ALL AML

Infobrief – December 2025

EU AML/CFT regulation

Status of the Regulatory Technical Standards

From 10 July 2027, the new EU AML/CFT regulatory framework will apply, and obliged entities will need to prepare for it by 2026. Some Regulatory and Technical Standard (RTS) documents, which are considered level 2 acts, will require financial institutions and alternative investment fund managers (AIFMs) to take relevant action within the next year.

In particular, two draft RTS documents published by the European Banking Authority (EBA) in October 2025 are currently under review by the newly established EU Anti-Money Laundering Authority (AMLA) in Frankfurt, and are expected to be enacted by the EU Commission in 2026.

Notably, the recent AML conference organised by the German supervisory authority (BaFin Geldwäsche-Fachtagung 2025) emphasised the importance of these RTS documents.

The RTS under Article 40(2) of Directive (EU) 2024/1640 establishes a common methodology that all supervisors within the EU must apply to provide the AMLA with comparable risk profiles of their obliged entities. To feed the dedicated risk scoring system, supervisors will have to periodically collect specific data points from obliged entities.

These data points, which are used to establish inherent risk levels, relate to the risk categories Customers, Products, Geographies, and Distribution Channels. For the customers category, this includes, for example, the number of legal entities with complex corporate structures, the number of customers engaging in high-risk activities and the number of legal entities with at least one UBO located in a non-EEA country. In other words, obliged entities must keep numerous data points up to date and ready for submission to BaFin by the end of 2026.

But it does not stop there. To enable the calculation of residual risk, obliged entities must also provide data on their AML/CFT risk controls. This data must be categorised by governance and compliance function, internal controls and outsourcing, risk assessment, customer due diligence and monitoring, transaction monitoring and suspicious activity reporting, targeted financial sanctions and the group-wide AML/CFT framework. Examples of such control data points include the number of customers for whom customer information was reviewed and updated in the last calendar year, and the number of customers whose CDD data and information does not yet comply with the requirements of Article 20 of the AMLR.

In contrast, the Draft RTS on Customer Due Diligence under Article 28(1) shall only enter into effect together with the AMLR in July 2027. According to the draft RTS, there will be a one-year transition period to apply customer due diligence standards to high-risk clients (i.e. until 10 July 2028), and a five-year transition period for low- and medium-risk clients (until 10 July 2023). Given the aforementioned data reporting obligations and the complexity of the new customer due diligence requirements, obliged entities will need to develop a sophisticated customer data review and update strategy by 2026.

Apart from the aforementioned new periodic customer data update cycles (notwithstanding necessary event-based updates), future customer due diligence standards will include significant new requirements and specifications, mainly in the following areas:

- Modified identification and verification standards for different types of natural and legal persons.
- Understanding of ownership and control structures, particularly complex, multi-tiered ownership structures, with enhanced documentation standards.
- Related to the above, observing many more criteria for identifying beneficial ownership and persons in control, both direct and indirect, through the calculation of beneficial interest or control by other means.
- More concrete research and documentation requirements regarding the source of wealth and funds, particularly in cases where enhanced due diligence is obligatory.
- Extension of risk scenarios involving enhanced due diligence and relevant documentation standards
- Increased risk screening requirements, which now officially include targeted financial sanctions apart from PEPs, high-risk countries and certain unusual transactions.
- Screening for customer high-risk activities (sector-related, as well as concerning professional activities and reputation).

Additional Regulatory Technical Standards (RTS) which are expected to set out more details regarding future PEP screening, sector risk and complex ownership structures have been postponed and will only be published after the Regulation and the RTS on Customer Due Diligence enter into force. In the meantime, however, customer due diligence and data management systems should be designed to be flexible enough to include additional RTS requirements as they are published. Some significant provisions and details of the future AML/CFT regulatory framework are still subject to change. Therefore, the coming years will likely present challenging and interesting audit exercises for obliged entities.

Links:

Regulatory Technical Standards package on compliance of institutions and supervisors with their AML/CFT obligations (European Banking Authority, undated)

EBA Response to the European Commission's Call for Advice on six AMLA Mandates (European Banking Authority, October 2025, pdf)

De-prioritisation of Level 2 acts in financial services legislation (European Commission, 6 October 2025)

7. Fachtagung zur Prävention von Geldwäsche und Terrorismusfinanzierung (BaFin, 20 November 2025)

EU and international – legal and regulatory updates

EU lists Russia as high-risk third country for AML/CFT; FATF removes four countries from grey list

The European Commission on 3 December announced that it had added Russia to the EU's list of high-risk jurisdictions with strategic AML/CFT deficiencies, with the measure expected to apply from early January 2026. Earlier, after the conclusion of its plenary meeting in Paris on 22-24 October 2025, the Financial Action Task Force (FATF) reaffirmed its suspension of Russia's membership due to ongoing geopolitical concerns.

After the same plenary session, FATF also announced that Burkina Faso, Mozambique, Nigeria and South Africa had been removed from its "grey list". The countries were removed from the list, which comprises jurisdictions under increased monitoring due to deficiencies in their AML/CFT regimes, after successfully completing action plans and on-site visits.

The FATF plenary also adopted new guidance on asset recovery, with the aim of improving the confiscation of criminal proceeds worldwide. In addition, mutual evaluation reports for Belgium and Malaysia were formally accepted, marking a shift towards outcome-focused assessments with clear remediation plans. The plenary also addressed emerging risks, including the misuse of generative AI and deepfakes in financial crime, emphasising the need for regulatory and technological adaptations.

Links:

Commission adds Russia to list of high-risk jurisdictions to strengthen international fight against financial crime (European Commission, 3 December 2025)
Outcomes FATF Plenary, 22-24 October 2025 (FATF, 24 October 2025)

Innovative compliance tools: EBA identifies heightened risks

On 28 July 2025, the EBA published its 2025 opinion on the evolving risks of money laundering and terrorist financing in the EU's financial sector. The evaluation highlighted increased vulnerabilities resulting from geopolitical developments, legislative changes and digital transformation. It warned that FinTech firms prioritising rapid growth often exhibited weak AML/CFT controls and poor governance, thereby raising the sector's risk exposure.

Despite promising developments in the sector, the EBA noted that RegTech solutions had led to serious compliance failures when implemented poorly, due to insufficient expertise and oversight. In addition, it noted that crypto-asset service providers (CASPs) remained highly exposed, with many lacking robust AML/CFT systems. The opinion also discussed the significant rise in attempts to circumvent regulation using artificial intelligence, outpacing the defensive capabilities of financial institutions.

The EBA acknowledged the ongoing challenges associated with the implementation of EU sanctions, highlighting that many institutions lacked the necessary systems to ensure effective compliance. However, newly introduced EBA guidelines, which will take effect by the end of 2025, aim to standardise sanctions risk controls across the EU.

Link:

A careless use of innovative compliance products can lead to money laundering and terrorism financing risks, the EBA says in its opinion (EBA, 28 July 2025)

EBA report highlights lessons from supervisory cases to strengthen AML/CFT in crypto firms

On 9 October 2025, the European Banking Authority (EBA) published a report on ML/TF risks in crypto-asset services. The report draws on lessons learned from recent supervisory cases across the EU and emphasises

how competent authorities can improve their oversight of this rapidly evolving sector, particularly in the context of the Markets in Crypto-Assets Regulation (MiCA). It identifies vulnerabilities in crypto businesses and provides guidance on how to improve compliance and oversight.

The report also reveals the strategies that some crypto-asset providers use to evade national AML/CFT supervision, including forum shopping and complex ownership structures. It highlights key safeguards introduced by MiCA and the revised AML/CFT framework, as well as elements necessary for effective application of the new EU rules. Overall, the report promotes the coordinated implementation of MiCA and a proactive approach to mitigating financial crime risks in the crypto sector.

Link:

Supervisors should learn from recent cases to prevent financial crime in crypto firms, the EBA says (European Banking Authority, 9 October 2025)

EBA finds AML/CFT colleges framework is maturing but key challenges remain

On 22 October 2025, EBA published its fifth and final report on the effectiveness of AML/CFT controls, highlighting their success in facilitating information exchange and improving AML/CFT supervision within the EU. However, the report noted that two significant challenges persist: an incomplete risk-based approach to college operations and a lack of meaningful discussion about common cross-border risks and coordinated action.

Although the colleges are now well-established and stable, efforts to identify and address cross-group risks remain limited. From 1 January 2026, responsibility for monitoring these colleges will transfer to AMLA, marking a new phase of enhanced supervisory coordination and effectiveness.

Link:

The AML/CFT colleges framework is maturing, the EBA finds (European Banking Authority, 22 October 2025)

Germany – legal and regulatory updates

BaFin AML/CFT Conference: Risk first, CFT focus and AMLA readiness

In a keynote speech at German financial regulator BaFin's 7th Conference on the Prevention of Money Laundering and Terrorist Financing on 20 November 2025, Executive Director Birgit Rodolphe emphasised that a successful anti-money laundering and countering the financing of terrorism (AML/CFT) strategy is dependent on a rigorous, risk-based approach. She stressed that prevention measures must be tailored to the risk taken, rejecting a "one-size-fits-all" method. According to Rodolphe, institutions – including small entities – must ensure the quality of their safeguards matches the risk profile of their activities, demanding that they truly know their customers and understand their business models.

A specific concern raised was the lack of focus on CFT. Unlike money laundering, terrorist financing often involves small amounts of legal funds. BaFin expects institutions to adjust their transaction monitoring to actively assess TF risks beyond indicators of illegal funds.

The speech also touched upon evolving geopolitical threats and sanctions noting that High-risk circumvention transactions, especially those linked to Iran and Russia are of concern. Institutions are expected to apply Enhanced Due Diligence where elevated sanctions risks exist (e.g., trade deals to countries close to sanctioned nations, or the use of crypto transfers). Deliberate sanctions circumvention mandates the termination of business relationships.

Finally, Rodolphe highlighted the establishment of the Anti-Money Laundering Authority (AMLA), which will bring uniform EU standards, prevent "regulatory arbitrage" and pool cross-border expertise. According to Rodolphe, AMLA will become a coordination hub and directly supervise about 40 select, high-risk EU institutions (e.g., payment service providers and crypto businesses). She also strongly urged all obliged entities to start getting prepared for the new AML/CFT regime, which will come into effect in July 2027.

Link:

Entscheidend in der Geldwäscheprävention ist immer das Risiko (BaFin, 20 November 2025)

New guidance from BaFin and FIU on suspicious activity reports

On 28 November 2025, BaFin and the German Financial Intelligence Unit (FIU) updated their orientation note on Section 43 of the German Money Laundering Law (Geldwäschegesetz, GwG) to clarify what "immediacy" and "completeness" means in practice, after consultations across financial and non-financial sectors. According to the new note Suspicious Transaction Reports (STRs) should be well researched, comprehensive and include a chronological record of investigative steps leading to the filing (completeness).

The guidance aims to prevent "defensive reporting" and clarifies that STRs, once complete, must be submitted no later than the following working day (immediacy).

It features five case studies, based on the results of the consultation, which are intended to facilitate and improve classification during practical, everyday tasks.

Links:

Geldwäscheprävention: Aktualisierte Orientierungshilfe zu Verdachtsmeldungen (BaFin, 28 November 2025)
Orientierungshilfe von BaFin und FIU zu Verdachtsmeldungen (FIU, undated)

AML/CFT enforcement action

BaFin fines JP Morgan record amount of EUR 45 million

On 6 November 2025, BaFin announced that it had fined JP Morgen SE EUR 45 million, the largest penalty it has issued to-date, for shortcomings in anti-money laundering controls. The fine was specifically linked to the bank's failure to submit STRs in a timely fashion to the FIU. It underlines the importance of STRs in assisting the FIU in effectively fulfilling in its mandate to identify potential criminal activity, and then provide leads and intelligence to law enforcement agencies for further investigation.

Notably, JP Morgan Chase was the subject of a New York Times report in September 2025, examining its relationship with Jeffrey Epstein and focusing on how the bank managed compliance and risk concerns amid the allegations against Epstein. The article detailed internal discussions among bank executives, regulatory pressures and efforts to reassess existing AML protocols.

The period during which BaFin identified shortcomings was between October 2021 and September 2022. Following BaFin's announcement, JP Morgan clarified that the timing of its STRs did not impede investigations and that remediation measures had been implemented. The case reiterates BaFin's resolve to ensure that Germany's financial sector has robust AML/CFT compliance frameworks in place.

Links:

Shortcomings in money laundering prevention: administrative fine of 45 million euros imposed on J.P. Morgan SE (BaFin, 6 November 2025)
How JPMorgan Enabled the Crimes of Jeffrey Epstein (New York Times, 8 September 2025)

BaFin imposes EUR 3.8 million fine on Varengold Bank

BaFin on 16 September 2025 announced that it had imposed a total fine of EUR 3.8 million on Varengold Bank AG due to severe and persistent deficiencies in its anti-money laundering controls. Regulatory inspections from 2022 to 2023 and a special audit in 2022 revealed weaknesses in fundamental areas such as risk assessment, IT transaction monitoring, customer due diligence and internal safeguards.

Of particular concern were violations relating to transactions linked to Iran, which require heightened scrutiny due to sanctions and elevated money laundering risks.

BaFin found that Varengold had failed to comply with supervisory orders banning certain Iran-related transactions, resulting in further coercive fines.

Link:

Announcements regarding Varengold Bank AG (BaFin, 16 September 2025)

C24 Bank ordered to strengthen AML/CFT controls and resources

On 24 November 2025, BaFin ordered C24 Bank GmbH to remediate deficiencies in its internal organisation and risk management related to AML/CFT. The measures require stronger internal safeguards, customer due diligence, ongoing transaction monitoring and processes for higher risk relationships. The bank was ordered to ensure appropriate staffing, clear responsibilities and adequate technical resources, with BaFin keeping the bank under close supervision and warning of further steps if remediation stalls.

Link:

Mängel in der Geldwäscheprävention: BaFin ordnet Maßnahmen gegen C24 Bank an (BaFin, 24 November 2025)

🔍 Financial crime and cybercrime investigations

Organised crime: Key insights from BKA's 2024 National Situation Report

The German Federal Criminal Police Office (Bundeskriminalamt, BKA) in October published its 2024 National Situation Report on organised crime (Bundeslagebild Organisierte Kriminalität). The report revealed that the threat level in Germany remained persistently high, with 647 investigations conducted, over 70 percent of which involved transnational actors. Organised crime caused damages amounting to around EUR 2.6 billion in 2024, with cybercrime accounting for almost 70 percent of these losses.

Money laundering was central to 146 proceedings, involving a financial volume of around EUR 230 million – with a notable increase in the use of cryptocurrencies and crypto mixers to obscure funds. Common methods included investing in real estate vehicles and businesses, as well as exploiting international financial networks to evade detection. However, only EUR 94 million were seized by the German authorities, highlighting the significant discrepancy between profits generated by criminal activity and funds recovered by the investigative authorities. The report emphasised the urgent need for improved international cooperation and targeted investigations to counter increasingly sophisticated money laundering tactics.

Link:

Bundeslagebild Organisierte Kriminalität 2024: konstant hohes Bedrohungspotenzial (BKA, 24 October 2025)

German authorities dismantle global EUR 300 million 'chargeback' fraud network

The BKA on 5 November 2025 reported the successful completion of Operation Chargeback, an extensive international operation targeting highly professional, worldwide fraud and money laundering networks.

This joint effort – involving the BKA, FIU, BaFin and international partners – resulted in the execution of 18 arrest warrants and searches of more than 60 properties across Germany and eight other countries on 4 November.

The networks are accused of systematically misusing the credit card data of more than 4 million cardholders from 193 countries between 2016 and 2021. The scheme's methodology was based on high-volume, low-value fraud:

- Fake subscriptions: Suspects allegedly generated over 19 million fraudulent subscriptions via approximately 2,000 fake websites (primarily for streaming, dating and entertainment).
- Crime-as-a-service: CaaS Vendors used to supply fake directors and forged KYC documents for shell companies mainly registered in the UK and Cyprus.
- Evasion of detection: The monthly fees charged to the compromised cards were intentionally kept small and disguised with cryptic payment references to avoid immediate detection by cardholders.
- The German nexus: The investigation revealed that the suspects allegedly exploited the infrastructure of four major German payment service providers, positioning Germany's financial hub as a key central location for receiving and distributing the illicit funds.

The total damage resulting from this sophisticated operation is estimated at more than EUR 300 million in actual charges to cardholders, with attempted losses reaching an estimated EUR 750 million. In Germany alone, assets worth EUR 35 million were secured during the raids.

The investigation was initially triggered by analysis conducted by the FIU that recognised a distinct pattern from numerous individual STRs submitted by financial institutions. The authorities targeted 44 individuals, including insiders such as compliance and risk managers working within the payment firms.

Link:

"Operation Chargeback" (Bundeskriminalamt (BKA), 5 November 2025)

Online money laundering service cryptomixer.io taken down

An international investigative team on 26 November 2025 took down the online money laundering service Cryptomixer.io and seized cryptocurrencies worth around EUR 25 million. Servers located in Switzerland, several email accounts and extensive digital evidence from a file hosting provider were also seized during the operation, which was jointly led by the Public Prosecutor General in Frankfurt (ZIT) and the Zurich Cantonal Prosecutor's Office, with the support of the German BKA, Europol and numerous other international authorities.

As a so-called "crypto mixer", Cryptomixer.io anonymised Bitcoin and other virtual asset transactions by pooling and redistributing users' coins in smaller amounts to new addresses, thereby deliberately disrupting traceability. Active since 2016, the mixer allegedly laundered billions in crypto by pooling and redistributing coins to break transaction trails, operating without customer identification.

The investigation is one of a number of recent BKA operations involving infrastructure takedowns, including other mixing services, darknet markets, DDoS "stresser" platforms and major malware such as ChipMixer, Qakbot and Emotet.

Link:

Online-Geldwäschedienst „cryptomixer.io" abgeschaltet (Bundeskriminalamt, 1 December 2025)

Long-running Kaupthing Luxembourg case ends with fines for former executives

A Luxembourg court has closed a 15-year legal case initiated by the duchy's financial regulator CSSF and was linked to the 2008 financial crisis. Three former managers at Kaupthing Bank Luxembourg were fined EUR 75.000 after accepting a consent judgment due to their involvement in questionable financial transactions prior to the bank's collapse.

The case involved accusations of forgery, misappropriation and money laundering relating to the transfer of assets between the Icelandic parent company, its Luxembourg subsidiary and offshore companies. The former managers pleaded guilty, thereby enabling the proceedings, to be closed.

Kaupthing Bank underwent complex restructuring after the crisis, partly supported by Luxembourg and Belgian state aid, which ensured that customer deposits were ultimately refunded. This case follows the earlier convictions of Kaupthing managers in Iceland on similar fraud charges .

Link:

Ex-Kaupthing executives fined after 15-year investigation (Luxembourg Times, 22 October 2025)

Bitkom report: Germany suffers record economic damage from cyber espionage and hacker attacks

A Bitkom study published in mid-September revealed that cyberattacks caused German companies record economic damage of EUR 289.2 billion over the past year, an increase of around 8 percent on the previous year. Nearly nine out of ten companies had been affected by cyberattacks in the previous 12 months, with the attacks increasingly traced back to perpetrators from Russia and China.

Although organised crime remains the most frequent source (68 percent) of these attacks, foreign intelligence services are also implicated in a significant proportion. Ransomware attacks, in which data is encrypted and a ransom is demanded for its release, affected 34 percent of companies, threatening the survival of many businesses.

In response, businesses have increased their security budgets to 18 percent of the overall IT spend. There remains room for improvement; experts recommend allocating one-fifth of the IT budget to security.

Link:

Bitkom-Studie in Deutschland: Rekordschaden durch Spionage und Hacker (ZDF heute, 18 September 2025)

🚫 Sanctions

EU reimposes sanctions on Iran following UN snapback activation

On 29 September 2025, the Council of the EU reimposed a comprehensive set of restrictive measures on Iran. The move followed the activation of the UN "snapback" mechanism, due to Iran's non-compliance with the Joint Comprehensive Plan of Action (JCPOA). The sanctions reinstate trade restrictions on a wide range of goods and technologies, including dual-use items and materials related to Iran's nuclear and military activities. They also impose prohibitions on precious metals and financial services.

The EU has also reintroduced targeted financial sanctions against more than 200 designated individuals and entities, including asset freezes and bans on specialised financial messaging services. Furthermore, the measures restrict Iran's access to international financial networks, prohibit cooperation in the oil and gas sectors, and block certain banking operations with Iranian institutions.

The transport sector faces prohibitions on services to Iranian vessels and to aircraft carrying restricted goods.

Transitional provisions allow some contracts signed before 30 September 2025 to be fulfilled until 1 January 2026.

Link:

Iran sanctions snapback: Council reimposes restrictive measures (European Council, 29 September 2025)

EU adopts 19th sanctions package against Russia

On 23 October 2025, the Council of the EU adopted its 19th sanctions package targeting Russia in response to its ongoing war against Ukraine and amid efforts to close circumvention gaps in previous measures. This package includes a complete prohibition on the import of Russian liquefied natural gas (LNG), more stringent limitations on major Russian energy companies including Rosneft and Gazprom Neft, and actions against Russia's shadow fleet aimed at disrupting energy exports.

In the financial sector, the package includes bans on transactions with an additional five Russian banks, as well as several banks in Belarus and Kazakhstan, due to their support for Russia's war economy. EU operators are prohibited from engaging with Russia's payment systems (Mir and SBP), issuing electronic money or providing crypto asset services to Russia.

Notably, for the first time, the EU is imposing sanctions targeting Russian stablecoins and crypto exchanges, banning the use of the rouble-backed stablecoin A7A5 and related offshore trading platforms. These measures are intended to eliminate loopholes and reinforce the EU's sanctions framework with regard to digital assets.

The package also introduces new rules that limit services provided to the Russian government, as well as travel restrictions on Russian diplomats within the EU. These comprehensive measures are intended to intensify economic pressure on Russia and prevent the circumvention of sanctions by designating entities in third countries that support Russia's military and energy sectors.

Link:

19th package of sanctions against Russia: EU targets Russian energy, third-country banks and crypto providers (European Council, 23 October 2025)

US Treasury sanctions major Russian oil companies in attempt to pressure Kremlin

In response to Russia's failure to engage seriously in a peace process for Ukraine, the US Department of the Treasury announced new sanctions targeting Russia's two largest oil companies, Rosneft and Lukoil, on 22 October 2025. The aim of these measures is to weaken Russia's ability to fund its war efforts by freezing the assets and interests of the companies and their subsidiaries under Executive Order 14024.

Numerous Russian subsidiaries involved in oil and gas production, refining and exploration have also been designated, and all US persons are prohibited from transacting with them unless authorised.

The sanctions also serve as a warning to foreign financial institutions of the risks of secondary sanctions for supporting Russia's military-industrial complex. The Treasury emphasised that the objective of these actions was to encourage positive behavioural change and support a peaceful resolution to the conflict.

Link:

Treasury Sanctions Major Russian Oil Companies, Calls on Moscow to Immediately Agree to Ceasefire (US Department of the Treasury, 22 October 2025)

Venture capital firm fined USD 216 million for sanctions violations

The US Treasury Department's Office of Foreign Assets Control (OFAC) imposed a USD 216 million penalty on the Silicon Valley-based GVA Capital Ltd earlier in 2025 for knowingly violating US sanctions against the Russian billionaire Suleiman Kerimov. The Cayman Islands-registered venture capital firm managed a USD 20 million investment in the US-based LiDAR technology company Luminar on Kerimov's behalf in 2016.

Kerimov was sanctioned in April 2018 for his role as a Russian government official and for alleged money laundering activities involving hundreds of millions of euros. Despite receiving legal advice in 2018 that any transactions involving the shares could not directly or indirectly involve Kerimov, GVA Capital's co-founders engaged in one prohibited transaction and attempted three others with Kerimov's nephew acting as proxy.

OFAC characterised the case as egregious, stating that the firm had undermined US foreign policy by facilitating a sanctioned individual's access to the US financial system.

Link:

Venture capital firm hit with $216 million penalty for 'egregious' violations of US sanctions against Russian billionaire (International Consortium of Investigative Journalists, 9 July 2015)

🔬 Other AML/CFT research reports

Basel AML Index introduces more nuanced risk levels for jurisdictions

The 14th edition of the Basel AML Index, due to be published on 8 December 2025, will introduce a more nuanced tiered system for the categorisation of jurisdictions' money laundering and financial crime risks. Experts participating in the annual review agreed that this change would help users to better identify lower-risk jurisdictions, thereby supporting the smarter application of risk-based AML approaches and the more efficient allocation of resources.

Traditionally, the Basel AML Index, a leading independent risk assessment tool, divided jurisdictions into low-, medium- and high-risk groups – although it recognised limitations due to the large majority clustering at medium risk. To address this issue, the Index will adopt the Jenks natural breaks classification method to redefine the categories as lower, medium and higher risk, with fixed thresholds that reflect the relative risk scores of the 203 jurisdictions included in the Index.

This approach aims to mitigate issues such as indiscriminate de-risking, whereby institutions cut off services to clients or entire countries without a nuanced analysis.

Link:

Identifying lower and higher risk jurisdictions for money laundering: Basel AML Index re-thinks risk levels (Basel Institute on Governance, 3 November 2025)

🪙 Crypto assets

European banks advance euro stablecoin amid heightened AML scrutiny

Nine leading European banks, including Germany's DekaBank, have joined forces to develop a euro-backed stablecoin in the second half of 2026. The stablecoin is intended comply with the EU's Markets in Crypto-Assets Regulation (MiCA) to facilitate fast, low-cost transactions around the clock. The participating banks have set up a new company in the Netherlands to oversee the stablecoin. This entity will be licensed and supervised as an e-money institution by the Dutch central bank.

The introduction of a MiCA-compliant euro stablecoin brings new challenges for transaction monitoring, since it must adhere to the framework for asset-referenced tokens and e-money tokens. Both MiCA and the EU Transfer of Funds Regulation apply the Travel Rule to all crypto transfers, ensuring the transparency of originator and beneficiary data.

As the consortium's stablecoin is designed with compliance in mind, every transaction will carry traceable metadata. However, the shift from IBAN-based monitoring to blockchain-based transfers requires transaction monitoring (TM) teams to track wallet movements and analyse token flows. Real-time screening is essential because stablecoin payments offer instant settlement, which challenges traditional, batch-oriented TM systems.

Integration with blockchain analytics tools is necessary to identify typologies such as wallet dusting, hopping and high-risk smart contract activity.

Links:

Kryptowährung: Neun führende europäische Banken entwickeln Euro-Stablecoin (heise.de, 25 September 2025)

Supervisors should learn from recent cases to prevent financial crime in crypto firms, the EBA says (European Banking Authority, 9 October 2025)

Cryptocurrency exchanges under scrutiny

According to "The Coin Laundry", an investigation by the International Consortium of Investigative Journalists (ICIJ) published on 17 November 2025, the major cryptocurrency exchanges Binance and OKX facilitated hundreds of millions of dollars-worth of illicit digital currency transactions, including funds linked to organised crime and human trafficking scams.

Despite legal action and compliance oversight, Binance received more than USD 408 million and OKX received over USD 226 million in Tether deposits from Huione Group, a financial firm that has been designated by US authorities as a "primary money laundering concern". OKX pleaded guilty to operating illegally, and Binance was assigned a court-appointed monitor following a 2023 plea agreement for AML violations.

The investigation highlighted the challenges that exchanges face in policing transactions amid complex blockchain technology, as well as the tension between compliance and revenue generation. Victims of crypto scams report having little recourse, as law enforcement struggles to trace and recover stolen funds. The study also revealed poorly regulated "cash desks" that allow users to anonymously cash out cryptocurrency outside of regulatory oversight.

Despite the ease of tracing crypto on public blockchains, law enforcement struggles due to a patchwork of global regulation and lack of standardised tools and resources, allowing criminals to obscure fund origins through anonymous wallets and automated swapping services. Any businesses dealing with digital assets or relying on CASPs should conduct Know Your Partner due diligence, focusing on their reputation and track record of freezing funds and cooperating with law enforcement.

Link:

Crypto giants moved billions linked to money launderers, drug traffickers and North Korean hackers (International Consortium of Investigative Journalists, 17 November 2025)

🔒 Information security and data protection

European Supervisory Authorities designate critical ICT providers under DORA

On 18 November 2025, the European Supervisory Authorities (ESAs – comprising of EBA, EIOPA and ESMA) published the first official list of critical ICT third-party providers (CTPPs) under the EU's Digital Operational Resilience Act (DORA). The designation is based on data collected from financial entities' Registers of Information on ICT outsourcing arrangements and a structured assessment methodology mandated by DORA.

In cooperation with national competent authorities from the banking, insurance, pensions and securities sectors, the ESAs carried out a multi-criteria criticality assessment considering systemic importance, support of critical or important functions, and the substitutability of the providers' services. Providers assessed as critical were formally notified and given the opportunity to submit a reasoned statement before final decisions were taken, in order to safeguard due process.

The designated CTPPs deliver a broad spectrum of ICT services, ranging from core infrastructure to business and data services, to financial entities of all sizes across the EU, underlining their pivotal role in the financial ecosystem. Under the DORA Oversight Framework, the ESAs will now directly engage with these providers to assess and promote robust ICT risk management and governance, with the aim of enhancing the operational resilience of the EU's financial sector and mitigating sector-wide ICT risk.

Link:

The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act (EBA, 18 November 2025)

EU Commission proposes simpler digital rules and new digital wallets

On 19 November 2025, the European Commission presented a "Digital Omnibus" package aimed at streamlining and updating existing EU rules on AI, cybersecurity and data. The package aims to reduce regulatory complexity and compliance burdens while maintaining protections for users and fundamental rights.

The proposals adjust the timelines and obligations set out in the AI Act, including the phased introduction of high-risk AI systems and certain transparency duties, such as the labelling of AI-generated content. The proposals also clarify the role of the new EU AI Office, which will be primarily responsible for supervising specific high-risk systems and coordinating enforcement to avoid overlap with national authorities.

Alongside this, the package introduces a framework for an EU-wide digital wallet. This is intended to provide citizens and businesses with a secure, interoperable tool for storing and using digital identity credentials and other official attestations across borders. This will make it easier to access public and private online services in all EU countries, support cross-border transactions and strengthen user control over personal data by establishing common technical and governance standards.

The Commission has positioned the omnibus package as targeted fine-tuning, rather than a reopening of the core legislation, focusing on implementation issues such as transitional periods, conformity assessments and alignment with existing sectoral rules. The package will now be examined by the European Parliament and the Council, who may amend the proposals before any final texts are adopted.

Those involved in digital services, AI and cybersecurity are encouraged to carefully review the proposed adjustments, as these affect deployment planning, labelling and monitoring obligations, as well as interactions with notified bodies and supervisory authorities.

Link:

Simpler EU digital rules and new digital wallets to save billions for businesses and boost innovation (European Commission, 19 November 2025)

Media Recommendations

Why real estate remains a magnet for dirty money (26 November 2025)

In this latest episode of Integrity Insights, Michael Hornsby and Elisabetta Marinoni, researchers working with Transparency International and the Anti-Corruption Data Collective (ACDC), discuss their new study: the Opacity in Real Estate Ownership (OREO) Index. The conversation explores how opaque real estate ownership structures enable corruption and money laundering, why data and legal frameworks both matter, and what their assessment of 24 jurisdictions reveals about global weaknesses in this sector.

Listen to the episode here

Money Laundering-as-a-Service: The booming business of dark web money laundering services (16 October 2025)

In this episode of the Integrity Insights podcast, Daniel Shkedi, Head of Product Marketing and Strategy at Refine Intelligence, talks about Money Laundering as a Service (MLAS) and how cybercriminals are adapting their operations. Daniel provides insights into his research, the typologies of money laundering services offered on the dark web, and why financial institutions need to pay attention to this growing threat.

Listen to the episode here

Two interesting documentaries about money laundering and terrorist financing in Germany are available to watch in the ARD media library.

"Dirty Money – Germany, a Money Laundering Paradise" (**Dirty Money: Geldwäsche-Paradies Deutschland**) shows how billions from drug trafficking, terrorist networks and organised crime flow into the German economy daily.

"German Money for Terror" (**Deutsches Geld für den Terror**) sheds light on how terrorist attacks carried out by groups such as the Islamic State and Hamas are financed with money from Germany.

A recent Deutschlandfunk report deals with the financing of hybrid attacks using cryptocurrencies. In cases of railway sabotage, mysterious drone flights or disinformation campaigns, the perpetrators are often paid in cryptocurrency to conceal their identities, which makes finding evidence difficult. However, the money trail can be traced.

Kryptowährungen. Wie hybride Angriffe finanziert werden (Deutschlandfunk, 1 December 2025)

Imprint

ALL AML GmbH
Hamburger Bahnhof 1
10557 Berlin
www.allaml.eu/

Amtsgericht Charlottenburg HRB 219815
Managing Directors: Dr. Carsten Giersch, Jennifer Hanley-Giersch

For more information see: https://allaml.eu/impressum/

Right of objection and data protection notice

You are receiving this information letter because you are either a client or an interested or associated party.

This newsletter aims to keep you informed about the latest developments in the area of anti-money laundering and terrorist financing. For this purpose, we process your personal data on the basis of Art. 6 (1) p. 1 lit. f) DSGVO or, in case you have given your consent, on the basis of Art. 6 (1) p. 1 lit. a) DSGVO.

If you no longer wish to receive this newsletter, you can opt-out at any time by sending us an e-mail at newsletter@allaml.eu.

For more information on data protection and your rights, please refer to the data protection notice on our website at https://allaml.eu/datenschutz/.