 February 2024. <https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240226~c6f7fc9251.en.html>
- ECB Banking Supervision. *Technology is neutral, governance is not: AI adoption in the banking sector* (speech), 24 February 2026. <https://www.bankingsupervision.europa.eu/press/speeches/date/2026/html/ssm.sp260224~6c5b64a77a.en.html>
- Joint ESAs (EBA, ESMA, EIOPA). Factsheets on online financial frauds and scams in an AI world (two factsheets, including the eight-page factsheet on digital-asset-related scams with 11 warning signs for consumers), 15 December 2025. <https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-key-tips-help-consumers-detect-prevent-and-act-online-frauds-and-scams>
- AMLA. Single Programming Document 2026 to 2028. <https://www.aml.europa.eu/system/files/2026-02/AMLA%20SPD%202026-2028.pdf>
- European Banking Federation and SAS. *Demystifying AI for AML* knowledge-partnership masterclass (Roger Kaiser, EBF Senior Policy Advisor; Stephanie Ora, SAS; Laura von Plötz, Commerzbank), October 2021. Cited for the “tick-the-box → intelligence-led” framing developed by Kaiser in the masterclass commentary. EBF–SAS Knowledge Partnership:

<https://www.ebf.eu/ebf-knowledge-partnerships/ebf-sas-knowledge-partnership/partnership-announcement> PDF: <https://www.ebf.eu/wp-content/uploads/2021/10/EBF-SAS-Knowledge-partnership.pdf>

- European Union Agency for Cybersecurity (ENISA). *Remote ID Proofing Good Practices*, November 2024. Operational EU reference for remote identity proofing; cites ISO/IEC 30107-3 (PAD) and ISO/IEC 19795 as baseline standards. https://www.enisa.europa.eu/sites/default/files/2024-11/Remote%20ID%20Proofing%20Good%20Practices_en_0.pdf
- European Union Agency for Cybersecurity (ENISA). EU Cybersecurity Certification Scheme for the EU Digital Identity Wallet (EUCC-W) — draft published 2 April 2026; final Implementing Act expected by end of 2026. <https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-schemes>

Industry / consortium (additional)

- Wolfsberg Group. *Effectiveness through Collaboration*, June 2022. <https://wolfsberg-group.org/resources/effectiveness/38>
- FATF. *Opportunities and Challenges of New Technologies for AML/CFT*, July 2021. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.html>
- Brookings Institution. Lee, N. T., Resnick, P., Barton, G. *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, 22 May 2019. <https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation/>
- European Banking Federation and SAS. *Demystifying AI for AML* knowledge-partnership masterclass (Roger Kaiser, EBF; Stephanie Ora, SAS; Laura von Plötz, Commerzbank), October 2021. EBF–SAS Knowledge Partnership: <https://www.ebf.eu/ebf-knowledge-partnerships/ebf-sas-knowledge-partnership/partnership-announcement> PDF: <https://www.ebf.eu/wp-content/uploads/2021/10/EBF-SAS-Knowledge-partnership.pdf>

Court of Justice and national courts

- College van Beroep voor het bedrijfsleven (Netherlands). *bunq vs De Nederlandsche Bank*, ECLI:NL:CBB:2022:707, 18 October 2022. Open AML standards under the Dutch Wwft accommodate documented AI-based screening methodology. <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:CBB:2022:707>
- Court of Justice of the European Union. C-634/21 SCHUFA Holding (Scoring), 7 December 2023. <https://curia.europa.eu/juris/document/document.jsf?docid=280649>

National supervisors

- Banque de France / ACPR. Sanctions decision on Caisse régionale de Crédit agricole mutuel du Languedoc (procedure 2021-05), 1 December 2022. First operational use of LUCIA documented; reprimand and €1.5M sanction; 540 GB / 750M payment operations from Jan 2018 to Jun 2020 analysed. <https://acpr.banque->

france.fr/sites/default/files/media/2022/12/07/20221207_decision_crcam_languedoc.pdf

- Banque de France. Denis Beau speech, 5 June 2024. <https://www.bis.org/review/r240621d.htm>
- Bank of Lithuania. *2026 m. priežiūros patikrinimų planas* (2026 inspection plan), Decision 2026/441-12, 20 January 2026. Listed institutions in scope: Luminor, Saldo Bank, Lietuvos centrinė kredito unija, RIA Lithuania, B4B Payments Europe, Bendras finansavimas. <https://www.lb.lt/lt/naujienos/lietuvos-bankas-patvirtino-2026-m-prieziuros-patikrinimu-plana>
- Bank of Lithuania. Enforcement records: PayrNet (licence revocation, June 2023), Verse Payments (€280K with personal director fine, March 2023), Foxpay (licence revocation, 22 November 2024), Revolut Bank (€3.5M, April 2025), ZEN.COM (€1.8M administrative fine plus a warning, Bank of Lithuania decision 4 December 2025; complaint filed). Bank of Lithuania enforcement-measures register: <https://www.lb.lt/en/enforcement-measures-1> · ZEN.COM regulatory update statement (12 December 2025): <https://www.zen.com/newsroom/regulatory-update-on-the-supervisory-review-of-uab-zen-com/>
- FCIS Lithuania. *Veiklos rezultatai 2024* (Activity Results 2024), Lithuanian-language annual report. Annual reports index: <https://fntt.lrv.lt/en/money-laundering-prevention/annual-reports/> · English-language press release on 2024 results (82.3K STRs received, sanctions-circumvention typologies): <https://fntt.lrv.lt/en/press-releases/the-fcis-in-2024-over-82-thousand-reports-on-suspicious-transactions-were-received-sanctions-circumvention-schemes-became-apparent/>
- FCA United Kingdom. *New Technologies and Anti-Money Laundering Compliance*, March 2017. <https://www.fca.org.uk/publications/research/new-technologies-and-anti-money-laundering-compliance-report>
- Office of the Comptroller of the Currency (US). *Comptroller's Handbook: Model Risk Management* (index). [https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html](https://www OCC.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html) (cited for model-risk management governance principles, NOT as a source for AML false-positive rates)

Industry / consortium

- Wolfsberg Group. *Statement on Effective Monitoring for Suspicious Activity, Part II: Transitioning to Innovation*, 27 August 2025. Wolfsberg resource page: <https://wolfsberg-group.org/resources/202/>
- FATF. *Horizon Scan: AI and Deepfakes, Impacts on AML/CFT/CPF*, 22 December 2025. <https://www.fatf-gafi.org/en/publications/Methodsandtrends/horizon-scan-ai-deepfake.html>

- Egmont Group. *Horizontal Analysis of AML/CFT Effectiveness in Europe (IO2, IO6, R29, R40)*, 2025/2026. <https://egmontgroup.org/wp-content/uploads/2026/01/EUII-Group-Horizontal-Analysis-of-IO2-and-IO6-Final-version.pdf>
- ENISA. *Threat Landscape: Finance Sector* (covering January 2023 to June 2024), 21 February 2025. https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf

Surveys / analysis

- McKinsey & Company. *The New Frontier in Anti-Money Laundering*. <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-new-frontier-in-anti-money-laundering>
- PwC. *EMEA AML Survey 2026: Mind the gap*, April 2026 (N=531; 40 EMEA countries). <https://www.pwc.lu/en/financial-crime/anti-money-laundering/emea-aml-survey-2026.html>
- SymphonyAI / AML Intelligence. *FinCrime Frontier 2025 to 26*, November 2025 (vendor-tagged). Direct PDF not located on the public SymphonyAI site as of 6 May 2026; closest reference is the SymphonyAI Sensa AML resources page: <https://www.symphonyai.com/glossary/ai/anti-money-laundering-aml/>
- ACAMS. *Global AFC Threats Report 2026*, 28 January 2026 (members-only). Resource page: <https://www.acams.org/en/resource/acams-global-afc-threats-report-2026>
- SAS / ACAMS. *Road to Integration: State of AI/ML in AML*, 25 February 2025 (vendor-sponsored). Direct PDF not located on the public SAS site as of 6 May 2026; closest reference is the SAS AML / financial crime page: https://www.sas.com/en_us/software/anti-money-laundering.html
- Deloitte Ireland. *Navigating the EU AML/CFT Landscape*, 15 October 2025. Direct PDF not located on the public Deloitte Ireland site as of 6 May 2026; closest reference is the Deloitte Ireland regulatory publications page: <https://www.deloitte.com/ie/en/services/risk-advisory/perspectives.html>
- NCA UK. *SARs Annual Report 2023 to 24* (UKFIU). <https://www.nationalcrimeagency.gov.uk/who-we-are/publications>
- FIU-Nederland. *Annual Reviews 2022 and 2023*. Annual reports archive: <https://www.fiu-nederland.nl/en/about-fiu-the-netherlands/publications/annual-review>
- LPA Consulting. *AI and Advanced Analytics in Anti-Financial Crime Compliance*, July 2024. Direct whitepaper PDF not located on the public LPA site as of 6 May 2026; closest reference is the LPA AFC compliance service page: <https://www.l-p-a.com/service/ai-in-afc-compliance/>

Independent benchmarks

- Halford, E., Gibson, I., Newfield, M. and Dhanwala, M. *Developing a scoring model for managing money laundering transactions using machine learning*. Journal of Money

Laundering Control 28(7):30-49, 2025. CC-BY 4.0 open access.
<https://doi.org/10.1108/JMLC-09-2024-0152>

- Allen, J. S. and Hatfield, M. S. S. *Can LLMs Improve Sanctions Screening in the Financial System? Evidence from a Fuzzy Matching Assessment*. Federal Reserve Board, FEDS staff working paper 2025-092, 2025. <https://doi.org/10.17016/FEDS.2025.092>
- Smith, C., Sesodia, M., Lindenberg, F., Schroeder de Witt, C. *OpenSanctions Pairs: Large-Scale Entity Matching with LLMs*. arXiv:2603.11051, 2026 (pre-print). <https://arxiv.org/abs/2603.11051>
- Jullum, M. et al. *Detecting money laundering transactions with machine learning*. Journal of Money Laundering Control 23(1):173-186, 2020. <https://doi.org/10.1108/JMLC-07-2019-0055>
- Jensen, R. I. T. and Iosifidis, A. *Qualifying and raising anti-money laundering alarms with deep learning*. Expert Systems with Applications 214:119037, 2023. <https://doi.org/10.1016/j.eswa.2022.119037>
- Eddin, A. N. et al. *Anti-Money Laundering Alert Optimization Using Machine Learning with Graphs*, 2022 (vendor-co-authored, Feedzai). <https://arxiv.org/abs/2112.07508>
- Leibig, C. et al. *Combining the strengths of radiologists and AI for breast cancer screening: a retrospective analysis*. The Lancet Digital Health 4:e507-e519, 2022. [https://doi.org/10.1016/S2589-7500\(22\)00070-X](https://doi.org/10.1016/S2589-7500(22)00070-X)

Innovation priorities and industry surveys

- Moncalvo, D., Oliva, M. and Díaz Castellano, A. *Innovation practices and priorities in AML/CFT financial intelligence*. Journal of Money Laundering Control 28(4-5):626-644, 2025. EFIPPP Innovation Working Group survey of 44 institutions across 21 countries. <https://doi.org/10.1108/JMLC-05-2025-0063>

Academic literature on AI and AML (additional)

- Akartuna, E. A. et al. *Motivating a standardised approach to financial intelligence: a typological scoping review of money laundering methods and trends*. Journal of Experimental Criminology, 2024. PRISMA-compliant review of 105 typologies-and-trends reports identifying 16 typologies, 200+ value instruments, 200+ actors/entities, and 2,565 red-flag indicators. City University of Hong Kong + UCL Department of Security and Crime Science. <https://doi.org/10.1007/s11292-024-09623-y>
- Bakry, A. N., Alsharkawy, A. S., Farag, M. S. and Raslan, K. R. *Automatic suppression of false positive alerts in anti-money laundering systems*. The Journal of Supercomputing 80:6264-6284, 2024. ASXAML framework using XGBoost + Optuna + RFECV; F-beta 0.86, 73% FP reduction at 92% recall. Al-Azhar University, Cairo. <https://doi.org/10.1007/s11227-023-05708-z>
- Han, J., Huang, Y., Liu, S. and Towey, K. *Artificial intelligence for anti-money laundering: a review and extension*. Digital Finance 2:211-239, 2020. Foundational survey including

next-generation NLP/deep-learning framework proposal. Affiliations: Vanke Service Research (Shenzhen), University College Dublin, KPMG Ireland. <https://doi.org/10.1007/s42521-020-00023-1>

- Pavlidis, G. *Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era*. Journal of Money Laundering Control, 2023. Examination through FATF San Jose principles, OECD AI principles, and EU AI Act lens. Neapolis University, Paphos, Cyprus. <https://doi.org/10.1108/JMLC-03-2023-0050>
- Singh, C. *Is generative AI (artificial intelligence) the next advent in the evolution of finance and navigating financial crime and regulation?* Journal of Financial Crime, 2024. UK FinTech / RegTech regulatory perspective. Holborn Chambers, London. <https://doi.org/10.1108/JFC-07-2024-0232>
- Horobets, N., Reznik, O., Maliyk, V., Vyhivskiy, I. and Bobrishova, L. *Artificial intelligence technologies in banking: challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives*. Journal of Money Laundering Control 28(4-5):593, 2025. Examines tension between legal compliance and AI's technological capabilities in banking AML; argues for specific EU regulation of AI use in finance. <https://doi.org/10.1108/JMLC-03-2025-0041>
- Karthikeyan, G. K. and Bhowmik, B. *Intelligent money laundering detection approaches in banking and e-wallets*. Journal of Computational Social Science 8:91, 2025. State-of-the-art survey including class-imbalance solutions and e-wallet detection strategies. <https://doi.org/10.1007/s42001-025-00421-8>
- Khan, A. A. et al. *BAML: blockchain-driven federated learning anti-money laundering framework*. Peer-to-Peer Networking and Applications 18:270, 2025. Hyperledger Fabric + Federated Learning prototype; simulation results 30% FP reduction, 25% detection improvement. <https://doi.org/10.1007/s12083-025-02086-6>
- *Explainable artificial intelligence models for detecting suspicious bank transactions*. International Journal of Machine Learning and Cybernetics 17:111, 2026. Hybrid intrinsic-plus-post-hoc XAI framework with F1 0.54-0.63 (AML) / 0.66-0.78 (fraud) on synthetic datasets. <https://doi.org/10.1007/s13042-026-02994-w>
- Ajagbe et al. *Anomaly detection for fraud and money laundering: machine learning algorithms comparison*. Discover Artificial Intelligence 5:144, 2025. Caveat: reported metrics (1.0 across accuracy/precision/recall/F1 on the dominant model) suggest overfitting and should be treated cautiously. <https://doi.org/10.1007/s44163-025-00397-4>

Privacy-Enhancing Technologies references

- EU Joint Research Centre, Privacy-Enhancing Technologies (PETs) — JRC Technical Report and related publications. https://joint-research-centre.ec.europa.eu/scientific-activities-z/privacy-enhancing-technologies_en

For education and discussion only. Not legal advice. Please do your own legal research before relying on it for compliance decisions.

- Tookitaki AFC Ecosystem (federated-learning AML platform; Typology Repository with 1,200+ curated scenarios). <https://www.tookitaki.com/afc-thoughts/tookitaki-afc-ecosystem-aml-transformation>
- Consilient (federated learning for financial crime). Federated-learning AML platform page: <https://www.consilient.com/our-platform/>
- Roseman Labs (homomorphic encryption / MPC; CBI Sandbox cohort 1). Roseman Labs financial-services solutions page: <https://rosemanlabs.com/solutions/financial-services/>

Adversarial knowledge frameworks

- MITRE Center for Threat-Informed Defense. *Fight Fraud Framework (F3)*, launched 9 April 2026 (Apache 2.0). Seven tactics covering the fraud-incident lifecycle from Reconnaissance through Monetisation; F1XXX-series technique identifiers; community-contributable. <https://ctid.mitre.org/fraud>
- FS-ISAC. *Cyber Fraud Prevention Framework* (“Leveling Up: A Cyber Fraud Prevention Framework for Financial Services”), 1 April 2025. Five-phase model: Reconnaissance → Initial Access → Positioning → Execution → Monetisation. Direct PDF: <https://www.fsisac.com/hubfs/Knowledge/Fraud/CyberFraudPreventionFramework.pdf>
- AMLTRIX (Amlyze, openly licensed under a custom open license based on Creative Commons principles; STIX 2.1 + ATT&CK Navigator machine-readable exports). <https://framework.amltrix.com/>

Trade finance and document AI

- Cleareye. *Natural Language Processing in Finance: Trade Compliance*. Trade-finance NLP and document AI vendor reference for sanctions-evasion detection in trade documents. <https://cleareye.ai/natural-language-processing-in-finance-trade-compliance/>
- *AI driven transformation in trade finance: A roadmap for automating letter of credit document examination*. ScienceDirect, 2025. Reports up to 68.3% process-risk reduction in LC document examination. <https://www.sciencedirect.com/science/article/pii/S2666954425000250>
- Trade Finance Global. *Using AI to combat financial crime*. <https://www.tradefinanceglobal.com/posts/using-ai-to-combat-financial-crime/>
- Windward. *2025 Sanctions: Trends, Evasion & Compliance Shifts*. Maritime sanctions-evasion detection vendor reference. <https://windward.ai/blog/sanctions-enforcement-is-evolving-are-you/>

Amlyze public commentary

- Amlyze. *Monitoring Before the Relationship — What AMLA’s Draft RTS Means for Transaction Monitoring*, 2026. RegTech-vendor commentary on the AMLA draft RTS (AMLR Article 19(9) empowerment); argues for pre-relationship monitoring as a first-class system requirement, critiques the 3-transactions-in-12-months and 1-month-rolling-

For education and discussion only. Not legal advice. Please do your own legal research before relying on it for compliance decisions.

period mechanical thresholds, references the 24-hour rolling period precedent under AMLD4 in Lithuania (MONEYVAL-evaluated), emphasises the “information available” principle from TFR Recital 11. <https://amlyze.com/amla-rtb-transaction-monitoring/>

- Amlyze. *Privacy Preserving Information Sharing in AML/CFT*, 2023 whitepaper. Architecture for synthetic-data exchange, federated learning, and structured shared knowledge. The synthetic-data thread Amlyze publishes on (distinct from AMLTRIX). Direct download URL not located on the public amlyze.com site as of 6 May 2026; local copy referenced in workspace research/vendor-reports/Amlyze_Privacy_preserving_information_sharing_in_AML_CFT_v1a.pdf. Amlyze homepage: <https://amlyze.com/>

Compiled by AMLYZE for participants of the Center of Excellence in Anti-Money Laundering webinar, 7 May 2026. Distribution permitted with attribution. Not legal advice.