ALL AML

Infobrief 12 – 15 May 2024

Germany – legal and regulatory updates

Financial watchdog fines Commerzbank for violations of supervisory obligations

Germany's financial regulator BaFin on 22 April announced that it had fined Commerzbank AG a total of EUR 1.45 million for violations of supervisory obligations. According to the financial watchdog, due to inadequate monitoring, employees at both Commerzbank and the former Comdirect Bank AG (which was integrated into Commerzbank in November 2020) violated anti-money laundering obligations by not updating customer data on time or sufficiently and by taking inadequate internal security measures. In addition, enhanced due diligence requirements were inadequately applied in three cases.

In its press release, BaFin noted that credit institutions are required to design their supervisory measures to prevent violations of obligations, or at least make such violations more difficult. BaFin also reminded companies of their legal obligation under the Money Laundering Act to update customer data and carry out enhanced due diligence on higher risk customers.

Link:

Money laundering prevention: Commerzbank AG must pay fines, 11/04/2023

BaFin announces measures against Deutsche Bank for transaction monitoring deficiencies

BaFin on 15 April announced that it had on 21 November 2023 ordered Deutsche Bank AG to take specific measures to improve its data processing systems for transaction monitoring to prevent money laundering and terrorist financing. It threatened to impose financial penalties on the bank if the demands – legally binding since 29 December 2023 – were not met. The financial watchdog also extended the mandate of its special representative to Deutsche Bank, appointed on 21 September 2018, in order to evaluate implementation of the order.

In its press release, BaFin reminded credit institutions of the need to continually update transaction monitoring processes to ensure their functionality.

Link:

Money laundering prevention: BaFin threatens penalty payment if deficiencies are not remedied, 15/02/2024

Public prosecutor investigates Signa Group for money laundering

German media on 13 March reported that the Munich public prosecutor had opened an investigation into suspected money laundering at the now-insolvent Signa Group controlled by Austrian entrepreneur Rene Benko. According to reports, the prosecutor suspects that hundreds of millions of dollars from a loan fraud in Germany were funnelled abroad via companies linked to Signa. Multiple companies linked to Signa Group had filed for bankruptcy since December 2023.

Link:

Suspicion of money laundering at Benko's Signa Group

BaFin takes action against Societe Generale's Frankfurt branch for transaction monitoring deficiencies

On 19 February, BaFin announced that it had on 18 January ordered Societe Generale SA's Frankfurt branch to improve its money laundering and terrorist financing prevention measures. Specifically, BaFin noted that the order was a response to significant deficiencies found in the Frankfurt branch's data processing systems for transaction monitoring transactions. Societe Generale's Frankfurt branch must correct this significant deficiency within a specified period, reporting on progress on an ongoing basis.

Link:

BaFin Order: Société Générale S.A. Frankfurt branch must correct a significant deficiency in money laundering prevention

Regulator warns managers over business organisation

BaFin on 20 February announced that it had issued warnings to two managers of an unnamed credit institution for deficiencies in the company's business organisation.

In its press release, BaFin noted that an essential part of proper business organisation is appropriate and effective risk management, which is intended to ensure the ongoing risk-bearing capacity of credit institutions. According to BaFin, as part of their risk management, credit institutions must ensure a functioning overall bank management and adequate risk controls.

Link:

BaFin warns business managers

Watchdog fines fintech for late submission of SARs

BaFin on 7 March announced that it had fined fintech company Solaris SE EUR 6.5 million, in a decision made legally binding on 6 February. BaFin said that the fine had been imposed because the company had "systematically submitted suspicious money laundering reports late". On announcing the fine, BaFin warned credit institutions that suspicious activity reports (SARs) must be submitted to the Financial Intelligence Unit (FIU) "immediately" if there are suspicions that a transaction or other business event could be related to money laundering or terrorist financing. According to Handelsblatt, a Solaris spokesperson said that the penalty related to suspicious activity reports from 2021 that were submitted late, but that the company had tightened its control mechanisms since then.

Links:

Money laundering prevention: BaFin imposes fine on Solaris SE, 07/03/2024

BaFin imposes fine of millions against the Berlin-based fintech

Finance ministry's asset concealment bill may lack teeth

German newspaper Welt on 23 April reported that a bill to combat money laundering being prepared by the German finance ministry may lack critical competences. In order to combat Germany's reputation as a paradise for money launderers, Germany's coalition government was reported to have agreed in principal to a draft law intended to grant new investigative powers with regards to suspicious assets, including to make it possible to clarify the origin of suspicious assets, even if no criminal proceedings have been initiated.

Welt claimed to have seen a draft version of the Asset Concealment Prevention Act (Vermögensverschleierung Bekämpfungsgesetz, VVBG). A special unit – the Investigation Center for Asset Concealment, which is being established as part of the new Federal Financial Crime Agency (FFCA) – will be set up to look into suspicious assets. Under the proposed law, in cases of suspected money laundering, the new authority can ask owners to supply information on the origin of funds. However, according to Welt, there will be no obligation to comply, nor is a direct confiscation of suspicious assets foreseen. Welt reported that the law stated that such requests to provide information would not be "a burdensome administrative act – the declaration is not mandatory and cannot be carried out using coercive means".

Link:

Im Kampf gegen Geldwäsche fehlt Lindners Spezialeinheit eine entscheidende Kompetenz

EU and international – regulatory developments

EU adopts package of new rules to combat money laundering

On February 24, the European Parliament finally adopted its long-awaited legislative package to bolster the EU's efforts in combating money laundering and terrorist financing (AML/CFT). The AML/CFT package – made up of the Sixth Anti-Money Laundering Directive, the EU Single Rulebook Regulation and the Anti-Money Laundering Authority (AMLA) regulation – was first proposed in July 2021.

The new laws:

- mandate increased due diligence and customer identity verification for banks, asset managers, real estate agents and other obligated entities, who must report suspicious activities to financial intelligence units (FIUs);
- impose stricter monitoring on wealthy individuals, cap cash payments at EUR 10,000 and boost efforts to ensure compliance with financial sanctions;
- expands the list of obliged entities, including to most of the crypto sector, including all crypto-asset service providers (CASPs); and
- enhances the powers of FIUs to analyse and detect money laundering and terrorist financing and to suspend suspicious transactions.

A key aspect of the package is the EU Single Rulebook Regulation, which introduces a harmonised AML rule book that will apply across the bloc, with the intention of eliminating local differences in AML legislation. Fund managers should be aware that they will be obliged to apply enhanced due diligence to so-called high-net-worth individuals (HNWIs). The specific requirements will be set out in the yet to be drafted Regulatory and Technical Standards (RTS) which will be prepared with the help of the European Banking Authority (EBA).

The AML package is now awaiting formal adoption by the EU Council before being published in the EU Official Journal.

Links:

New EU rules to combat money-laundering adopted

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

Frankfurt chosen as home for EU's new AML authority

Frankfurt on 22 February won its bid to host the EU's new anti-money laundering body, the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). Frankfurt gained a simple majority in a joint vote between EU MEPs and EU ambassadors, in the culmination of a two-year process that saw the German city beat rivals Brussels, Dublin, Madrid, Paris, Riga, Rome, Vilnius and Vienna in several rounds of voting.

AMLA will be created as part of the wider package of reforms to the EU's AML/CFT framework that was adopted by the EU parliament on 24 April. The new authority will have direct and indirect supervisory powers over obliged entities. It will also intervene in case of supervisory failures and impose sanctions and other measures. AMLA is expected to begin operations in mid-2025 and have at least 400 staff.

Links:

Frankfurt to host EU dirty money watchdog, 22/02/2024
Begeisterung über Ansiedlung der EU-Behörde in Frankfurt, 22/02/2024
Frankfurt will be the home of the EU Anti-Money Laundering Authority

EU adopts corporate due diligence rules relating to human rights and sustainability

The European Parliament on 24 April approved new corporate due diligence rules aimed at mitigating the negative impacts of businesses on human rights and the environment. The Corporate Sustainability Due Diligence Directive (CSDDD) requires EU and non-EU companies meeting certain turnover thresholds to address issues such as slavery, child labour, labour exploitation, biodiversity loss and pollution in their own and their business partners' operations. Companies must integrate due diligence into their policies, seek contractual assurances from partners and adopt transition plans to align with the Paris Agreement's 1.5°C global warming limit.

The rules will eventually apply to all EU-based companies with more than 1,000 employees and a worldwide turnover of more than EUR 450 million. They will also apply to non-EU companies meeting the same thresholds within the EU.

Member states are required to provide detailed online information on the related obligations and establish supervisory authorities to enforce compliance. Penalties for non-compliance include fines up to 5 percent of net worldwide turnover and public naming and shaming. Companies will also be liable for damages and required to compensate victims.

The directive, set to be gradually implemented from 2027 to 2029, will become law after formal endorsement by the Council and publication in the EU Official Journal. Although not currently directly relevant to most investment funds, the new rules may be relevant to portfolio investments depending on the number of employees. Also any infringements under the CSDDD will qualify as predicate crimes to money laundering.

Link:

Due diligence: MEPs adopt rules for firms on human rights and environment

BaFin reminds companies of obligations under EU's new cyber-crime regulation amid growing number of attacks

Germany's Federal Criminal Police Office (BKA) on 13 May published its Federal Cybercrime Situation Report for 2023, which showed a 28 percent increase in cyberattacks committed from abroad but causing damage in Germany compared to the previous year. The report also highlighted an industry survey indicating that cybercrime caused the Germany economy some EUR 148 billion in damages in 2023.

Earlier, BaFin on 12 April reminded German financial sector companies of the requirement to implement the EU's new regulation to protect against cyber threats from next year. According to BaFin, more than 3,600 companies will be subject to the regulation. As an example of the threats faced, BaFin highlighted the cyberattack carried out in the summer of 2023 by the cyber gang Clop, which exploited weaknesses in the MoveIT data transfer program, causing thousands of companies to be affected by data breaches.

The EU Digital Operational Resilience Act (Regulation (EU) 2022/2554) (DORA) aims to enhance the operational resilience of the financial sector, including alternative investment funds (investment funds), by establishing uniform requirements for the security of network and information systems enabling obliged entities to mitigate information and communication technology (ICT) risks and manage disruptions.

Like with the AML/CFT regulatory framework, DORA places the ultimate responsibility for compliance on the management of the fund, requiring it to define, approve, oversee and remain accountable for a fund's ICT risk management framework.

Compliance with DORA is expected by January 2025. Although it is only mandatory for fully licensed investment funds to meet all the requirements by 17 January 2025, smaller investment funds (*registrierte KVG*) should proactively undertake a mapping and gap analysis to define an implementation plan for DORA. This will help smaller funds to develop a realistic

plan of action, ensuring that they will be able to meet the comprehensive requirements over time and be ready once the other requirements linked to the application of a full license become a priority.

Links:

DORA: the countdown has begun

Im Fokus: Bundeslagebild Cybercrime 2023

UAE and Gibraltar removed from FATF 'grey list' but remain on EU high risk jurisdictions list

The EU parliament on 23 April blocked a proposal by the European Commission to remove the United Arab Emirates (UAE) and Gibraltar from the EU's list of AML-related high-risk third countries. This is despite the Financial Action Task Force (FATF)'s 23 February decision to remove both UAE and Gibraltar from its so-called 'grey list' of countries subject to increased monitoring due to the risks posed by financial crime. The Dubai Unlocked data leak published by OCCRP on 14 May showcases many incidents of money laundering in real estate sector in Dubai.

FATF said that it had removed the UAE from its grey list because it had "strengthened the effectiveness of its AML/CFT regime to meet the commitments in its action plan regarding the strategic deficiencies that the FATF identified in February 2022". However, the 23 April decision reflects ongoing concerns about deficiencies in the UAE's AML framework, as well as its status as a hub for illicit financial flows and sanctions evasion efforts. It also means that enhanced due diligence should continue to be applied for investors based in both UAE and Gibraltar.

Links:

European Parliament opposes EC decision to remove Gib from 'high risk' list

UAE dropped from financial crime watch list in win for nation

FATF announces decision to remove the United Arab Emirates from its grey list

Dubai Unlocked

Glitzer, Gangster, Geldwäsche – Datenleck zeigt kriminelle Immobilienbesitzer in Dubai

US to force private fund managers to improve AML/CFT measures

The US Department of the Treasury on 13 February announced a new proposed rule requiring certain investment advisers to comply with AML/CFT measures under the Bank Secrecy Act (BSA). This move targets registered investment advisers (RIAs) and exempt reporting advisers (ERAs), aiming to close gaps in the financial system that have allowed money launderers and corrupt officials to exploit the investment advisory sector. The proposed rule mandates the implementation of risk-based AML/CFT programs, reporting suspicious activities to the Financial Crimes Enforcement Network (FinCEN) and adhering to recordkeeping requirements.

The Treasury Department said that its recent risk assessment identified significant national security risks, including cases where sanctioned individuals and foreign adversaries had utilised investment advisers to invest in US assets and access sensitive information. It noted that, despite some advisers voluntarily applying AML/CFT measures, the lack of comprehensive regulations left the sector vulnerable. The proposed rule is intended to standardise enforcement across the industry, ensuring that violations are met with appropriate penalties, including fines and potential prison sentences.

The rule also seeks to enhance information-sharing between FinCEN, law enforcement and financial institutions. While the proposal excludes immediate requirements for customer identification and beneficial ownership information, these aspects will reportedly be addressed in the future. The comment period for the proposed rule ended on 15 April 2024, with implementation set for 12 months after the final rule's effective date.

Links:

Fact Sheet: Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers and Exempt Reporting Advisers Notice of Proposed Rulemaking (NPRM)

EBA to begin collecting information on natural persons in its AML/CFT database

The European Banking Authority (EBA) on 2 May announced that EU supervisors would now be able to report the names of individuals to EuReCA, its central AML/CFT database. The EBA said that the step was expected to enhance the effectiveness, targeting and informativeness of supervision, bolstering the EU's efforts to combat money laundering and terrorist financing.

EuReCA compiles information on significant AML/CFT deficiencies identified in financial institutions by EU supervisors and the corrective measures taken. Supervisors can now include information on individuals, such as customers, beneficial owners or key management personnel, linked to these deficiencies. Since its inception on 31 January 2022, some 41 authorities have made more than 1,400 entries into EuReCA.

Link:

The EBA will start collecting information on natural persons through its AML/CFT database, EuReCA

UK's FCA warns it will enhance monitoring due to AML failings

The UK's Financial Conduct Authority (FCA) on 5 March issued a letter to CEOs highlighting significant weaknesses in the financial crime controls of Annex 1 firms, which include some lenders, safe custody providers, money brokers and financial leasing companies. This follows recent assessments that revealed common deficiencies in areas such as risk assessment, due diligence and senior management oversight. The FCA has directed these firms to conduct gap analyses and address these shortcomings within six months or face potential regulatory actions.

According to the FCA, the letter signals its intention to enhance its monitoring and adopt a more proactive supervisory approach. Annex 1 firms are urged to evaluate their financial crime controls rigorously to comply with the FCA's expectations.

Link:

Action needed in response to common control failings identified in anti-money laundering frameworks

Panama Papers criminal trial commences in Panama

Reports on 8 April indicated that the first criminal trial in Panama in relation to the Panama Papers data leak had begun. Some 27 defendants stand accused of money laundering by means of the establishment of 215,000 letterbox companies in tax havens, in which politicians, celebrities and athletes were reported to have concealed their wealth. One of the defendants is the German lawyer Jürgen Mossack, co-owner of the now dissolved law firm at the centre of the data leak, Mossack Fonseca.

The trial comes eight years after multiple media outlets, coordinated by the International Consortium of Investigative Journalists, published investigations exposing the offshore financial dealings of powerful individuals around the world. The reports were based on 11.5 million files from Mossack Fonseca leaked to German newspaper Süddeutsche Zeitung.

Links:

Panama Papers trial begins with denials eight years after historic tax evasion exposé

Erste Gerichtsverhandlung zu Panama Papers begonnen, 08/04/2024

Terrorist financing

BaFin increases focus on terrorism financing

BaFin on 6 February issued a press release reminding companies of its increased focus on preventing terrorist financing. According to BaFin, in the past year, the financial watchdog examined the risk analysis, customer acceptance processes and transaction monitoring of selected credit and payment institutions. It emphasized the need for institutions to address specific risks and distinguish between measures for combating money laundering and terrorist financing.

According to BaFin, it previously surveyed more than 40 credit and payment institutions under its supervision to assess their risk of misuse for terrorist financing and the measures they have implemented. The majority were found to be actively addressing the issue and deriving appropriate security measures. Based on these findings, BaFin aims to further raise awareness among obligated institutions about the importance of preventing terrorist financing.

Link:

Terrorist financing: increasing focus on preventive measures, 06/02/2024

Hamburg bank reported to be suspected ‘financial hub’ for Iranian terror

Politico on 9 February reported that a small Hamburg-based bank, Varengold Bank AG, was under investigation by BaFin over alleged money laundering concerns involving Iran's covert financial network. According to Politco, Western intelligence agencies suspect that the bank was used by Iran to funnel money to terror affiliates such as Hezbollah and the Yemeni Houthi rebels, bypassing Western sanctions by laundering the proceeds from illicit oil sales. The investigation has led to a significant reduction in the bank's commercial operations.

Varengold has denied the accusations, claiming that its business with Iran was strictly humanitarian, limited to shipping medical equipment and food. However, intelligence officials believe the bank facilitated transactions linked to Iran's Quds Force, an arm of the Revolutionary Guard that supports terror activities across the Middle East. They allege that Iran's government provides oil to the Quds Force, which sells it through a complex network to obtain hard currency for clandestine operations, primarily targeting China as a buyer. Politico noted that the case served as “a glaring example” of the relative ease with which Tehran was able to circumvent Western sanctions, as well as “underscoring the high risks firms face when they fail to adhere to the highest standards of money laundering prevention”.

Link:

Hamburg bank suspected as ‘financial hub’ for Iranian terror, 09/02/2024

Ex-Israeli spy chief claims targeting Hamas’ financial network could have prevented terror attack

The BBC on 20 February reported that former senior Israeli intelligence officer Udi Levy had in an interview claimed that Israel could have used financial tools to dismantle Hamas' control over Gaza, years before its deadly attack on Israel in October 2023. Levy, who headed economic warfare in Mossad until 2016, said that he had advised Israeli Prime Minister Benjamin Netanyahu to target Hamas's finances.

Levy highlighted a significant funding stream, including a multi-million-dollar investment portfolio managed from Turkey, which he claimed to have brought to Netanyahu's attention in 2014. He contended that if these financial resources had been curtailed, Hamas might not have had the means to build its extensive tunnel network and maintain a 30,000-strong military force. The former spy chief linked Netanyahu's alleged inaction to

the subsequent scale of the 7 October attack, in which approximately 1,200 Israelis were killed and more than 250 hostages taken.

A BBC investigation revealed extensive investments by Hamas across the Middle East and North Africa, including in the construction, pharmaceuticals and real estate sectors. Documents obtained in 2020 suggest that Hamas's investment portfolio may be worth more than EUR 422 million, including substantial real estate assets. The US Treasury Department's Office of Foreign Assets Control (OFAC) has since 2022 sanctioned six of the companies involved.

Link:

Israeli PM 'missed chance' to cut off Hamas cash, says ex-spy chief, 20.02.2024

Sanctions

EU parliament approves law to strengthen sanctions enforcement

The European Parliament on 12 March approved new legislation to standardize the enforcement of EU sanctions across member states. The directive aims to criminalize the violation and circumvention of EU sanctions. It is intended to address inconsistencies in how sanctions are currently applied by establishing common definitions and minimum penalties for offenses such as failing to freeze funds, ignoring travel bans and conducting business with sanctioned entities.

The new rules also specify that circumventing sanctions, such as concealing funds or failing to report required information, will be considered a punishable offense. Violations can lead to prison sentences of up to five years and significant fines for companies, with penalties potentially based on a company's global annual turnover. This measure aims to prevent “forum shopping”, where entities exploit the weakest enforcement among member states, and to strengthen the EU's overall sanctions regime. The directive's implementation will require formal approval by the Council before it becomes law. Once approved, member states will have one year to integrate the provisions into their national laws.

Link:

EU sanctions: new rules to crack down on violations

EU announces 13th package sanctions against Russia

The EU on 23 February adopted its 13th package of sanctions against Russia in response to its war of aggression in Ukraine. The package was focused on further limiting Russia's access to military technologies, including parts for drones, and on listing additional companies and individuals involved in Russia's war effort.

An additional 106 individuals and 88 entities were designated under the package, bringing the total number of listings to more than 2,000. They included 140 companies and individuals linked to Russia’s military-industrial complex, as well as ten companies and individuals involved in shipping armaments from North Korea to Russia. It also included companies both in Russia and third countries that have been supplying key electronic components for drones to Russia.

The package also expanded the list of "advanced technology items that may contribute to Russia's military and technological enhancement or to the development of its defence and security sector" to include: components used for the development and production of drones such as electric transformers, static converters and inductors found (inter alia) in drones, as well as aluminium capacitors with military applications.

Link:

EU adopts 13th package of sanctions against Russia after two years of its war of aggression against Ukraine, 23/02/2024

EU reportedly considers first sanctions on Russia's LNG sector

Politico on 6 May reported that it had seen documents indicating that the European Commission has for the first time proposed sanctions on Russia's liquefied natural gas (LNG) industry. The report claimed that the measures - proposed as part of the EU's 14th package of restrictive measures against Russia - would not bar Russian LNG imports to the EU. However, they would bar countries from re-exporting Russian LNG and ban their involvement in future LNG projects in Russia. The measures would also force companies to share information on their Russian LNG imports.

According to Politico, the measures would mark a "significant shift in strategy" from the EU amid evidence that Western efforts to stymie Russia's revenue from fossil fuels are failing. The report suggested that such sanctions would force Russia to overhaul its LNG business model, which uses Spain, Belgium and France as hubs for exports to Asia.

Link:

EU proposes first sanctions on Russia's LNG sector

US' OFAC cracks down on crypto, terrorism funding

In late March, the US government imposed a series of financial sanctions related to crypto-asset activities, including linked to terrorism financing. Between March 20 and 27, the Treasury Department's OFAC executed four actions targeting individuals and entities accused of online disinformation, sanctions evasion and terrorist financing.

On 20 March 20, OFAC added Ilya Gambashidze, head of the Moscow-based company Social Design Agency, to its sanctions list for spreading Russian disinformation; it also sanctioned two of this individual's addresses for Tether (a cryptocurrency).

On 25 March, it sanctioned two individuals and 13 entities, including crypto exchanges Bitpapa and NetExchange, for providing blockchain services that enable the evasion of Russian sanctions.

The next day, on 26 March, OFAC sanctioned an individual named Tawfiq Muhammad Sa'id Al-Law for aiding the Lebanese organisation Hizbollah with crypto wallets and financial support. It claimed that Al-Law provided Hezbollah with crypto-asset wallets that the Lebanese organisation used to receive funds from Iran.

On March 27, OFAC sanctioned Gaza Now – a Gaza-based online fundraising platform – for raising funds for Hamas after its 7 October 2023 attack on Israel. Several crypto addresses used by Gaza Now were also identified. The UK's Office of Financial Sanctions Implementation mirrored the sanctions on Gaza Now on the same day.

These actions illustrate the critical necessity of robust sanctions due diligence for investors involved in the cryptocurrency industry.

Links:

Treasury Sanctions Hamas-Aligned Terrorist Fundraising Network

Counter Terrorism Designations; Syria Designations

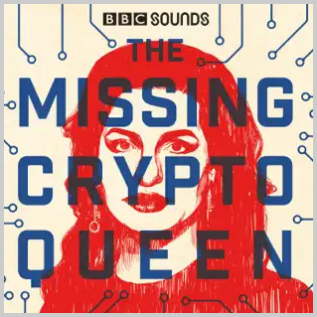
Treasury Designates Russian Companies Supporting Sanctions Evasion Through Virtual Asset Services and Technology Procurement

Iran-related Designations; Non-Proliferation Designations; Russia-related Designations

Audio Recommendations

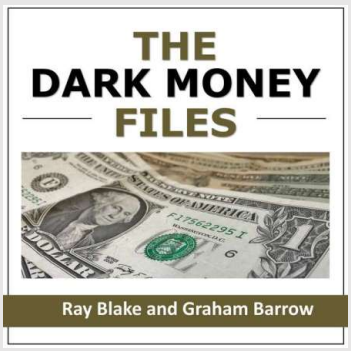
Integrity Insights is a podcast from Berlin Risk, a Berlin-based corporate intelligence and compliance advisory firm. In the podcast, we cover the latest developments in the fields of financial crime, political risk, sanctions, open source investigations and much more. The podcast is hosted by Filip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

Episode 5: Russia-linked Ransomeware attacks
(Spotify / Apple Podcasts)



The Missing Crypto Queen: 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.

Episodes 1-11: The Missing Queen
(Spotify) / (Apple Podcasts)



The Dark Money Files is a podcast on money laundering and wider financial crime issues presented by two financial crime experts, Graham Barrow and Ray Blake.

The Dark Money Files
(Spotify) / (Apple Podcasts)

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/.