ALL AML

Infobrief 13 – 17th October 2024

Germany – legal and regulatory updates

BaFin – Revised AML/CTF Guidance

On 9 July 2024, the German Financial Supervisory Authority BaFin published a revised draft version of its AML/CFT Guidance and initiated a consultation process inviting obliged entities under the AML Law to send their comments by 9 August 2024.

Although the final outcome of the consultation is not clear at the time of writing, the new Guidance is expected to enter into force in early 2025. It should be noted, that the new Guidance is not meant to anticipate the new EU AML/CFT package approved in 2024, including Regulation 2025/1624 and the still to be published Regulatory and Technical Standards (RTS), applicable for obliged entities by 10 July 2027. The exception is the EU Fund Transfer Regulation 2023/1113, regarding information accompanying transfers of funds and certain crypto-asset, which will be applicable as of 1 January 2025 (see below).

The revised BaFin AML/CFT Guidance is likely to introduce a number of relevant changes concerning the topics of risk assessment and relevant internal safeguards.

The risk management provisions are more pronounced. This concerns in particular the companywide risk assessment, beginning with the detailed steps to be taken in preparing a risk inventory as well as risk identification, including references to relevant sources. Additional guidance on the rating of identified risks has been added. This includes a differentiation between inherent risks and residual risks, taking into account the appropriateness and effectiveness of the relevant prevention measures and safeguards as well as documentary requirements linked to the monitoring of the safeguards' functionality. In addition, any relevant changes to the risk assessment should be summarised in updated versions.

Other elements of the draft provision concern costumer due diligence, including requirements for the identification of legal persons, beneficial owners and politically exposed persons (PEP). Likely to change are the periodic updates of costumer data, replacing „every 15 years" for low risk costumer with a „risk appropriate" criterion, „every 10 years" for medium risk costumer with „every 5 years" and „every two years" for high risk costumers with „annual update". However these provision may only be applicable by 10 July 2027.

The procedures regarding Suspicious Transaction Reporting will also be refined, and relevant adjustments will, together with other changes, be reported in due course, once the final BaFin Guidance is available.

Link:

BaFin announcement on guidance update

Growth cap lifted on N26 after additional fine was imposed

In May 2024, the German neobank N26 was fined EUR 9.2 million by Germany's financial regulator, BaFin, for delays in reporting suspected money laundering in 2022.

This fine was part of ongoing scrutiny over the bank's anti-money laundering (AML) processes, which began after concerns surfaced regarding its compliance with financial crime regulations.

In 2021 BaFin had already imposed a EUR 4.25 million penalty on N26 due to delays in submitting suspicious activity reports for transactions, a deficiency, which BaFin had already urged the bank to address in 2019. The enforcement action saw N26 invest over EUR 80 million to improve its reporting and compliance infrastructure.

One of the most significant developments following the fine was the lifting of a growth cap that BaFin had imposed on N26 in 2021. The cap had restricted the bank to onboarding only 50,000 new customers as opposed to the average of 170,000.. With the cap now lifted as of June 2024, N26 can once again onboard an unlimited number of customers.

N26 continues its discussion with BaFin to address outstanding financial crime and money laundering weaknesses in their AML/CFT compliance program.

Link:

Geldwäscheprävention: BaFin setzt Geldbuße gegen N26 Bank AG fest, 21/05/2024

Germany's North Channel Bank employees face trial in money laundering case

In early June 2024, Germany's Koblenz Higher Regional Court ordered seven former employees of the defunct North Channel Bank to face trial on charges of laundering EUR 160 million tied to tax fraud schemes affecting Denmark and Belgium from 2015 to 2017. The accused, including two former executives, allegedly facilitated large-scale money laundering through the Mainz-based bank, distributing funds derived from false tax claims. Prosecutors state that these funds were linked to fabricated dividend certificates meant to secure fraudulent tax rebates for numerous U.S.-based pension funds, which were largely fictitious.

The North Channel Bank reportedly played a central role in a broader tax evasion network reminiscent of the notorious Cum-Ex scandal. This network leveraged circular stock trades to claim unwarranted tax refunds, exploiting loopholes in dividend taxation. The legal proceedings have encountered delays due to prior court rulings that initially dismissed the charges, reasoning that foreign tax fraud does not constitute a predicate offence under German law. However, the higher court upheld the charges, asserting that jurisdictional location does not exempt money laundering cases.

The trial for former employees of North Channel Bank on charges of money laundering is scheduled to start in January 2025. This trial will be pivotal in determining accountability and closing legal loopholes that allow these types of fraudulent transactions to thrive.

Link:

Banker müssen in riesigem Geldwäschefall auf die Anklagebank, 04/06/2024

Prominent German law firm under investigation due to links to a Russian oligarch

In June 2024, German authorities started investigating whether a partner at the German law firm Pöllath + Partners assisted Russian oligarch Alisher Usmanov in structuring possibly illegal tax arrangements. This investigation, led by the Munich II Public Prosecutor's Office, focuses on the role of these advisors in potentially aiding Usmanov with tax avoidance schemes. Investigators raided Pöllath's Munich office and the tax advisor's premises in Baden-Württemberg, seeking evidence linked to these alleged activities.

The case centres on Usmanov's tax residency status in Germany, with suspicions that he spent substantial time in Bavaria, where he might own multiple properties (formally owned by Swiss trusts). Although Usmanov claims that his primary residence is in Russia and that he pays taxes there, authorities believe he may exert control over the assets held in the Swiss trusts, possibly using advisors as intermediaries. In addition to tax fraud, Usmanov faces charges of violating Germany's Foreign Trade and Payments Act and is under scrutiny for alleged money laundering, with related investigations involving his yacht "Dilbar" and other assets.

Pöllath is one of the most well-known law firms in Germany for wealth advisory services. It provides advisory services to entrepreneurial families, high-net-worth individuals, foundations, and foreign trusts through long-term engagements.

Link:

Hatte der Oligarch Hilfe bei illegalen Steuerdeals, 20/06/2024

Crackdown on unauthorised crypto ATMs in Germany

In August 2024, Germany's financial regulatory authority BaFin executed a crackdown on unauthorised crypto ATMs across the country, targeting operators conducting unlicensed cryptocurrency transactions. This enforcement operation covered 35 locations where crypto ATMs were suspected of facilitating financial transactions without BaFin's approval. The regulatory body stressed the importance of following "Know Your Customer" (KYC) guidelines to mitigate risks of money laundering and fraud associated with these machines.

BaFin's actions reflect its commitment to regulating the crypto market to ensure transparency and user safety, highlighting that unlicensed operators face serious legal consequences, including penalties and potential prison sentences. This aligns with BaFin's broader initiative to tighten control over the digital finance space.

As BaFin continues these efforts, it underscores the need for stricter adherence to licensing requirements and preventive measures against illicit financial activities in the crypto market.

Link:

BaFin-Razzia gegen Betreiber von Krypto-Automaten, 20/08/2024

Germany's Grenke Bank under regulatory scrutiny

In September 2024, Germany's financial regulator, BaFin, instructed Grenke Bank AG, a German financial institution that is part of the Grenke Group, to take corrective measures to strengthen its anti-money laundering (AML) and compliance protocols. BaFin's directive follows a comprehensive audit and annual reporting that revealed weaknesses in the bank's AML framework, particularly in risk assessment, transaction monitoring, and internal control processes.

Grenke Bank AG is required to submit periodic progress reports to BaFin over a 12-month period. These updates will help the regulator monitor the bank's efforts in improving its AML infrastructure and adherence to legal standards.

Link:

GRENKE BANK AG: BaFin ordnet Sicherstellung der ordnungsgemäßen Geschäftsorganisation und Mängelbeseitigung in der Geldwäscheprävention an, 06/09/2024

EU and international – regulatory developments

EU AML/CTF Package in force – Implementation by 2027

In June 2024, a new EU Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) regulatory package entered into force and is due to be implemented by 2027.

The EU AML/CFT Package aims to harmonise AML/CFT regulations across the EU and to close gaps that criminals exploited by transferring funds across jurisdictions. The framework specifies stringent standards for customer due diligence, beneficial ownership transparency, and oversight of crypto transactions, all designed to create a robust system that could adapt to new financial technologies and methods used for illicit finance.

The period between agreement and implementation will allow the EU time to set up the new supervisory authority, AMLA, which us due to start working in 2025, and finalise the operational details necessary for effective enforcement and to select those obliged entities which it will supervise as well as to coordinate with national supervisors and Financial Intelligence Units (FIUs).

During this transition, the European Banking Authority (EBA) plays a supporting role by overseeing AML/CFT compliance within the EU banking sector until AMLA is fully operational. The EBA continues its supervisory tasks, including setting regulatory standards, offering guidance, and coordinating with national authorities to ensure consistent rule application across borders.

AMLA, once fully established, will take over direct oversight of high-risk institutions and work closely with the EBA and national FIUs to enhance intelligence sharing, coordinate responses to cross-border financial crimes, and enforce compliance across financial sectors, reinforcing the EU's collective resilience against financial crime.

Link:

Latest update on Anti-money laundering and countering the financing of terrorism legislative package (including links to FAQs on new rules)

New AML rules for financial advisers in the U.S.

In September 2024, the Financial Crimes Enforcement Network (FinCEN), a bureau within the United States Department of the Treasury, finalised new Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) obligations for "investment advisers" by adding them to the definition of "financial institution" under FinCEN's regulations implementing the BSA and including any adviser registered or required to be registered with the SEC (Registered Investment Advisers (RIAs) and Exempt Reporting Advisers (ERAs)).

These new regulations require investment advisers including venture capital and private equity firms to implement a risk-based AML/CFT program that must be approved by the board of directors or equivalent governing body.

The key components of this program include filing Suspicious Activity Reports (SARs) for transactions involving at least USD 5,000 if they are suspected to be connected to illegal activities or designed to evade regulatory requirements. Investment advisers are also required to comply with recordkeeping and reporting obligations, such as filing Currency Transaction Reports (CTRs) for transactions over USD 10,000 and adhering to the "travel rule" for transfers exceeding USD 3,000.

The rule allows for the delegation of certain compliance functions to third-party service providers, whereby like in the EU, the investment advisers retain full responsibility for their AML obligations. Foreign-located investment advisers are also subject to the rule, but only for advisory activities that occur in the U.S. or involve U.S. clients. The final rule come into force on 1 January 2026.

FinCEN also proposed to apply customer identification program (CIP) requirements. The finalization of the proposed CIP rule is still pending as the US Department of the Treasury and the SEC are reviewing comments on the proposed rulemaking.

Links:

Third Time Was the Charm: FinCEN Finalizes AML Compliance Requirements for Certain Investment Advisers, 09/09/2024

FinCEN Finalizes Anti-Money Laundering Program Rule for Investment Advisers, 03/09/2024

Issues Final AML Program and SAR Filing Requirements Rule for Investment Advisers

FinCEN issues new AML rule impacting registered investment advisers and exempt reporting advisers

FINMA bars HSBC's Swiss unit from new high-risk clients following major AML violations

On 18 June 2024, the Swiss Financial Market Supervisory Authority (FINMA) concluded an investigation into HSBC's Swiss private bank, finding it in serious violation of anti-money laundering (AML) regulations.

FINMA highlighted HSBC's inadequate due diligence of USD 300 million worth of transactions conducted between 2002 to 2015 involving politically exposed persons (PEPs) from Lebanon.

These funds moved between Lebanon and Switzerland through HSBC's Swiss accounts without sufficient screening of the origin, purpose, or legitimacy of the funds. FINMA criticised HSBC's failure to report suspicious activity promptly and mandated the bank to cease new high-risk business relationships, especially with PEPs, until it completes a comprehensive review of its current high-risk and PEP client accounts.

The bank is now required to implement significant corrective measures, including the appointment of an independent auditor to monitor and review its compliance processes and report directly to FINMA. HSBC responded by stating that the findings were based on historic issues and indicated plans to appeal the decision.

Link:

HSBC breached money laundering rules in Switzerland, watchdog says, 03/09/2024

Monaco and Venezuela added to the FATF grey list, Turkey removed

As of 28 June 2024, Monaco and Venezuela were added to the Financial Action Task Force (FATF) grey list. This designation subjects the countries to increased monitoring due to identified deficiencies in its anti-money laundering and counter-terrorism financing (AML/CFT) frameworks.

In the case of Monaco, the FATF cited several specific deficiencies, including inadequate risk assessment related to money laundering and tax fraud from foreign sources, insufficient enforcement of sanctions, and challenges in beneficial ownership transparency. Despite improvements made in response to earlier assessments, the FATF found Monaco's efforts to be incomplete.

With regards to Venezuela, the FATF raised concerns about the country's large informal economy and illegal mining sectors, which pose heightened money laundering risks. Additionally, Venezuela's economic ties with Iran, a high-risk FATF jurisdiction, contributed to concerns around potential terrorist financing risks. The FATF also highlighted a lack of sufficient protocols to effectively monitor and prevent financial crimes, particularly regarding transparency in beneficial ownership and the prosecution of financial crime.

Monaco has committed to collaborating with FATF and MONEYVAL to strengthen its regulatory measures and aims to meet the required standards and be removed from the list by January 2026. The government has since its listing committed to a detailed 18-month action plan, aiming for removal from the grey list by January 2026. This plan includes enhancing its financial intelligence unit, increasing sanctions application, and improving judicial efficiency in handling financial crimes..

Venezuela has not yet publicly announced a specific action plan or timeline to exit the FATF grey list.

Turkey was removed from the list in June 2024 after it had been found to have sufficiently addressed previously identified deficiencies.

Links:

Turkey removed from FATF money laundering grey list in boost to standing, 06/28/2024

Monaco government affirms determination to leave FATF grey list, 06/28/2024

Venezuela set to join SA on FATF "grey list" as sanctions pressure mounts, 06/23/2024

The Austrian Raiffeisen Bank under further regulatory scrutiny

On 28 June 2024, the Austrian Financial Market Authority (FMA) imposed a fine of EUR 2.07 million on Raiffeisen Bank International (RBI) for anti-money laundering (AML) compliance failures. FMA highlighted deficiencies in RBI's due diligence processes in particular in relation to correspondent banks based in Cuba and Bahrain where RBI failed to implement adequate AML controls in place to prevent financial crime.

RBI has contested the FMA's ruling, arguing that the bank fulfilled its AML obligations and plans to appeal the decision. This regulatory action against RBI follows broader scrutiny over its operations in Russia and its overall commitment to maintaining compliance standards amid international sanctions and regulatory expectations.

Beyond the current fine, the US authorities have been scrutinising Raiffeisen's connections to Russia for some time. The US who frequently warn international banks that they could be cut off from the dollar system if they violate US sanctions against Russia have also raised their concerns directly with Raiffeisen.

Link:

FMA-Millionenstrafe für RBI wegen Verstößen gegen Geldwäscheregeln, 06/28/2024

New AML requirements for crypto transactions

In July 2024, the European Banking Authority (EBA) issued Travel Rule Guidelines to address new anti-money laundering (AML) requirements under Regulation (EU) 2023/1113, which extends AML obligations to crypto-asset transactions in addition to traditional financial transfers. This measure aims to apply the same measures to crypto-assets as those used for fiat currencies, mandating detailed identification information for both the senders and recipients of crypto transactions. The guidance will come into force in December 2024.

These guidelines specify the role of Payment Service Providers (PSPs) and Crypto-Asset Service Providers (CASPs) in verifying and documenting payer and payee information. The EBA highlights procedures for detecting, managing, and rectifying missing information to ensure accurate identification linked to cross-border crypto transactions. By establishing a common regulatory framework, the EBA seeks to support European supervisory bodies in enforcing compliance consistently across member states.

The guidelines further address technical limitations, encouraging PSPs and CASPs to achieve interoperability and align data standards across various systems. This aspect is crucial for cross-border compatibility and helps ensure a seamless, standardised approach to data-sharing in financial transactions involving crypto assets.

Notably, the European Banking Authority's Travel Rule Guidelines cover both fiat-to-crypto and crypto-to-crypto transfers. This broad application ensures that all forms of fund transfers, including intra-crypto

transactions, meet anti-money laundering and counter-terrorism financing requirements under EU Regulation 2023/1113.

It is notable in this context that, in early July 2024, Russia's central bank openly encouraged Russian businesses to use cryptocurrencies and other digital assets to facilitate payments with foreign partners to counter Western sanctions imposed over the Ukraine conflict.

Links:

Russian regulator encourages use of crypto to counter sanctions, 07/03/2024

EBA Travel Rules Guidelines

Terrorist financing

EU Council updated Terrorist Sanctions List, listing first far-right entity ever

On 26 July 2024, the EU Council updated its list of designated terrorist organisations adding a new entity, 'The Base', a far-right extremist group implicated in terrorist activities. The Base is the very first far-right organisation to appear on the EU's list of designated terrorist organisations. This move highlights an evolving threat landscape and suggests a notable shift in counter-terrorism priorities within the EU.

The group was founded by Rinaldo Nazzaro in 2018 who according to BBC reports is directing the organisation from Russia. The Base has already been sanctioned by Canada, the UK, Australia and New Zealand.

Following its listing, The Base is subject to the freezing of its funds and other financial assets or economic resources in all EU member states. It is also prohibited for EU operators to make funds and economic resources available to the organisation.

Notably, one month earlier, in June 2024, the United States Department of State designated the Nordic Resistance Movement and its leaders as Specially Designated Global Terrorists, citing their involvement in violent extremist activities and posing a threat to U.S. national security.

Until earlier this month, the only other far-right terrorist group designated under Executive Order 13224 by the US government was the Russian Imperial Movement (RIM), which was sanctioned by the Trump administration in April 2020.

Links:

Sanctions against terrorism: Council renews the EU Terrorist List and designates a new entity

US designates Nordic Resistance Movement, 3 of group's top officials as terrorists, 06/15/2024

Integrity Insights podcast episode with Hans Jacob Schindler

Sanctions

EU's 14th sanctions package tightens grip on Russia: expands energy bans, strengthens financial restrictions, and targets sanctions evasion efforts

The EU's 14th sanctions package against Russia, adopted in June 2024 includes companies and individuals active in the energy and maritime sectors, banning EU investment in Russian LNG projects and restricted access to EU ports for Russian vessels linked to military logistics. The EU also added 27 ships to its sanctions list, targeting those involved in transporting military goods, stolen Ukrainian grain, and LNG components critical to Russia's energy projects.

An additional 69 individuals and 47 entities linked to military, political, and industrial support for Russian activities in Ukraine have been added to the sanctions list.

To address the serious issue of sanctions circumvention, the EU has introduced requirements for foreign subsidiaries of EU firms to ensure compliance with EU sanctions. The package also restricts intellectual property transfers to prevent the misuse of EU-origin technology in Russia.

The package has banned EU-based banks outside Russia from using Russia's SPFS financial messaging system and restricting transactions with third-country banks connected to SPFS. It also prohibits dealings with banks and crypto asset providers supporting Russia's defence industry, aimed at weakening Russia's financial and defence resources. These financial restrictions are complemented by expanded export controls on technology items, machinery, and chemicals that could benefit Russia's military capabilities.

Link:

EU adopts 14th package of sanctions against Russia for its continued illegal war against Ukraine, strengthening enforcement and anti-circumvention measures

US sanctions target Georgian individuals

In recent months, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has taken significant actions against individuals in Georgia, primarily focusing on cracking down on human rights abuses and anti-democratic activities. In September 2024, OFAC sanctioned two Georgian government officials and two private citizens involved in violently suppressing peaceful protests and political opposition.

These sanctions were enacted under the Global Magnitsky Human Rights Accountability Act, which targets individuals responsible for serious human rights violations globally. The Georgian government officials were implicated in using violence against peaceful demonstrators, while the private individuals were linked to media activities that encouraged hate speech and violence against marginalised groups.

Furthermore, the Department of State also took additional steps to impose visa restrictions on more than 60 Georgian individuals and their family members responsible for, or complicit in, undermining democracy in Georgia. These individuals include senior government and municipal figures, business leaders involved in

corrupt practices, persons who have spread disinformation and promoted violent extremism, members of law enforcement who were involved in the beating of protesters, and members of parliament who played a critical role in advancing undemocratic legislation and restricting civil society.

OFAC's actions are part of a broader U.S. response to concerns over the erosion of democratic freedoms in Georgia, including the controversial "foreign influence" law passed in May 2024, which restricts the activities of NGOs and media receiving foreign funding. This law has been widely criticised for stifling free speech and aligning Georgia with anti-democratic policies.

Links:

Treasury Sanctions Georgian Officials and Extremists for Serious Human Rights Abuse
U.S. sanctions four Georgians for human rights abuses under Global Magnitsky Act, 09/16/2024

Russian oligarch fights back against Luxembourg

The Russian oligarch Mikhail Fridman was sanctioned by the EU in 2022 due to his alleged ties to the Russian government. The sanctions led to a freeze on his extensive asset base across Europe, impacting his business operations.

In early 2024 Fridman successfully challenged his inclusion on the EU sanctions list, arguing that the sanctions were imposed without due process. However, the legal complexities surrounding the unfreezing of his assets remain unresolved. He launched a lawsuit against Luxembourg in early August 2024 due in order to resolve the issue of the asset freeze despite Fridman being partially removed from the EU sanctions list.

If Fridman wins the court case, it could set a precedent for other sanctioned individuals, potentially leading to more legal cased filed against the EU's sanctions regime. This case is significant as it could force the EU to reassess its procedures and evidentiary standards for imposing and maintaining sanctions, particularly concerning due process and the protection of investor rights.

Link:

Russian oligarch files $16B claim against Luxembourg over frozen assets, 08/14/2024

United States expand sanctions on foreign banks in effort to cut Russian access to global financial system

In June 2024, the U.S. Treasury expanded its secondary sanctions program on Russia, now targeting any foreign bank transacting with sanctioned Russian entities. Previously, only financial institutions directly involved with Russia's military-industrial sector faced sanctions. Under a new measure, secondary sanctions now cover over 4,500 Russian entities, including major banks such as Sberbank and VTB. This expansion reflects the U.S. position that Russia has been transformed into a war economy since the full-scale invasion of Ukraine. U.S. Treasury Secretary Janet Yellen emphasised that the objective is to disrupt Russia's access to foreign resources that support its military activities.

This move will heighten risks for financial institutions in countries such as China, that have maintained ties with Russian entities.

Although China and Russia are exploring ways to conduct transactions through a limited number of Chinese banks, these talks are progressing cautiously due to the potential impact of U.S. sanctions. Experts suggest that the expansion is aimed at deterring banks globally from supporting Russia's war efforts by creating legal grounds for imposing penalties on foreign institutions involved in such transactions.

However, as of the end of September 2024, no specific foreign bank has been publicly targeted with sanctions under the expanded U.S. measures on Russian-related financial activities.

Link:

As Russia Completes Transition to a Full War Economy, Treasury Takes Sweeping Aim at Foundational Financial Infrastructure and Access to Third Country Support

Yevgeny Prigozhin's use of Western financial institutions

In October 2024, the Financial Times published a story based on documents leaked analysed by the Center for Advanced Defense Studies (C4ADS), that revealed that the late Russian warlord Yevgeny Prigozhin used major Western banks, including JPMorgan and HSBC, to facilitate payments for Wagner Group operations through his companies like Meroe Gold in Sudan.

Despite being under U.S. sanctions since 2016, Prigozhin managed to bypass restrictions by routing payments through international financial systems thereby moving goods, generate revenue, and support activities that included alleged human rights abuses in Africa, as accused by the U.S. Treasury.

Following Prigozhin's death in 2023, Wagner's African operations, rooted in Prigozhin's business networks, were absorbed by the Russian defence ministry, allowing Moscow to maintain its influence in the region.

Link:

Yevgeny Prigozhin secretly used JPMorgan and HSBC for Wagner payments

Financial crime reports

Over USD 3.1 trillion in illicit funds circulating in global economy in 2023

In late May 2024, Verafin, an anti-money laundering platform owned by Nadsdaq, published its 2024 Global Financial Crime Report emphasizing the vast global impact of financial crime, with over USD 3.1 trillion in illicit funds circulating globally in 2023. This includes USD 782.9 billion in drug trafficking, USD 346.7 billion in human trafficking, and USD 11.5 billion in terrorist financing. Fraud alone accounted for USD 485.6 billion in losses, driven by scams like business email compromise, romance fraud, and elder abuse.

The report highlights the critical need for stronger collaboration between financial institutions, law enforcement, and governments to combat these crimes. It stresses that financial institutions face rising operational costs due to outdated systems and manual processes, making it difficult to detect and prevent

sophisticated financial crime activity. While institutions are investing in compliance and anti-crime programs, many rely on rules-based systems that generate too many false positives, increasing the strain on resources.

In response to evolving threats, the report emphasises the growing role of technology, particularly artificial intelligence (AI), in detecting and preventing fraud. AI is being adopted for tasks such as transaction monitoring, Know Your Customer (KYC) procedures, and sanctions screening. Financial institutions are also seeking to break down internal silos and improve data sharing across organisations to fight financial crime more effectively.

Finally, the report underscores the human cost of financial crime by sharing stories from survivors of fraud, human trafficking, and other crimes. These personal accounts highlight the lasting emotional and financial damage inflicted on victims, reinforcing the urgency of addressing the growing financial crime epidemic.

Link:

Nasdaq examines the state of financial crime, its deep human impact, and how it threatens the integrity of global financial system

Crypto-based money laundering harder to detect, but not impossible

Chainalysis' July 2024 report on money laundering and cryptocurrency highlights the increasing use of cryptocurrencies for money laundering activities, especially as the technology becomes more mainstream. Criminals are leveraging cryptocurrencies to conceal illicit funds from various off-chain crimes such as narcotics trafficking, cybercrime, and fraud. Although public blockchains are transparent, bad actors use techniques like layering, mixers, and cross-chain bridges to obfuscate their transactions and avoid detection.

One of the major trends discussed is crypto-native money laundering, which involves using cryptocurrencies for on-chain crimes, including darknet market sales and ransomware. Criminals often move funds through intermediary wallets to make it harder to trace, a process known as layering.

Link:

Money Laundering and Cryptocurrency: Trends and new techniques for detection and investigation

German Federal Criminal Police Economic Crime Report 2023

The latest report on economic crime in Germany published by the German Federal Criminal Police Bundeskriminalamt ('BKA') in July 2024 reveals a significant decline in recorded cases of economic crime (for the year 2023), marking a 46.8% reduction from the previous year. Despite fewer cases, the total financial damages from economic crimes rose substantially to EUR 2.679 billion, highlighting the ongoing financial risks posed by these offences. This decrease contrasts with recent upward trends, attributed largely to the resolution of a large-scale fraud case in Schleswig-Holstein involving an online dating platform. Economic crime now accounts for only 0.7% of all recorded offences, the lowest level in five years. However, specific areas, such as labour-related crimes and insolvency fraud, showed an increase.

Within the different types of economic crime, notable decreases occurred in fraud (-66.4%) and investment and financing offences (-23.5%), while insolvency fraud cases rose by 12.4%. Health care billing fraud, though down in frequency, saw a sharp increase in financial impact, escalating by 174.1% to nearly 199 million euros in losses. Cases of online investment fraud—often executed through complex networks involving call centres, software providers, and affiliated marketing entities—remain prevalent. This type of fraud frequently uses manipulative schemes, such as the "Pig Butchering" romance scam, which deceives victims via online dating platforms into investing in false opportunities.

The digital space remains a major enabler of economic crime, with internet-related cases growing by 8.8%. Cybercrime tactics, such as email phishing and manipulative social media advertising, are widely used in fraudulent investment schemes.

International cooperation has been critical in addressing this issue, with numerous raids and arrests conducted in coordinated efforts to dismantle call centres and other infrastructure used in these crimes. The highly professional and organised nature of these criminal networks allows perpetrators to adapt quickly to regulatory changes, ensuring continuity of their illicit activities.

The report underscores the need for enhanced cross-border cooperation and an updated regulatory framework to combat evolving digital economic crimes. The blending of economic and cybercrime poses new challenges for law enforcement, emphasising the importance of preventive measures, public awareness, and advanced investigative techniques to identify and dismantle organised crime networks effectively. The Bundeskriminalamt highlights the ongoing necessity for both law enforcement adaptation and public education to reduce the impact of economic crime.

Link:

Bundeslagebild Wirtschaftskriminalität 2023

Cybercrime

First global cybercrime convention drafted by the UN

In August 2024, the United Nations finalised a draft of the UN Convention against Cybercrime, which is expected to be adopted by the General Assembly, marking the first global, legally binding instrument specifically addressing cybercrime. This convention aims to establish unified international measures to combat cybercrime, enhance law enforcement cooperation, and streamline procedures for evidence-sharing across borders. The convention covers various cyber-related crimes, including digital terrorism, drug trafficking, and human trafficking, recognizing the rapid expansion of cyber threats that exploit technology on a massive scale.

Further details on the convention will be available as the UN General Assembly approaches its final adoption phase later this year.

Link:

Draft United Nations convention against cybercrime

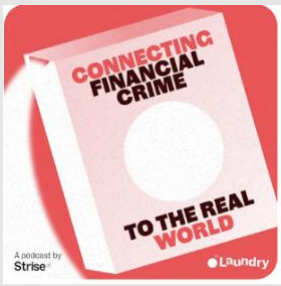
Audio Recommendations

Integrity Insights is a podcast from Berlin Risk, a Berlin-based corporate intelligence and compliance advisory firm. In the podcast, we cover the latest developments in the fields of financial crime, political risk, sanctions, open-source investigations and much more. The podcast is hosted by Filip Brokes, consultant at Berlin Risk.

Episode 7: Countering right-wing extremism with sanctions
(Pod Link)

The Missing Crypto Queen podcast series: Dr Ruja Ignatova persuaded millions to join her financial revolution. Then she disappeared. Why? In the BBC podcast, Jamie Bartlett presents a story of greed, deceit and herd madness.

Episode 12: Wanted: Dead or Alive
(Pod Link)



The Laundry is a podcast hosted by Marit Rødevand and Fredrik Riiser – this podcast features renowned experts from sectors such as banking, fintech, compliance, and investigative journalism.

Episode 98: Which economies are winning from sanctions on Russia?

The Dark Money Files
(Pod Link)

The Suspicious Transaction Report is a podcast which explores challenges posed by illicit finance and practical analysis of the policy responses. The hosts interview top thinkers and influential voices who unpack the complex world of money laundering, corruption, sanctions evasion and illicit flows, and explain how this shapes the evolving global security landscape, and what democracies and international institutions must do to stay ahead when it comes to the financial dimensions of the global threat outlook

Latest episode: A Conversation with Former FATF President
Dr Marcus Pleyer (RUSI)

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 our clients.

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/.