About Us

Founded in 2014, Aperio Intelligence is a specialist, independent corporate intelligence firm, headquartered in London. Collectively our team has decades of experience in undertaking complex investigations and intelligence analysis. We speak over twenty languages in-house, including all major European languages, as well as Russian, Arabic, Farsi, Mandarin and Cantonese.

We have completed more than 3,000 assignments over the last three years, involving some 150 territories. Our client base includes a broad range of leading international financial institutions, law firms and multinationals.

Our role is to help identify and understand financial crime, integrity and reputational risks, which can arise from a lack of knowledge of counterparties or local jurisdictions, enabling our clients to make better informed decisions.

Our due diligence practice helps clients comply with anti-bribery and corruption, anti-money laundering and other relevant financial crime legislation, such as sanctions compliance, or the evaluation of tax evasion or sanctions risks. Our services support the on-boarding, periodic or retrospective review of clients or third parties.

Our investigations practice advises clients in a wide range of complex disputes and other contentious matters, including complex cross-border asset tracing claims, litigation support, internal investigations, market intelligence, supply chain analysis and country risk assessments.

Our team has specialist knowledge of and access to a very broad range of public and proprietary data sources, as well as a longstanding network of reliable, informed local contacts, cultivated over decades, who support us regularly in undertaking local enquiries on a confidential and discreet basis. As a specialist provider of corporate intelligence, we source information and undertake research to the highest legal and ethical standards. Our independence means we avoid potential conflicts of interest that can affect larger organisations.

We work on a “Client First” basis, founded on a strong commitment to quality control, confidentiality and respect for time constraints. We offer robust, cost-effective solutions, providing our clients with work of the highest quality at favourable rates.

Please do not hesitate to get in touch with us if you would like to know more about Aperio’s services or discuss how we might be able to help you:

Email info@aperio-intelligence.com or find out more at: aperio-intelligence.com
INTRODUCTION

Welcome to the April 2020 edition of the Financial Crime Digest. News this month continues to be dominated by the impact of the Covid-19 pandemic and in our special feature we review the financial crime impacts of the crisis, together with some of the responses to date from regulators, law enforcement and government agencies. Notwithstanding the volume of Covid-19 information, many other financial crime-related issues continue to develop and emerge; this edition of the Financial Crime Digest covers just a proportion of key updates, more of which are accessible via our online portal. We hope you find the Financial Crime Digest an informative read and welcome your feedback.

EDITOR’S PICKS

ENFORCEMENT

20 April 2020
US authorities fine Korean bank $86m over AML failings and Iran sanctions breaches

SPECIAL FEATURE

30 April 2020
The financial crime implications of the Covid-19 pandemic: an overview

REPORTS AND SPEECHES

17 April 2020
North Korea using ‘clandestine’ financial networks to transact with Iran, finds UN experts

30 April 2020
Chinese money laundering groups control hundreds of UK bank accounts, finds NCA report

DATES FOR THE DIARY

MAY 13
European Commission webinar on enabling an EU framework for markets in crypto-assets

MAY 18
UK Joint Money Laundering Steering Group consultation on its crypto-asset guidance closes

MAY 15
European Banking Authority public hearing on its revised money laundering and terrorist financing risk factor guidelines consultation

MAY 27
UK Treasury Committee deadline for the call for evidence on the economic impact of the coronavirus
US authorities fine Korean bank $86m over AML failings and Iran sanctions breaches

US prosecutors announced on 20 April a $51 million settlement with Industrial Bank of Korea (IBK) to resolve criminal charges that its “deficient” AML programme allowed its former client Kenneth Zong and his companies to funnel more than $1 billion through US financial institutions to the Iranian government in 2011, in violation of the International Emergency Economic Powers Act.

The South Korean state-owned bank entered into a deferred prosecution agreement (DPA) with the US Attorneys’ Office for the Southern District of New York (SDNY) and a non-prosecution agreement (NPA) with the New York Attorney General’s Office (NYAG) after they determined that IBK’s New York branch “wilfully” failed to establish, implement and maintain an adequate AML programme between 2011 and 2014, despite repeated remedial requests from its compliance officer.

New York State’s Financial Services Department (NYDFS) separately announced on 20 April that IBK agreed to pay $35 million as part of a consent order to resolve violations of the Bank Secrecy Act (BSA) and failures to detect Zong’s alleged money laundering and sanctions evasion scheme.

The NYDFS determined that, from 2010 to 2019, IBK had “poor” internal controls, including a “deficient” transaction monitoring scheme that failed to identify and prevent the $1 billion fraud at its New York branch. The firm entered into a 2016 written agreement with the NYDFS and Federal Reserve Board to remediate longstanding compliance deficiencies.

According to the statement of facts, IBK has made “significant” efforts to improve its BSA/AML programme since learning of the agencies’ investigations and entering into the written agreement. Remedial measures undertaken include improving AML and sanctions compliance oversight, hiring new compliance officers and reworking its transaction monitoring processes and systems.

In December 2016, Alaskan prosecutors indicted Zong, a US citizen, for sanctions evasion and money laundering. The NYAG stated on 20 April that South Korean authorities have convicted Zong of “certain crimes” and that he is not allowed to leave the country.

NYDFS press release
NYDFS consent order
NY Attorney General press release
Former FSM official allegedly aided fake vessel registration and money laundering scheme

The Federated States of Micronesia (FSM) announced on 27 April criminal charges against four individuals who allegedly conspired since 2015 to falsely register foreign ships as FSM vessels through the bogus Micronesia International Ship Registry (MISR) and then laundered the proceeds.

More than 100 foreign-flagged ship, including fishing vessels and oil tankers, reportedly paid between $2,000 and $14,000 for an FSM registration through the MISR, the Guam Daily Post reported on 29 April. The FSM government only allows domestic vessels to fly the FSM flag.

The illicit “flags of convenience” scheme was uncovered by Kaselehlie Press, which reported in December 2016 that Lukner Weilbacher, Secretary of the FSM Transportation, Communications and Infrastructure Department, asked local lawyer Martin Jano to help “Captain Sharma” obtain a foreign investment permit to issue ship registries.

Prosecutors allege Suniel K Sharma, who resides abroad, sold bogus MISR ship registrations through Jash International Maritime Law & Business Management (a unit of Ascent Navals Thailand) and then laundered some of the profits. Lukner Weilbacher is accused of peddling political influence, while his nephew Renwick Weilbacher and lawyer Jano are charged with money laundering.

Bank of Lithuania revokes Bruc Bond UAB’s licence over systematic AML/CFT violations

The Bank of Lithuania announced on 22 April that it has revoked Bruc Bond UAB’s licence to operate as a payment institution due to non-compliance with the licence requirements, serious infringements of its anti-money laundering and terrorist financing (AML/CFT) obligations, and inadequate safeguarding of customer funds.

Following the revocation of its licence, Bruc Bond UAB can no longer provide payment services and must return the funds received to its customers.

The AML/CFT-related inspection identified

- “Serious and systematic breaches" of Lithuania’s Law on the Prevention of Money Laundering and Terrorist Financing with respect to the assessment of ML/TF risks, identification and verification of the customer and the customer’s representative, implementation of international financial sanctions, and staff awareness of AML/CTF requirements
- The tools used to monitor customers’ business relationships and transactions were "ineffective and insufficient" to ensure timely identification of suspicious transactions and/or activities
- The company failed to manage the risk of potentially being exposed to ML/TF risks
Former Alstom US manager sentenced to supervised release in Indonesia bribery case

Former Alstom Power US regional sales manager Larry E. Puckett was sentenced in the US District Court for the District of Connecticut on 13 April to two years of supervised release for his role in a conspiracy to violate the US Foreign Corrupt Practices Act (FCPA) relating to a bribery and money laundering scheme in Indonesia between 2002 and 2009.

The case against Puckett was filed on 10 June 2019, when the defendant pleaded guilty to the FCPA violations. According to US prosecutors, Puckett was only a “minimal participant” in the bribery offences related to securing a power services contract for the Indonesian Tarahan project and demonstrated “prompt recognition and affirmative acceptance of personal responsibility for the offence”. In addition to the sentence, Puckett was ordered to pay $5,000 fine and perform 100 hours of community service.

In November 2019, Puckett’s testimony helped convict Alstom SA senior executive Lawrence Hoskins on seven counts of violating the FCPA and related money laundering charges in the same case. In February, Hoskins was given 15 months in prison for money laundering, after the judge decided to drop the foreign bribery charges over insufficient evidence. Alstom SA pleaded guilty in December 2014 to violating the FCPA by bribing officials in Indonesia, Saudi Arabia, Egypt and the Bahamas and agreed to pay $772.2 million to settle with the US Department of Justice.

US SEC charges former UK investment banker with bribing Ghana officials

On 13 April, the US Securities and Exchange Commission (SEC) charged former investment banker at the UK subsidiary of a US bank, Asante Berko, with orchestrating a scheme to funnel at least $2.5 million through a Turkish energy company to a Ghana-based intermediary to bribe Ghanaian officials for a state energy contract.

Berko, who is charged with violating anti-bribery provisions of the Foreign Corrupt Practices Act (FCPA) and federal securities laws, allegedly hid the bribery scheme that took place between 2015 and 2016 from his employer, which was identified as Goldman Sachs by the Financial Times on 13 April.

According to the SEC’s 37-page complaint, Berko endeavored “at all times” to keep the bribery scheme hidden from legal and compliance staff at the UK subsidiary and US holding company by “circumventing” their internal controls, including anti-bribery and other anti-corruption policies. The SEC stated that Berko “never disclosed” to compliance officers the actual role of the intermediary company, the energy company or his own role in arranging the alleged bribery scheme.

The agency also claimed that Berko attempted to mislead his firm’s compliance team about the intermediary company’s role when they conducted additional due diligence to assess the potential reputational risks of the power plant project and address other concerns. Further investigation led to the firm terminating its involvement in the project.
US SEC announces $24.5m settlement with Eni over alleged FCPA violations in Algeria

The US Securities and Exchange Commission (SEC) announced on 17 April a $24.5 million settlement with Eni SpA, which allegedly breached the internal accounting controls provisions of the Foreign Corrupt Practices Act (FCPA) by failing to detect fraudulent payments made by its subsidiary Saipem SpA to an intermediary to help funnel bribes to Algerian officials for state oil contracts.

According to SEC filings, Saipem conducted “little or no due diligence” before entering into four “sham” contracts with the intermediary between 2007 and 2010, received no legitimate services from the intermediary and “falsely” characterised its payments to the intermediary as lawful brokerage fees in its books and records, which were consolidated into Eni’s records during the relevant period.

International investigation identifies €15m face mask scam involving cloned Dutch website

Interpol announced on 14 April that a joint investigation by German, Irish, Dutch and UK Financial Intelligence Units (FIUs), with support from Europol and Interpol, has exposed a €15 million scam carried out by criminals looking to exploit the increasing demand for face masks during the Covid-19 pandemic. Three suspects in Ireland and the Netherlands are being investigated for alleged fraud and money laundering.

The investigation was launched after a German company placed an order for 10 million face masks on a Dutch website and made a down payment of €1.5 million into an Irish company’s bank account, which was described as a “trusted” dealer able to put the purchaser in contact with the Dutch supplier. The German buyer paid an additional €880,000 “to secure the merchandise”, of which €498,000 was transferred to a UK bank account, which was destined for an account in Nigeria.

During the joint operation it was revealed that the German company had entered into a deal with a fraudulent Spanish entity that had cloned the website and email address of a legitimate Dutch company and opened a bank account with a similar name at the same Dutch bank as the real company. On 27 March, the German contractor realised that the shipment had never taken place and got confirmation from the real Dutch company that the order had not been received. All funds were identified by the Irish, Dutch and British authorities and returned to the Netherlands.
Former FBI agent charged with conspiracy linked to Armenian organised crime network

Recently retired FBI agent Babak Broumand was arrested and charged with conspiracy to accept bribes, according to a 24 April statement by the United States Attorney for the Central District of California. Broumand allegedly conspired to receive over $200,000 in bribes from a lawyer who worked for convicted Armenian organised crime boss Levon Termenzhyan. In exchange for monthly bribes and other gifts, Broumand is accused of obstructing federal investigations and providing information to that same lawyer, who is now a cooperating witness.

According to US prosecutors, the unnamed lawyer referred to as CW1 is alleged to have given $30,000 to a company owned by Broumand and his wife, which was then used as down payment for a Lake Tahoe holiday home estimated to be worth $1.3 million. Broumand allegedly received further payments in monthly cash and bank deposit increments of $10,000, along with gifts that included hotel stays, transportation, and escort services.

Termenzhyan, also known as Lev Aslan Dermen, who is believed to be a member of an Armenian organised crime group that allegedly benefitted from Broumand’s protection, was convicted on 16 March of conspiracy and money laundering involving a $1 billion biodiesel tax fraud scheme. Termenzhyan faces a maximum of 30 years in prison, while Broumand faces up to five years if convicted.

UK Gambling Commission suspends Triplebet’s licence over ‘serious’ AML failings

The UK Gambling Commission announced on 7 April that it suspended on 17 February the licence of Triplebet, which operates the ‘Matchbook’ betting exchange and remote casino, due to “serious” anti-money laundering failings over a three-year period.

Triplebet was also fined £740,000 and ordered to implement remedial measures, which include submitting an independent auditors’ report on its AML compliance at six-monthly intervals.

The regulatory panel found that Triplebet failed to:
- Update its AML policy between November 2014 and October 2017
- Conduct due diligence on members of gambling syndicates
- Require enhanced due diligence for high-risk customers
- Investigate high-value gamblers’ source of funds or wealth
- Adequately monitor the top ten customers of its betting exchange
- Monitor or detect suspicious transactions
UK Gambling Commission fines operator over “extremely serious” AML and customer failings

The UK's Gambling Commission announced on 2 April that it has fined casino operator Caesars Entertainment UK Limited (CEUK) a record £13 million for "extremely serious" social responsibility, money laundering (ML) and customer interaction failings, particularly in relation to VIP client management practices between January 2016 and December 2018.

CEUK is the parent company of London Clubs Management Limited (LCM) which owns and operates 11 land-based casinos across Britain. The Commission’s regulatory review found "systemic failings" within CEUK’s governance systems and its oversight of licenced entities and key failings in its AML/CFT processes, in violation of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and the Commission’s AML guidance for remote and non-remote casinos.

As a result of the investigation, which continues in relation to the 11 individual casinos, three senior managers have had their personal licences revoked. To address the shortcomings, CEUK has implemented an improved system of governance, revised its regulatory procedures, hired new senior and compliance staff, completed a review of its high-value customers and commissioned an external risk and governance review. A list of additional regulatory conditions have been agreed to, such as undertaking outsourced role-specific AML training and carrying out an annual review of the effectiveness of the CEUK’s AML and social responsibility policies.

The AML failures identified

- The operator failed to carry out adequate source of funds checks and enhanced customer due diligence for high-value customers, politically exposed persons (PEPs) and consumers losing large sums of money
- Poor decision-making and delays in reviewing the risks posed by customers and a low understanding of the responsibilities of the compliance team and front-line staff operations
- The AML compliance team was not adequately resourced
- A lack of adequate documentation and audit trails

UK police freeze €2m in 25 bank accounts linked to Italian criminal syndicate

The UK's Metropolitan Police announced on 23 April the freezing of nearly €2 million in 25 bank accounts as part of an investigation into an Italy-based organised crime network that allegedly funnelled a large amount of suspicious EU funds through dozens of UK front companies.

False identities were used to obtain business banking facilities at a major bank and millions of euros were laundered through UK bank accounts before being transferred back to Italian accounts. Westminster Magistrates Court granted the account freezing order (AFO) under the Proceeds of Crime Act 2002 after London police and Italian authorities identified a series of transactions across multiple accounts that attempted to disguise and obscure the source of funds.
**EU dismantles investment-fraud network**

Eurojust and Europol announced on 7 April that European authorities have dismantled an international criminal network that defrauded investors of approximately €80 million and laundered the proceeds.

Advertising banners and mass emails promising above-average profits lured thousands of individuals into registering with unlicensed online trading platforms and investing in binary options and contracts for difference (CFDs). Investors’ funds were then distributed to a large number of participants in a complex money laundering network that had a chain of companies across Europe.

The joint action by law enforcement and judicial authorities from Austria, Bulgaria, Germany and Serbia resulted in the arrest of nine individuals, including two alleged leaders of the criminal network.

Serbian authorities placed 30 bank accounts under surveillance and seized five apartments, three cars, a "considerable amount" of cash and some IT equipment. In Germany, €2.5 million was frozen in the bank account of a company allegedly involved in the fraudulent scheme.

**Inter-American Development Bank bans Brazilian construction company for kickbacks**

The Inter-American Development Bank (IDB) announced on 24 April the debarment of Brazilian company Andrade Gutierrez Engenharia S.A. and eleven of its subsidiaries for paying public officials nearly $50 million in kickbacks in connection with four IDB-financed projects in Brazil. The debarment has been reduced from 3 years and 1 month to 2 years and 6 months due to the company receiving credit for voluntary restraint.

Following an investigation by the Office of Institutional Integrity (OII), AG Engenharia admitted that it schemed to bribe government officials in exchange for contracts between 2009-2012. Based on the value of the contracts, the kickbacks paid by the company potentially totalled $1.9 million. AG Engenharia fully cooperated with the investigation, which "is reflected in a significantly reduced sanction," states the IDB press release.

As part of the settlement agreement, AG Engenharia has committed to report on its compliance programme through an independent monitor. If AG Engenharia fails to fulfil its obligations, debarment will continue until the conditions are met, up to a maximum of 9 years.

In 2018, the company reached a separate settlement agreement with the Brazilian authorities over corruption allegations as part of "Operation Car Wash," in which the company agreed to pay $381 million in fines.
Eurojust targets criminals abusing the pandemic

Eurojust issued a statement on 8 April on its efforts to support several investigations into online fraud and hacking by criminal organisations looking to abuse the Covid-19 crisis. The investigations related to requests for assistance from Germany, France and the Czech Republic.

According to the statement by Eurojust, 202 new cases were opened from 13 to 30 March 2020, with eight coordination meetings organised by Eurojust to assist judicial authorities.

Details of the cases

- The German investigation, which led to the arrest of two suspects in the Netherlands and the freezing of €2 million in assets, involved a fraudulent offer of ten million face masks. Suppliers from Asia allegedly tricked a German sales company into paying an advance of €2.4 million to foreign accounts in exchange for the masks, which were never delivered.

- A French company in Dijon was similarly tricked into transferring €132,500 to a Hungarian account in exchange for masks and hand sanitizer, which was never delivered. Cooperation between the French and Hungarian authorities led to the freezing of the Hungarian account.

- In the Czech Republic, a Brno hospital was shut down after hackers encrypted the hospital’s computer system, freezing access to patient records. Follow-up investigations are being conducted in France and Switzerland.

La Tresorerie fined for unlicensed cash service

The Dubai Financial Services Authority (DFSA) announced on 23 April a $612,790 settlement with La Tresorerie Ltd for operating an illegal cash service that had a high risk of money laundering between 2015 and 2017.

The DFSA’s 37-page decision notice states that La Tresorerie misled another DFSA authorised firm and a UAE bank about the nature and purpose of certain cash transactions when the entities conducted anti-money laundering (AML) due diligence checks.

The unlicensed cash service allegedly

- Operated with the knowledge and involvement of the firm’s senior management at the time and was reported by the new management in January 2017.

- Provided more than $7.3 million in cash and received $220,000 in fees from approximately 100 transactions ranging in value from €2,560 to €500,000.

- Enabled the transportation of large amounts of cash from the UAE to Switzerland.

- Used false invoices and transferred client funds to unregulated companies outside the Dubai International Financial Centre (DIFC) without clients’ knowledge or consent.
US designates Russian Imperial Movement and alleged leaders as global terrorists

The US State Department announced on 6 April the listing of Russian Imperial Movement (RIM) and three of its alleged leaders as specially designated global terrorists (SDGTs), citing RIM’s purported provision of paramilitary-style training in St Petersburg to neo-Nazis and white supremacists convicted for terrorist attacks in Sweden.

The designations under Executive Order 13224 block RIM from accessing the US financial system and impose asset freezes and visa bans on Russian nationals Stanislav Anatolyevich Vorobyev, Denis Valliullovich Gariev and Nikolay Nikolayevich Trushchalov.

Aperio Analysis

This is the first time a white supremacist group has been named as a SDGT. The move is surprising as RIM is a relatively small organisation, mostly operating in Russia. One of the sanctioned individuals, Nikolay Trushchalov, reportedly left the organisation in 2019. Donald Trump's administration has previously been criticised for not taking the threats posed by white supremacist movements seriously and this may have been intended to counter that impression. Most groups recognised by the US as terrorist organisations are linked to Islamic extremism and/or are known to have used violence to achieve political goals. It is unclear whether the sanctions will have an impact on the situation in Ukraine, where RIM is known to have sent around 100 volunteers to fight on the side of the pro-Russian separatists. The Russian government has never acknowledged any support for or links to RIM, but the organisation has been able to operate in the country, and in Ukraine, without any major difficulties. The sanctions against RIM may lead to a more organised fight against white supremacist movements globally.

Hong Kong regulator fines Bocom International Securities for AML failings

Hong Kong’s Securities and Futures Commission (SFC) announced on 20 April that Bocom International Securities Limited (BISL), the local arm of China’s Bank of Communications’ securities unit, has been fined $19.6 million for a range of “inadequate and ineffective” internal controls, including AML failures concerning the handling of third party deposits into client accounts.

According to the SFC’s statement, third party deposits made through cheques in 2009 and 2011 and bank transfers in 2015 were not identified until March 2016 and BISL failed to implement effective controls to identify depositor’s information apart from the details provided by account holders. SFC identified additional shortcomings in the authorisation and recording of transactions conducted in client accounts and the confirmation of client identities and transaction details.

In addition, the SFC’s review of BISL’s margin lending and margin call policy between December 2012 and November 2016 found “serious and extensive” deficiencies in particular in relation to the management of margin calls and the keeping of records concerning explanations for deviations from margin lending policy.

In deciding on the disciplinary sanction, SFC considered both BISL’s clean disciplinary record and its agreement to hire an independent expert to conduct a review of its internal controls.
Latvian authorities investigate alleged €7 million plastics laundering scheme

The Latvian Tax and Customs Police have started criminal proceedings against individuals accused of laundering €7 million in illicit funds through a fictitious transaction scheme involving the sale and purchase of overpriced biopolymer pellets, according to a 9 April announcement by the State Revenue Service (VID). The alleged scheme involved "a fictitious chain of companies" which were registered in Latvia, Belarus, Russia and Austria.

Six police searches in the Riga area led to the seizure of approximately €5 million worth of plastic granules, alleged to have been marketed at inflated prices in order to cover up illegally sourced currency. It is alleged that from 1 August 2019 to April 2020, up to €7 million was laundered through these companies.

The investigation is ongoing, and no individuals or companies have yet been named by the VID.

Former Ecuadorian president Correa sentenced to eight years in prison over bribery charges

Ecuador's National Court of Justice found former president Rafael Correa guilty of corruption charges and sentenced him to eight years in prison on 7 April. Correa was accused of being the head of a "criminal structure" comprised of 19 other officials and accepting $7.5 million in bribes in exchange for public contracts to finance his party's election campaign between 2012 and 2016.

According to the Court, 18 defendants were sentenced to eight years in prison, including Correa, while two individuals received more lenient sentences for cooperating with prosecutors.

Correa, who is in exile in Belgium, stated in a tweet that the verdict is "absolutely grotesque" and accused his political opponents of "manipulating justice to achieve what they could never achieve at the ballot box". Correa's defence has reportedly stated that it will appeal the Court’s ruling, which also bans Correa from being involved in politics for 25 years.
Uganda arrests four officials over aid fraud

The Uganda State House Anti-Corruption Unit headed by President Museveni’s Military Assistant Lt. Col. Edith Nakalema arrested on 9 April four government officials, including the Permanent Secretary in the Office of the Prime Minister (OPM) Christine Guwatudde Kintu, following accusations of fraud in the procurement of food aid for vulnerable people during the Covid-19 lockdown.

According to a press statement from the Uganda State House Anti-Corruption Unit, an investigation into the procurement of relief items revealed that officials were “inflating prices and rejecting lower price offers from various suppliers of maize flour and beans”. Those arrested include accountant Joel Wanjala, Assistant Commissioner of Procurement Fred Lutimba, and Disaster Management Commissioner Martin Owor.

UN designates FDPC leader over human rights abuses in Central African Republic

The United Nations Security Council (UNSC) listed Martin Koumtamadji on 20 April and imposed an asset freeze and visa ban against the commander-in-chief of the Front Démocratique du Peuple Centrafricain (FDPC), an armed group allegedly engaged in violent activities in the Central African Republic (CAR).

According to the UNSC, the FDPC has committed numerous human rights violations under the leadership of Koumtamadji, who allegedly cooperated with sanctioned individual Nourredine Adam and engaged in arms trafficking with a close associate of Adam to increase the FDPC’s military capabilities.

UK FCA issues final notice against former equities dealer convicted of insider trading

The UK’s Financial Conduct Authority (FCA) issued a final notice on 27 April prohibiting former equities dealer Paul Milsom from performing any function in relation to any regulated activity carried on by any authorised person, exempt person or exempt professional firm, after he pleaded guilty to 28 counts of insider dealing and was sentenced to two years in prison in March 2013.

According to the FCA summary of reasons, Milsom’s role in the scheme involved using insider information whilst in his position as equities dealer at the central dealing desk at Legal & General Investment Management Ltd between October 2008 and March 2010 to gain £245,657.58 in illicit profit from the trades.
US charges former Fox executives in FIFA probe

The long-running investigation into corruption surrounding world football’s governing body, FIFA, saw more charges brought forward on 6 April when the US authorities unsealed indictments against two former senior executives at 21st Century Fox – Hernan Lopez, the former chief executive of Fox International Channels and Carlos Martinez, the former president of Fox Latin America.

The indictment alleges that the duo "relied on loyalty secured through the payment of bribes" to South American football officials in order to "advance the business interest of Fox" and gain "confidential bidding information" to win US TV rights to the 2018 and 2022 World Cup competitions. The charges include fraud, bribery, money laundering and racketeering.

This latest indictment also sets out charges against Gerard Romy the former chief executive officer of Spanish media company Imagina Media Audiovisual SL, and Uruguayan media company Full Play Group SA. It is also alleged that four unnamed co-conspirators occupied various levels of seniority at FIFA and South American football administrations.

"Over a period of many years, the defendants and their co-conspirators corrupted the governance and business of international soccer with bribes and kickbacks, and engaged in criminal fraudulent schemes that caused significant harm to the sport of soccer," said William F. Sweeney Jr, Assistant Director in charge of the FBI’s New York field office.

The indictment details various schemes involving the payment of bribes to South American football federation (CONMEBOL) and Confederation of North, Central American and Caribbean Association Football (CONCACAF) officials to secure broadcast rights to football competitions.

Over 40 people and entities have been charged as part of the US government’s ongoing investigation of bribery in world football, which started in 2015. Lopez and Martinez are scheduled for arraignment in federal court on 9 April and could face up to 20 years in prison.

Reuters reported on 9 April that Lopez, Martinez, and Full Play Group SA have entered not guilty pleas to the criminal charges brought by the US government.

Central Bank of Kenya suspends Absa Bank from Forex trading over KYC failings

The Central Bank of Kenya (CBK) announced on 9 April that it has taken regulatory action against Absa Bank Kenya PLC, suspending the firm from Forex trading, due to Absa Kenya’s failure to provide information about certain foreign exchange trades conducted in March 2020.

Following an investigation into certain Forex trades made by Absa Kenya, the CBK found that Absa Kenya neither had "satisfactory assurance" as to the underlying commercial transactions supporting these trades (as per regulatory requirements), nor did Absa Kenya ensure that these transactions complied with anti-money laundering and combating the financing of terrorism (AML/CFT) regulations as well as know-your-customer (KYC) requirements.

In response, the CBK suspended Absa Kenya from Forex trading for six days (from 9-15 April) and directed the firm to implement a "robust framework" to ensure that all relevant documents for Forex transactions are available, in addition to adhering to all AML/CFT and KYC requirements, by 15 April.
Swiss federal tribunal ruling requires Ukrainian lawmaker’s assets to remain frozen

Switzerland’s Federal Tribunal upheld on 8 April a ruling by the Federal Administrative Court to freeze the assets of Ukrainian parliamentarian Yuri Ivanyushchenko, following a decision by the Swiss government to block the assets of former Ukrainian president Viktor Yanukovych and 30 other people in his entourage – approximately CHF 70 million (£58 million) – over money laundering charges.

The Tribunal stated that Ivanyushchenko’s assets must remain blocked because of pending criminal proceedings against him in Switzerland and Ukraine. Ivanyushchenko is accused of illegal enrichment by orchestrating corrupt schemes at the customs agency and embezzling funds received by Ukraine from the sale of Japanese greenhouse gas emissions quotas under the Kyoto Protocol.

In 2017, Ivanyushchenko requested that his name be removed from the list of sanctioned Ukrainians whose assets had been frozen by the Swiss authorities, following the EU’s decision to release his funds. The Swiss courts rejected Ivanyushchenko’s request.

New Zealand warns broker over AML breaches

Tiger Brokers was required to submit a plan to the regulator before 17 April 2020 on how it will rectify the issues identified. It must then complete these actions by 30 September 2020 or face enforcement action.

According to the regulator, Tiger Brokers failed to:
- Adequately conduct enhanced and ongoing CDD
- Adequately verify customer identification documents
- Obtain adequate source of funds or wealth information relating to high-risk customers, and take reasonable steps to verify that information
- Report suspicious activity to the authorities within three working days
- Take reasonable steps to determine whether a customer or any beneficial owner was a PEP

The FMA also issued formal warnings to another six business over their AML practices but has decided not to name these entities. Four entities failed to have their AML risk assessment and programme audited in a timely manner; one failed to provide an audit of its AML risk assessment and programme; and the other failed to have an AML programme in place, undertake a risk assessment, and designate an employee to maintain the programme.
Bank Hapoalim to pay $905m to resolve money laundering, bribery and tax evasion charges

The US Justice Department (DOJ) announced on 30 April that Bank Hapoalim BM and GHBM Bank Hapoalim (Switzerland) Ltd agreed to pay nearly $875 million to the US Treasury Department, Federal Reserve and New York State Department of Financial Services (NYDFS) after the Israeli lender’s Swiss subsidiary admitted to helping US taxpayers hide more than $7.6 billion in 5,500 secret Swiss and Israeli bank accounts from 2002 to 2014.

The firms also agreed under a non-prosecution agreement (NPA) to forfeit $20.7 million and pay a criminal penalty of $9.3 million after admitting that some of their employees conspired to launder through US financial institutions more than $20 million in bribes and kickbacks to officials from Fédération Internationale de Football Association (FIFA) and other football federations between December 2010 and February 2015.

OFAC finds AmEx subsidiary processed payments for US-designated Gerhard Wisser

The US Treasury Department’s Office of Foreign Assets Control (OFAC) announced on 30 April that American Express Travel Related Services Company, a subsidiary of American Express Company, provided a prepaid card to US-listed Gerhard Wisser and processed 41 transactions worth $35,247 for him in 2015, in violation of the Weapons of Mass Destruction Proliferators Sanctions Regulations.

OFAC stated in its finding of violation that the firm disclosed and took remedial action to address the sanctions breaches, which were caused by human error and screening system defects. No monetary penalty was issued.
Honduras ex-police chief charged with drug trafficking offences in US, president implicated

The US Justice Department announced on 30 April that the former chief of the Honduran National Police Juan Carlos Bonilla Valladares, known as El Tigre, has been charged in a federal court with using his position to facilitate the import of 40 tonnes of cocaine into the US as part of a drug trafficking conspiracy between 2003 and 2020, which involved Honduran President Juan Orlando Hernández Alvarado's brother as the main co-conspirator, and the president himself.

The president's brother Juan Antonio Hernández Alvarado was convicted of drug trafficking in the US in October 2019 and is expected to be sentenced in June. According to the complaint, at the request of Hernández Alvarado and other corrupt politicians, Bonilla Valladares ensured the safe passage of Venezuelan and Colombian drugs through Honduras towards the border with Guatemala and eventually into the US, in exchange for bribes paid in drug proceeds. In addition, he provided his co-conspirators with sensitive law enforcement information to facilitate cocaine shipments and ordered the murder of a rival Honduran drug trafficker in 2011.

US prosecutors allege that President Hernández Alvarado and his brother helped Bonilla Valladares move higher up the ranks of the National Police to protect their drug trafficking activities.

In a press release issued on 30 April, the Honduran government announced that it would extradite drug traffickers and dismantle criminal structures. According to the statement, the president will continue to fight international organised crime regardless of the false charges, which were allegedly based on a former drug trafficker's confession seeking to negotiate a reduced sentence in the US.

---

German government bans Hezbollah as terrorist organisation, confiscates assets

Germany’s Federal Interior Ministry banned Hezbollah as a terrorist organisation on 30 April and announced asset seizures and a prohibition on promoting the Lebanese Shiite group’s activities.

Investigators raided four German associations suspected of belonging to Hezbollah, along with the private residences of their purported leaders, over their alleged financial and marketing support to the organisation.

On 30 April, the US State Department commended Germany’s actions against Hezbollah, which it claimed is “a terrorist organization dedicated to advancing Iran’s malicious agenda”, and called for other EU member states to “follow suit” and hold Hezbollah accountable for its activities.
The financial crime implications of the Covid-19 pandemic: an overview

The Covid-19 pandemic has presented a clear opportunity for criminals to profit from the upheavals and anxiety felt by populations and governments around the world. Feeding on the sense of urgency and crisis affecting so many people, opportunistic individuals as well as organised crime groups (OCGs) have moved swiftly to exploit the situation. This article examines the response by regulators, law enforcement agencies and multilateral organisations to the development of financial crime risks resulting from the Covid-19 pandemic.

Responses can be grouped under several headings:

- Guidance on emerging financial crime risks and measures that individuals or organisations can take to address these risks
- Reminders of regulatory expectations of firms in the regulated sector concerning their response to the Covid-19 crisis
- Measures that certain regulators and law enforcement agencies are taking in response to Covid-19 related risks
- The impact the Covid-19 pandemic is having on regulatory timetables and deadlines

Emerging financial crime risks from the Covid-19 pandemic

Many national and multilateral organisations have issued papers, guidance or warnings addressing the financial crime risks and associated security risks of Covid-19, including Europol, Interpol, the OECD, the Council of Europe’s Group of States Against Corruption GRECO, Eurojust, the Financial Action Task Force FATF, the UK National Crime Agency NCA, the US Federal Bureau of Investigation FBI, the UK National Cyber Security Centre NCSC, the US Treasury Financial Crimes Enforcement Network FinCEN, and the US Internal Revenue Service IRS.

This guidance draws attention to financial crime risk emanating from several areas:

- **Increased cybercrime activity.** According to Europol, the lockdown instituted in response to the Covid-19 pandemic has widened the “attack surface” and the “attack vector” for cybercriminals. The types of activity, such as email or text message phishing scams, malware and distributed denial of service (DDoS) attacks, as well as the actors involved, have not changed significantly since before the crisis. What has changed, according to Europol, is the speed at which some of these actions are being perpetrated as well as the sophistication of some...
of the schemes. For example, Eurojust reported that timeframes for ransomware attacks have accelerated between point of infection and demand for payment in an effort by criminals to take advantage of the crisis and maximise profits in the shortest available period. The UK’s NCA emphasised that Covid-19 was being used as “a hook to commit fraud” with criminals using phishing emails to entice recipients to access fake websites spreading malware or purporting to provide essential goods such as personal protective equipment (PPE).

- **Exploitation of cloud-based systems.** Lockdowns resulting from the Covid-19 pandemic have resulted in many organisations being forced to adapt to remote working. Security weaknesses around cloud-based systems, including video conferencing and Voice over Internet Protocol (VoIP) communications have been exploited, with the FBI warning that hackers are disrupting online conferences in an activity dubbed “Zoom-bombing”. Hackers may seek to compromise remote desktop applications or listen into confidential communications. The FBI also warned on the risks of relying on leased IT equipment from foreign suppliers which may not have been sufficiently sanitised and may contain pre-installed malware.

- **Amplification of existing fraud threats.** Criminals have exploited the pandemic to recycle existing scams, such as advance fee fraud. In one case cited by Eurojust, suppliers from Asia allegedly tricked a German company into paying an advance of €2.4 million to foreign accounts for face masks that were never delivered; in a second case, a French company was persuaded to make payments to an account in Hungary for protective equipment and hand sanitiser that was also not delivered. Fraudsters have engaged in setting up multiple front companies and fake websites (including cloned sites of legitimate organisations), often in conjunction with falsified documents, whilst relying on their victims’ sense of urgency and lack of adequate due diligence to successfully perpetrate fraud.

- **Increased prevalence of counterfeit goods.** High demand for goods such as PPE and anti-viral pharmaceuticals has encouraged a sharp increase in the circulation of counterfeit goods, according to Interpol. The agency said that protective face masks were the most commonly counterfeited item, but that various forms of coronavirus “sprays”, “medicines” or “packages” were also prevalent amongst items seized by police and customs authorities. Based on a limited set of evidence, a Europol report found the profits from the supply of counterfeit goods supplied in connection with Covid-19 often flow back to countries of production including China and India. It said that in the EU, illicit gains are laundered via cash intensive businesses. Front companies supplying counterfeit goods are known to have been registered at addresses in Bulgaria, Germany, the Netherlands, Poland, China, India and the United States. Speaking at the end of March 2020, Ursula von der Leyen, President of the European Commission, said “our fear has become their business opportunity”. She said an operation by Europol had resulted in the dismantling of 37 organised crime groups, the takedown of 2,500 false links or adverts and the seizure of 4.4 million units of fake products.

- **Fake investment and giving schemes.** FATF warned of an increased risk of fraudulent investment offers and fake charity fundraising activities associated with the pandemic crisis. It encourages the use of FinTech, RegTech and SupTech solutions “to the fullest extent possible” to mitigate the financial crime risks arising from the Covid-19 pandemic. The UK NCA’s analysis of recent Suspicious Activity Reports (SARs) found evidence of victims cheated into believing they are investing in companies developing a coronavirus vaccine. The FBI warned about possible investment scams promising returns “too good to be true” as well as forms of blackmail demanding payment in cryptocurrency.

- **Subversion of government schemes.** The UK’s HM Revenue & Customs (HMRC) warned that UK government schemes designed to support companies and individuals were likely to be the target of criminals seeking to profit from them. This includes claims for fake employees as well as inflated claims. However, HMRC emphasised four specific safeguards to prevent abuse, including a whistleblowing hotline. In the United States, the IRS warned against the risk of identity theft from criminals posing as the IRS, requesting financial information in exchange for tax refunds or stimulus payments. Both the OECD and GRECO have warned about the risks of public sector fraud and corruption, including conflicts of interest, arising from emergency procurement processes and economic stimulus packages created in response to the Covid-19 pandemic.

- **Infiltration of the mainstream economy by mafia-type OCGs.** Organised Crime Groups, including mafia-type organisations, have been quick to adapt to the new situation. According to Europol, these groups have sought to exploit individual vulnerabilities, recruiting and coercing younger people into areas such as loan sharking, extortion and racketeering. Europol has warned that OCGs are also seeking opportunities to invest in legitimate businesses, particularly in the construction,
money service bureau, and import/export industries. As demand for healthcare products has increased, there is a further risk that OCGs will seek to infiltrate healthcare institutions and secure access to in-demand products.

- **Reduced checks on cash deposits.** Europol has noted the risk that OCGs will use the Covid-19 pandemic as cover to move cash outside the EU to economies that are desperate to receive funding and where it is less likely that checks will be made on the source of funds. In the longer-term, the pandemic may however reduce the level of cash transactions making it relatively harder for criminals to launder physical cash through the legitimate economy. Europol expects this may drive criminals to explore other avenues for money laundering as a result.

- **Increased threat of trade-based money laundering.** An increase in the volume of cash transactions, wider use of falsified documentation and the rapid emergence of (sometimes fake) companies seeking to benefit from the pandemic crisis gives rise to elevated risks of trade-based money laundering schemes.

- **Money laundering via refunds for cancelled purchases.** Criminals attempting to launder money may claim that unexplained deposits (sometimes via previously inactive bank accounts) are the result of refunds from cancelled purchases, such as a planned holiday, a house or a car, according to an analysis of trends by the UK’s NCA. They may also seek to rapidly withdraw sums of money, claiming they have lost faith in the banking system as a result of the Covid-19 crisis.

- **Money mule schemes.** The FBI has warned that individuals seeking work may be tempted to participate in work-from-home schemes that promise easy money for little effort. Instead, the FBI said certain schemes tempted individuals into acting as money mules, for example by enticing them to make or receive funds from their personal bank account, open bank accounts under their name for a business, or they may receive instructions to retain a portion of the money they transfer.

- **Involvement of state-backed actors.** State-backed actors may be involved in spreading disinformation to advance their own geopolitical aims or engage in cybercrime/cyber espionage activities related to the attempted extraction of intellectual property. This includes laboratories or medical facilities working on vaccines or treatments for Covid-19.

- **Increase in drug transactions via the Darknet.** Interpol warned that the pandemic has led to an increase in the use of drug commerce via social media, encrypted applications and the Darknet.

- **Sham bankruptcies, sham litigation or false loans.** The UK NCA has identified concerns over facilitating “emergency” loans to subjects about whom they hold money laundering concerns. Sham bankruptcies and litigation have also featured in previous international money laundering cases and the Covid-19 crisis may provide cover for such actions in the future as businesses experience distress or failure.

### Reminders of regulatory expectations

In light of the Covid-19 crisis, a number of regulators have emphasised measures that regulated firms should be taking to address financial crime risks:

- The UK Financial Conduct Authority (FCA) and the UK Prudential Regulation Authority (PRA) published guidance that dual-regulated firms should ensure that individuals performing senior management functions (SMFs), such as compliance oversight and money laundering reporting officers, should be furloughed as “a matter of last resort”. The authorities added that if an individual performing a mandatory or required SMF becomes absent, the firm must appoint alternative individuals to continue performing these SMFs to ensure the firm continues to meet its regulatory and legal obligations.

- The European Banking Authority (EBA) said in a statement that it expects financial institutions to ensure digital operational resilience, adequate ICT capacity, governance and security of their online services to better prevent cybercrime. It also stressed the need for financial institutions to ensure their business continuity plans are updated and adapted, including considerations for potentially longer-term measures related to Covid-19.

- The European Insurance and Occupational Pensions Authority (EIOPA) has outlined its expectations as to how national competent authorities and the EU’s institutions for occupational retirement provision (IORPs) should manage the exposure to fraud and other financial crime risks arising from the Covid-19 pandemic, including cybersecurity and data protection issues related to remote working.

- The US Department of Treasury’s FinCEN set out further guidance on measures financial institutions should take to meet their legal obligations under the Bank Secrecy Act (BSA) during the Covid-19 pandemic. Included in this were certain relaxations of the new currency transaction
report (CTR) filing obligations for sole proprietorships and legal entities and a suspension of requirements for re-verification of existing customers in relation to the Paycheck Protection Programme (PPP). However, FinCEN advised financial institutions to remain alert to malicious or fraudulent transactions in line with its 2017 advisory regarding disaster-related fraud and a 16 March advisory, alerting financial institutions to investment scams and insider trading.

- The US Department of Treasury’s Office of Foreign Assets Control (OFAC) encouraged financial institutions to get in touch at the earliest possible opportunity if they anticipated delays in meeting regulatory deadlines for responding to administrative subpoenas, submitting licence reports or filing blocking or rejection reports. OFAC indicated it would consider reallocation of sanctions compliance resources during the pandemic if it was consistent with its risk-based approach, in determining any administrative penalties.

- The Hong Kong Monetary Authority (HKMA) encouraged the use of FinTech solutions to manage remote client on-boarding. It also said it would allow simplified due diligence measures where authorised firms open accounts solely for the purpose of the government’s HK$10,000 cash payout scheme. It encouraged public/private sharing of information and typologies to help prioritise and address Covid-19 related fraud risks.

- The French financial markets regulator, Autorité des marchés financiers (AMF), encouraged market participants to “exercise judgement” when filing suspicious transaction and order reports (STORs) to avoid those that are purely a result of volatile markets. AMF said that market operators are not prohibited from working from home but should be mindful of possible risks of conflicts of interest and lag times when trading.

### Measures taken by regulators and law enforcement in response to the pandemic

In addition to publishing warnings and advisories regarding the threats of financial crime associated with the Covid-19 pandemic, some government agencies have introduced additional specific measures:

- The UK NCA announced a SAR glossary for reporting coronavirus-related fraud. The UK’s Financial Intelligence Unit has since published guidance on trends relating to Covid-19.

- The UK NCSC launched a cross-governmental “Cyber Aware” campaign to promote behaviours to mitigate cyber security threats. As part of the campaign, it established the Suspicious Email Reporting Service (SERS) to help assess and take down malicious content and provide guidance on emerging scams seeking to take advantage of the pandemic.

### Impact of Covid-19 on regulatory timetables

In response to the Covid-19 pandemic, several delays to regulatory timetables have been announced or suggested:

- FATF said that it was issuing a temporary suspension to all assessments and follow-up deadlines. High-risk jurisdictions would be given a four-month extension on their current deadlines although some have volunteered to continue with their current schedules.

- The EBA issued guidance that national competent authorities may temporarily postpone “non-essential onsite inspections”, performing virtual meetings and inspections where appropriate.

- The UK Financial Conduct Authority (FCA) issued a six-month extension to its strong customer authentication (SCA) deadline, until 14 September 2021, citing the “exceptional circumstances” of the Covid-19 pandemic.

- The UK Department of Trade and Industry (DIT) has extended its consultation on plans to create up to 10 freeports across the UK as part of its post-Brexit planning until 13 July. The consultation was launched in February 2020.

- The European Banking Federation (EBF) and a group of nine other banking and insurance associations have asked the European Commissioner for Economy Paolo Gentiloni to extend the deadline for mandatory disclosure obligations under the revised cross-border tax directive (Directive on Administrative Cooperation, known as DAC6) until 1 July 2021, citing significant challenges including the Covid-19 pandemic.
On 3 April, the UK’s National Crime Agency (NCA) released its annual assessment of serious and organised crime (SOC) and warned that hundreds of billions of pounds may be laundered through the UK each year, with most of the illicit funds deriving from abroad.

SOC trends include:

- Specialist international controller networks are laundering money for criminals, predominantly dealing in cash but also using more complex methods such as trade-based money laundering (TBML) to disguise international money movements and meet clients’ needs
- Money services businesses (MSBs), informal value transfer systems and cross-border deliveries continue to be exploited for cash-based money laundering in the UK
- Counterfeiters may increasingly shift their attention towards supplying £50 banknotes following the introduction in February of the £20 polymer note, which is more difficult to counterfeit
- The most vulnerable sectors to bribery and corruption are construction, extractives, pharmaceuticals, aerospace and defence; the involvement of politically exposed persons (PEPs) in the illegal wildlife trade is an emerging threat
- The relatively high spend and complex supply chains within social care and construction make it likely that these sectors of local councils are particularly vulnerable to organised crime
- Large scale, multi-vendor markets remain the principal source of trading drugs, weapons, malware and false documentation on the dark web
- Criminals are increasingly using encryption tools, the dark web and virtual assets such as blockchain, bitcoin, crypto-assets and cryptocurrencies to conduct their activities

SOC statistics include:

- There were 99 reports of suspected financial sanctions breaches, reportedly worth a combined £262 million, in 2018/19
- More than 40,000 cases of suspected money mule account activity were reported in 2018, the latest available figures, up 26 percent on 2017
- A suspected 929 UK companies were involved in cases of corruption and money laundering in 2019, amounting to £137 billion in economic damage
- At least 350,000 individuals and 4,772 organised crime groups (OCGs) are believed to be involved in SOC in the UK
- A quarter of all OCGs are assessed to have the intent and capability to infiltrate, bribe or corrupt private and/or public sector employees
- 37 percent of all OCGs mapped in the UK are involved in drugs activity; the cocaine market across England, Scotland and Wales is estimated to be worth between £9.4 billion and £11.8 billion annually
- Victim reported losses from fraud increased by 38 percent to £2.2 billion in the year ending March 2019; losses from romance, courier and computer software service fraud totalled £90 million in the year ending February 2020
UK’s NCA to create public-private fraud forum, increase asset seizures in 2020/21

The UK’s National Crime Agency (NCA) announced in an annual report published on 3 April that more than £275 million in assets were frozen, £7 million in cash was forfeited and £110 million was restrained between 5 April 2019 and 9 March 2020.

The NCA’s strategic priorities for 2020/21 include:

- Forming a public-private fraud forum to increase disruptions, identify high-harm offenders and protect against high-impact fraud
- Identifying money laundering in the UK and the individuals responsible for it
- Increasing the amount of criminal funds targeted with asset freezes and confiscations
- Leading and coordinating the UK response to cybercrime threats, collaborating with international partners to pursue cybercriminals, and providing the investigative response for the “highest severity” cybercrime incidents and support where incidents are delegated to other authorities for investigation
- Prosecuting individuals and disrupting organised crime groups responsible for modern slavery, human trafficking and immigration offences
- Leading a cross-system operational response to increase the risk and difficulty of obtaining and distributing child sexual abuse material online
- Disrupting the county lines criminal business model for drug distribution and lowering the level of violence in the UK’s illicit drug market
- Reducing the availability of firearms to the criminal market by cracking down on cross-border arms trafficking and the diversion of legal weapons in the UK market

OECD finds Switzerland and Brunei ‘largely compliant’ with tax transparency requirements

The OECD’s Global Forum on Transparency and Exchange of Information for Tax Purposes published on 6 April peer-review reports on eight jurisdictions’ compliance with international requirements to obtain beneficial ownership information on legal entities and arrangements, in line with Financial Action Task Force ( FATF) Recommendations.

Brunei Darussalam, Macau (China), Switzerland, Peru and Tunisia were found to be “largely compliant” with the international standard on transparency and exchange of information on request (EOIR).

Barbados and the Seychelles were downgraded from “largely compliant” to “partially compliant” since their last reviews, while Liberia was rated “partially compliant” in its first full review.
UK FCA Business Plan for 2020/21 prioritises efforts to tackle Covid-19 related crime

According to the Business Plan, in 2020 the FCA will start implementing activities aimed at reducing the risk of financial crime, in particular money laundering and fraud. In line with commitments set out in the UK’s National Economic Crime Plan, the FCA will assess whether firms have adequate systems and controls to detect, prevent and disrupt financial crime and will continue to take enforcement action in cases of serious misconduct.

As part of its anti-money laundering (AML) strategy, the FCA will consult on extending the Financial Crime Data Return to additional firms to help strengthen its risk-based supervision and will ask the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) to test how professional body supervisors in the legal and accountancy sectors have implemented AML strategies.

The FCA will continue running its anti-fraud ScamSmart campaign and will prioritise reducing consumer harm caused by high-risk illiquid retail investments. The FCA estimates that serious and organised crime costs the UK at least £37 billion annually and urges firms to put in place better economic crime prevention systems.

Europol report on counterfeit pharmaceutical trade identifies intelligence gaps

A report by Europol published on 17 April warns that criminals trading in counterfeit goods, particularly counterfeit pharmaceutical and healthcare products, have been quick to exploit the Covid-19 pandemic. Europol states that the use of document fraud, the extent of criminal profits derived from the distribution of these goods and the money laundering schemes to convert the proceeds all present significant intelligence gaps.

“The profits obtained from the trade of these goods are likely substantial,” states the report. Based on the limited information available on the associated illegal money flows, there are indications that a significant proportion of the profits flow back to countries of production such as China or India, and in the EU the illicit gains are likely laundered via cash intensive business.

Analysis of the data provided to Europol reveals that the companies targeting the EU for distribution of counterfeit pharmaceutical products and equipment are registered to addresses in Bulgaria, Germany, the Netherlands, Poland, China, India, and United States. The Europol report states that companies trading in counterfeit goods are highly diverse and quick to establish additional front companies to obscure their activities.
North Korea using ‘clandestine’ financial networks to transact with Iran, finds UN experts

The United Nations Security Council’s (UNSC) panel of experts on North Korea announced in a 266-page annual report released on 17 April that Pyongyang continued to violate international sanctions by illicitly enhancing its nuclear and ballistic missile programmes, exporting commodities and importing petroleum and luxury goods in 2019.

The panel also determined that North Korea evaded sanctions and accessed international banking channels by

- Establishing clandestine financial networks throughout Europe to hide transactions with Iran
- Smuggling gold and cash through Dubai and Tehran airports using “diplomatic channels” with Iran
- Using third-party intermediaries to obfuscate illicit payments, such as to acquire maritime vessel ‘New Regent’ and import Belarusian luxury vodka
- Using shell companies to disguise beneficial ownership and form joint ventures with unsuspecting foreign companies
- Exploiting embassy personnel and using suspicious documents to attempt to access frozen assets, including funds frozen by an Austrian bank on suspicion of money laundering
- Continuing to perpetrate increasingly sophisticated cyberattacks against financial institutions and cryptocurrency exchanges globally to illicitly obtain fiat currencies and cryptocurrencies

UN report

RUSI issues report on North Korean Proliferation Financing in Southern and Eastern Africa

The Royal United Services Institute (RUSI) published a paper on 24 April, which examines the methods North Korea employs in Southern and Eastern Africa to fund its nuclear weapons programme – known as proliferation financing (PF) – and puts forward a number of recommendations to help combat the problem.

Historically, North Korean PF efforts in the region have included revenue generation efforts, which involve carrying out fundraising activities such as military cooperation or wildlife smuggling, as well as the establishment of “financial and corporate networks” that use a variety of tactics, such as the use of front companies, to facilitate the transfer of funds across and out of Southern and Eastern Africa on behalf of the North Korean regime.

In their study of countries that belong to the Eastern and Southern African Anti-Money Laundering Group (ESAMLG), the authors of the RUSI report found that many of these countries “lack the necessary legislation and regulation” to fully satisfy international counter proliferation financing (CPF) obligations – leading the authors to recommend, amongst other policies, the implementation of more stringent CPF regimes that “go beyond” targeted financial sanctions screening.

RUSI report
EU’s Barnier calls on UK to ‘engage seriously’ in talks for economic and security partnership

The EU’s Brexit negotiator, Michel Barnier, warned on 24 April that the UK “refused” during the second round of negotiations over its future relationship with the bloc to “engage seriously” on resolving several “fundamental” issues contained in the political declaration both parties signed in October 2019.

The head of the EU’s taskforce for relations with the UK stated that “disappointing” progress was made in recent negotiations over police and judicial cooperation in criminal matters; governance and enforcement of the future partnership; a level playing field for British and European businesses; and arrangements for fisheries.

Barnier noted that the EU gave the UK on 18 March a full draft legal text, which includes measures to prevent money laundering and terrorist financing, while the UK has only provided confidential proposals on “some areas” and stipulated that these cannot be shared with EU member states, the European Parliament or news agencies.

UK’s Covid-19 job retention scheme likely target of organised crime, warns HMRC

As part of a UK parliamentary inquiry into the economic impact of Covid-19, the First Permanent Secretary and Chief Executive of HM Revenue and Customs (HMRC), Jim Harra, told the House of Commons Treasury Select Committee on 8 April that organised criminals and fraudsters are likely to target the government’s Covid-19 job retention scheme. However, noted Harra, the plan includes safeguards to help protect the scheme from abuse.

According to Harra, the new scheme is expected to pay out large sums of money and therefore “attracts criminals that want to defraud it and people that are genuinely entitled to it who inflate their claims”. To counter this, the government has put in place “four lines of defence”.

Key anti-fraud measures

- A whistleblower hotline to encourage workers to report abuse by their employer

- A requirement that “furloughed” worker was already on the payroll on 28 February to ensure that no payments are made to “fake” employees

- An obligation that the employer has already been authenticated by HMRC’s online system

- Checks before and after wage payout to ensure the worker’s claim is real, in particular in high-risk sectors
Interpol’s Covid-19 global threat assessment finds sharp increase in cyber and fraud threats

Interpol published on 6 April the findings of a global threat assessment, which looks at the impact of Covid-19 on existing criminal markets, the rise of new criminal opportunities and the impact on police infrastructure.

The report identifies challenges affecting policing across different regions, best practices and the use of innovative tools to address the ongoing challenges, such as the use of drones, biometrics and artificial intelligence. The report is available for law enforcement only and will be updated regularly as new threats emerge.

Key findings

- The pandemic has led to a significant increase in cyber threats and drug commerce via social media, encrypted apps and the Darknet
- Interpol has issued several purple notices in relation to increased ransomware attacks and new types of Covid-19 related fraud
- Health service providers and essential product outlets are increasingly being targeted as critical infrastructure, which includes an increase in fraudulent and counterfeit trade in personal protective equipment (PPE) and anti-viral pharmaceuticals
- Individuals and businesses on reduced incomes have become the target of loan sharks
- Burglaries targeting empty factories or business premises and an increase in the online activity of paedophiles and domestic violence cases have also been identified

EU Parliament’s thinktank identifies crypto-asset ‘blind spots’ in AML/CFT regime

The European Parliament’s thinktank published on 7 April a report recommending measures to address “blind spots” in the bloc’s efforts to combat money laundering, terrorist financing and tax evasion through crypto-assets.

The 77-page report states that the EU’s AML/CFT framework “already lags behind the current reality” in cryptospace and is not fully equipped to counteract financial crime.

Recommended measures include

- Introducing a European AML watchdog to assess risks, promote information sharing, serve as a knowledge pool and probe suspected compliance breaches
- Updating EU financial services legislation to ensure existing financial rules apply to crypto-assets that are financial instruments
- Ensuring an adequate regulatory approach to financial institutions that have crypto-asset dealings or holdings
- Broadening the list of obliged entities under the EU’s AML/CFT framework to possibly include crypto-asset issuers or offerors

- Including tokens under the EU Money Laundering Directive’s definition of virtual currencies
- Establishing minimum cybersecurity standards for intermediaries that offer custodial services for crypto-assets
- Assessing the technical feasibility of blacklisting coins used in ransomware cyberattacks and the potential impact on the crypto market as a whole
Financial Stability Board report to G20 on cross-border payments identifies AML/CFT 'frictions'

The Financial Stability Board (FSB) published on 9 April its first report for the G20 on its plans to develop a roadmap to enhance cross-border payments, which sets out the challenges of running transactions across multiple jurisdictions with diverse legal and regulatory practices. The report highlights the need to address ongoing "frictions", such as the uneven implementation of anti-money laundering and countering the financing of terrorism (AML/CFT) rules and the divergent licensing regimes and prudential supervision practices.

The FSB report highlights the impact of divergent national AML/CFT standards on the effectiveness of cross-border payments

The report explains that weaknesses in the implementation of the Financial Action Task Force (FATF) AML/CFT standards by jurisdictions and firms, as well as weak sanctions screening policies, will exacerbate cross-border risks of illicit finance and will increase the need for correspondents and other institutions in the payments chain to apply additional controls. In addition to this, divergences in the national sanctions lists might lead to different stakeholders obtaining different information which may contain errors.

The report also states that differences between the national regimes make compliance checks more costly to design, hamper automation and may lead to significant delays or the rejection of payments; problems which will be more evident in transactions involving high-risk jurisdictions. A question to explore further, in the FSB’s opinion, is which type of initiatives could be adopted to make AML/CFT checks more efficient and less costly and build stronger regulatory frameworks.

The FSB report was due to be considered by the G20 Finance Ministers and Central Bank Governors at their virtual meeting on 15 April.
IMF warns Malta risks FATF greylisting over ‘significant’ AML deficiencies

The International Monetary Fund (IMF) warned in a 10 April report that Malta needs to urgently address “significant deficiencies” in the effectiveness of its anti-money laundering (AML) regime, including by ensuring the Malta Financial Services Authority (MFSA) is adequately and independently resourced to supervise regulated firms.

IMF assessors warned that a failure to address shortcomings in the effectiveness of Malta’s AML supervision, investigation, prosecution and confiscation – as highlighted in a July 2019 report by Moneyval – may result in the EU member state being placed on FATF’s “greylist” of jurisdictions with strategic AML deficiencies by early 2021.

The MFSA stated on 11 April that it “remains on track” in addressing recommendations by the IMF and other international institutions to improve its AML supervisory oversight.

Recommended areas of focus

- Improving understanding and risk-based AML supervision of financial flows associated with non-resident clients, remote gaming, virtual financial assets (VFAs) and the individual investor programme
- Increasing the frequency and “intrusiveness” of supervisory inspections to ensure banks implement customer due diligence (CDD) measures for non-resident clients and verify beneficial ownership information
- Strengthening supervision of high-risk sectors such as remote gaming and VFAs in line with recently conducted sector risk assessments
- Imposing timely enforcement actions with “dissuasive and proportionate” sanctions for AML/CFT breaches
- Prioritising investigations, prosecutions and related confiscations for high-level and complex money laundering cases

UN’s Mali experts uncover transnational crime network linked to sanctioned individual

The UN Security Council’s panel of experts on Mali warned in a midterm report on 16 April that designated individual Mohamed Ben Ahmed Mahri (aka Rouggy) has a “string” of shell companies in Algeria, Mali, Morocco and the Niger likely established for laundering drug money and financing trafficking operations.

Those allegedly linked to Mahri

- Algerian-based Tilamsi Distribution, of which Mahri and his associate Ben Kazou Moulati are directors, and his brother Attaye Ben Ahmed Mahri (aka Attaye Ould Sidi Mohamed) is the manager and person in charge of the parent company in Gao
- Algeria-registered linked entity Tilams or Taldis, of which both brothers are company directors
- Groupe Sekouni International, an import-export company with a Laayoune-registered parent company, whose founder Mohamed Lamine Sekouni (aka Mohamed Ould Maatala) was arrested with Moulati in April 2018
- Niger-based import-export company Siyama, which was founded by Ben Ahmed Mahri’s associate Sidi Ahmed Mohamed (aka Hamadana), who was arrested following a major drug bust in March 2019
FATF MER advises South Korea to address money laundering risks from PEPs

The Financial Action Task Force (FATF) warned in a 16 April statement accompanying a mutual evaluation report (MER) that South Korea needs to step up efforts to prevent domestic and foreign politically exposed persons (PEPs) from laundering the proceeds of corruption.

Intergovernmental assessors rated South Korea as “compliant” or “largely compliant” with 32 of FATF’s 40 Recommendations and “partially compliant” with eight Recommendations. The nation was given “substantial” effectiveness ratings for five of FATF’s 11 immediate outcomes and “moderate” ratings for the remainder.

Priority actions include

- Expanding the scope of anti-money laundering (AML) obligations to include domestic and foreign PEPs, given South Korea’s identification of corruption as a major predicate offence to money laundering
- Preventing and detecting the use of “borrowed name” accounts, which are a common typology for money laundering and tax crimes in South Korea, and enabling law enforcement to investigate and trace the movement of funds through such accounts
- Expanding the list of predicate offences to money laundering to enable prosecutions for laundering the proceeds of all types of tax crimes, given that the only tax crime included within the scope of South Korea’s predicate offences is fraudulently obtaining tax rebates of more than ₩500 million (£326,400)
- Creating a forum for authorities to exchange information and monitor developments in proliferation financing

FATF press release
Report
UK's FIU publishes modern slavery high-risk indicators for the legal sector

The UK’s Financial Intelligence Unit published a report on 8 April on modern slavery and human trafficking in the legal sector. The report notes that the areas most exposed to such risks relate to immigration, criminal law, employment law and conveyancing, on which many of the red flags overlap with money laundering indicators.

Key high-risk indicators

- Unusual behaviour of asylum seekers referring asylum claims to immigration practitioners
- An unregulated individual approaching a regulated legal practitioner asking to enter a supervision arrangement
- The customer is always accompanied by the same individual and is not allowed to speak to the solicitor on their own
- Conveyancing practitioners should be aware of indicators likely to provide grounds for suspicion, such as excessive fluctuations in property value, unexplained investments into property, acquisitions in countries with high numbers of modern slavery offenders or other ML indicators

NCA report

United States commission on religious freedom recommends expanded sanctions

The US Commission on International Religious Freedom (USCIRF) released on 28 April its 2020 annual report, which recommends that the State Department increases its use of targeted sanctions to discourage international persecution of religious minorities, in accordance with the Global Magnitsky Human Rights Accountability Act and other sanctions-related legal authorities.

The USCIRF calls for the designation of India, Nigeria, Russia, Syria and Vietnam as “countries of particular concern” (CPCs) due to these governments’ involvement in religious abuses and the designation of six non-state actors as “entities of particular concern” (EPCs), including al-Shabaab in Somalia, Boko Haram in Nigeria, the Houthis in Yemen, Islamic State in Khorasan Province and the Taliban in Afghanistan and Hay’at Tahrir al-Sham in Syria. The USCIRF recommends that 15 other countries are placed on the "special watch list".

Key recommendations

- Impose targeted sanctions on Chinese government agencies and officials responsible for severe violations of religious freedom
- Impose sanctions on Burmese, Eritrean, Indian, Pakistani, Tajikistani, Turkmenistani, Nicaraguan, Cuban and Russian agencies and officials responsible for violations as well as on Iraqi Popular Mobilization Forces who direct militia engagement in severe violations of religious freedom
- Work with European allies on using targeted sanctions to pressure Russia to end religious freedom abuses and allow an international monitoring presence in Crimea
- US Congress to pass the Ukraine Religious Freedom Support Act, calling on the President to consider Russia’s religious freedom violations in Crimea and Donbas when determining designations
- Consider the permanent codification of the State Department’s authority under its annual appropriations law to impose individual visa bans for gross human rights violations

USCIRF press release
USCIRF 2020 annual report
GRETA's annual report on human trafficking

The Group of Experts on Action against Trafficking in Human Beings (GRETA) published its annual report for 2019 on 3 April. The report finds that the number of people across Europe identified as victims of human trafficking increased by almost half between 2015 and 2018 (from 10,598 to 15,310), and highlights problem areas in the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings.

Key findings include

- The punishment of traffickers continues to be unsatisfactory, with the number of prosecutions and convictions being too low in many countries, while when convictions occur – the sentences imposed are too lenient and the confiscation of a trafficker's assets only occurs on rare occasions
- GRETA has also noted some positive developments; there has been an increase in countries implementing legal provisions that allow the non-punishment of victims of trafficking who have engaged in unlawful activities as a result of their trafficking, while there has also been an increase in the number of countries that have criminalised the knowing use of services of victims of trafficking.

UN report finds violation of arms embargo and illicit exploitation of South Sudan’s resources

The UN panel of experts on South Sudan published its final report on 28 April, which details the developments since the formation of the transnational government in February 2020, particularly regarding the incomplete implementation of the security compromises made under the Revitalised Agreement on the Resolution of the Conflict in South Sudan. Concerns identified in the report include violation of the arms embargo, a lack of transparency in the management and sale of the country’s oil, and the illicit extraction and exploitation of gold and timber.

The panel determined that

- The National Security Service (NSS) arbitrarily detaining civilians and committing serious human rights violations, as well as violating the arms embargo, by receiving three deliveries of weapons
- The National Pre-Transitional Committee – the body which oversaw the pre-transitional period – failed to transparently manage the national funds allocated for peace implementation
- The NSS has benefited from the country’s largest economic resource – oil revenue – through its businesses, including the company Sudd Security Services Co Ltd, which has received payments for services relating to South Sudan’s oilfields. Furthermore, the NSS and the South Sudan People’s Defence Forces (SSPDF) have received in-kind non-monetary and off-budget donations for their protection of the oilfields
- The Eastern Equatoria administration has allowed unlicensed miners to extract gold using illegal equipment, and the SSPDF has received payments to protect the transportation of illegally harvested timber
The Sentry published on 2 April a 33-page report claiming that South Sudan’s opaque minerals sector is “riddled with corruption” and identifying indicators of possible money laundering.

The non-governmental organisation (NGO) recommended that financial institutions take “immediate steps” to identify and monitor the bank accounts of government officials, their business networks, family members and inner circles.

The report also called on US sanctions authorities to restrict transactions with foreign persons active in key sectors “captured” by South Sudan “regime elites” and to amend designations of South Sudanese individuals to include their family members.

The report alleges:

- South Sudan’s mining sector has poor accountability and oversight mechanisms, with opaque licencing processes, community agreements and public payments to the government.
- Alcardinal Mining Ltd, the company that holds the most mining licences in South Sudan as of February 2020, is owned by Ashraf Seed Ahmed Hussein Ali, a businessman known as Al-Cardinal who was designated by the US in October 2019 over alleged corruption.
- The President’s daughter, Winnie Salva Kiir, has an 11 percent holding in Chinese-owned Fortune Minerals and Construction Ltd, which has three active exploration licences in South Sudan.
- Manajem Company Ltd, which has three mining licences in South Sudan, lists the former vice president James Wani Igga’s son, Emmanuel Maring Wani Igga, as a 4 percent shareholder.
- Politically exposed persons including Lawrence Lual Malong Yor Jr and Deputy Defence Minister Malek Reuben Riak Rengu, who were placed under sanctions by the US and UN, control companies that received provisional gold dealing licences in 2016.
- The Governor of Eastern Equatoria, Louis Lobong Lojore, owns luxury real estate in Kenya and has ties to numerous mining companies through his wives Semira Ayen Althaeb and Natalina Leonard Madrawi, son Nachek Louis Lobong, and associate Lawrence Lual Malong Yor Jr.
- Consolidated Minerals & Energy Resources was 50 percent owned in 2012 by Agyedho Adwok Nyaba, daughter of then-government minister Peter Adwok Nyaba; the company currently holds a mining licence in Central Equatoria.
- Children have been identified as shareholders of two mining companies with active licences in South Sudan, Jok Bell International Trading Co Ltd and Harmony International Company, indicating possible money laundering.

The Sentry press release

Report
OPCW report finds Syrian government forces responsible for chemical attacks, EU to consider additional sanctions

The Organisation for the Prohibition of Chemical Weapons’ (OPCW) Investigation and Identification Team (IIT) published its first report on the use of chemical weapons in Syria on 8 April, which concludes that there are “reasonable grounds” to believe that the Syrian Arab Air Force was responsible for two aerial sarin attacks on the town of Ltamenah and the dropping of a cylinder of chlorine on the Ltamenah hospital in March 2017.

The report notes that the IIT could not find any evidence of criminal investigations conducted by the Syrian authorities in relation to the Ltamenah incidents during its investigation, which was conducted between June 2019 and March 2020. In addition, the report found that the strategic military operations in Ltamenah could “only occur pursuant to orders from the highest levels of the Syrian Arab Armed Forces”, but the IIT could not draw “definitive conclusions to the requisite degree of certainty as regards the specific chain of command for the orders in these three incidents”.

The report was shared with all OPCW state parties and the UN Secretary-General. OPCW Director General Fernando Arias said that it is for the OPCW member states and the UN to take any further action on the findings, as the IIT is not a judicial body able to assign individual criminal responsibility nor does it have the power to make findings on non-compliance with the Chemical Weapons Convention. The IIT began its work in June 2019 following a decision by the OPCW Conference of the State Parties in 2018, which mandated the IIT to identify those responsible for the use of chemical weapons in Syria in cases where the OPCW’s Fact-Finding Mission determined that chemical weapons have been used or likely used.

Both the US Secretary of State Mike Pompeo and the EU’s High Representative Josep Borrell praised the OPCW report. In Pompeo’s view, “the Syrian regime retains sufficient chemicals – specifically sarin and chlorine – and expertise from its traditional chemical weapons (CW) program to use sarin, to produce and deploy chlorine munitions, and to develop new CW”. Borrell said that the EU “strongly” condemns the use of chemical weapons by the Syrian Arab Air Force and is ready to consider imposing additional sanctions on Syria in view of the IIT’s findings.

In a statement released on 9 April, the UK’s Foreign Secretary Dominic Raab condemned the chemical attacks by the Assad regime and called on “all states party to the Chemical Weapons Convention, the UN Security Council, and other bodies to respond decisively and hold those responsible to account”. In his response to the report on 14 April, the UK Permanent Representative to the OPCW Peter Wilson said that “there is no room for any reasonable doubt about Syria’s responsibility for these attacks” and called on the international committee to support multilateral and national mechanisms to “ensure accountability for the crimes committed”.

In a letter sent to the UN Secretary-General on 13 April, the Syrian Ministry of Foreign Affairs condemned “in the strongest terms the report of the illegal Investigation and Identification team and rejects it in form and substance”. The letter claims that the OPCW report is “misleading” and its conclusions are “false and fabricated” to serve the “hostile plans of the United States of America and its allies and into an arena for settling political scores with Syria”.

In his speech on 15 April at the closed UN Security Council meeting on Syria, the UK Chargé d’Affaires to the UN Jonathan Allen said that the evidence produced by the IIT confirms the findings of previous UN-mandated investigations which found the Assad regime responsible for using chemical weapons. According to Allen, Syria remains in breach of its CWC obligations and UN Security Council resolution 2118 “by retaining a chemical weapons capability” contrary to its commitments and by failing to cooperate fully with the OPCW.

OPCW press release
OPCW report
OPCW Director General’s statement
Chinese money laundering groups control hundreds of UK bank accounts, finds NCA report

The UK’s National Crime Agency (NCA) published on 30 April a report on money laundering through Chinese underground banking channels and the use of “Daigou” to illicitly export to China goods purchased with criminal funds in the UK. The report was finalised in October 2019 to support applications for account freezing orders under the UK’s Proceeds of Crime Act (POCA).

The NCA found some Chinese students in the UK were being as "money mules" by money laundering gangs

Investigators determined that Chinese informal value transfer system (IVTS) providers are readily able to source “money mule” bank accounts in the UK, with the majority initially set up by UK-based Chinese students recruited through social media by members of Chinese money laundering gangs. In one case, a money laundering group that is known to control accounts at multiple financial institutions was able to gain control of approximately 600 accounts at one bank.

Investigators believe it is likely that funds from individual bank accounts controlled by Chinese money laundering groups are transferred to accounts of businesses that export high-end luxury goods to China, effectively as a form of trade-based money laundering. The exported goods are likely mis-described or undervalued on import into China to evade customs controls and import duties and taxes, according to the report.

Aperio Analysis

China has strict foreign currency controls and limits outbound foreign exchange transactions to $50,000 per Chinese citizen per annum. Underground banking channels have been created to move cash out of the country, which are deeply embedded in the international financial system, and includes hundreds of bank accounts. A large number of middle-class Chinese or government officials reportedly use underground banking services to buy properties or set up companies overseas. When it comes to cross-border real estate transactions involving Chinese buyers, increased KYC procedures are needed in order to ensure the money used to purchase properties has been transferred out of China legitimately.
The Financial Action Task Force (FATF) published on 30 April its mutual evaluation report (MER) on the United Arab Emirates (UAE), which recognises that UAE’s AML/CFT system has advanced significantly but that its effectiveness has yet to be confirmed. The report calls for “fundamental and major improvements” to limit the illicit finance risks the country still faces and to make national prevention systems more effective.

The MER notes that the UAE addressed many of the outstanding AML/CFT shortcomings by developing its national risk assessment (NRA), strengthening coordination mechanisms and the Financial Intelligence Unit (FIU) and resolving technical deficiencies in legislation. In addition, the main elements of an effective framework to prevent organised criminals and terrorists from misusing the UAE financial system are mostly in place but it is too early to assess their impact.

According to FATF, the country’s understanding of the AML/CFT risks and those associated with the funding of weapons of mass destruction is still developing. Investigations of TF offences have produced results, but the limited number of ML prosecutions and convictions remains a concern. Despite significant efforts by authorities, formal international cooperation is still not working effectively.

Key recommendations include:

- Pursue "the most immediate and pressing" ML risks, such as professional international money laundering networks
- Enhance the use of financial intelligence and improve identification of cross-border movements of cash and precious metals and stones
- Build a better understanding of TF sanctions and evasion among authorities and the private sector
- Expedite the implementation of AML requirements across the 39 company registries and develop the understanding of beneficial ownership to reduce the risk of legal persons misuse for ML/TF

---

Aperio Analysis

The structure of the UAE economy – split over seven emirates within which there are over 30 free zones and a total of 39 different company registries with varying beneficial ownership disclosure requirements – leaves it exposed to regulatory arbitrage. On top of this, factors such as the high use of cash, the use of the informal hawala money transfer system and the flow of large volumes of gold, increase the UAE’s vulnerability to TF and ML. In addition, Dubai’s real estate market is widely considered to be a haven for laundered cash. The UAE cannot afford to jeopardise its reputation as the Middle East’s main financial hub, on which it depends to continue to attract foreign businesses, particularly in the context of falling oil prices. The Basel Institute of Governance AML Index for 2019 rates the UAE as the country with the 52nd highest level of ML and TF risk out of 125 countries, the highest risk rating of any GCC country. Saudi Arabia became the first Arab country to join FATF in June 2019. The UAE is not currently a member of FATF.
Europol report predicts rise in money laundering and corruption levels as a result of Covid-19

Europol published a report on 30 April on the impact of Covid-19 on the serious and organised crime (SOC) landscape in the EU, which concludes that long-lasting criminal risks are likely to emerge from the pandemic, such as the increased use of non-EU countries with weaker anti-money laundering (AML) systems by organised criminals seeking to launder illicit profits.

Europol expects the impact of the pandemic on SOC and terrorism to unfold in several stages, the first of which brought about an increase in the levels of cybercrime, fraud and counterfeiting, carried out by individuals and organised criminal groups (OCGs). In medium term, the potential easing of lockdown measures will likely mean a return to previous levels of crime as well as new opportunities for criminal activities that will be exploited beyond the end of the crisis.

Europol has urged AML regulators to be vigilant over sectors such as real estate and construction.

Key points

- The pandemic might prompt EU-based OCGs to shift their ML operations to non-EU countries and higher risk jurisdictions in order to introduce larger amounts of capital from illicit sources
- AML regulators must better monitor the real estate and construction sectors, companies involved in the import and export of goods and money services businesses as potential investment targets for money launderers
- Shell companies and companies based in offshore jurisdictions are likely to be exploited at the placement stage to receive illicit cash deposits
- The OCGs active during the Covid-19 pandemic are largely the same as before the crisis, but cybersecurity threats have evolved during the crisis into more sophisticated attacks
- Mafia-type OCGs are expected to take advantage of economic hardship by recruiting vulnerable young people to engage in loan sharking, extortion and racketeering
- The aftermath of the crisis might see a perceived or real increase in the level of corruption by EU public officials
- Europol expects little long-term impact on the trade of illegal drugs and a potential increase in migrant smuggling post-coronavirus
Banks should better embed fraud compensation standards, finds UK Lending Standards Board

A summary report published by the UK’s Lending Standards Board (LSB) on 30 April finds that all banks have taken steps to implement the requirements of the Contingent Reimbursement Model (CRM) code for authorised push payment (APP) scams, but more efforts are needed to streamline refund processes, better identify vulnerable fraud victims, issue effective warnings and keep accurate records of compensation claims.

The voluntary CRM code, launched on 28 May 2019, provides protection for customers, micro-enterprises and small charities that fall victim to APP scams, and applies to transactions on or after that date. The LSB's review took place between October 2019 and January 2020 and focussed solely on the requirements of the code for reimbursing fraud victims. Based on the review’s findings, the LSB has issued tailored recommendations to the nine code signatories. The LSB is due to carry out a full review of the code and complete other follow-up thematic reviews later this year.

Responding to the LSB’s report, UK Finance Managing Director Katy Worobec said on 30 April that the share of APP scam losses being refunded has more than doubled since the entry into force of the CRM code, reaching an overall level of 43 percent in the last six months. According to UK Finance, signatory firms continue to assess the fraud landscape to tailor their warning messages and train their staff to better recognise customers’ individual vulnerabilities when submitting their scam claim and ensure evidence is recorded effectively. In addition, UK Finance makes the case for addressing issues of liability and reimbursement through new legislation due to the limitations of a voluntary agreement such as the CRM code.
US guidance recommends banks improve response to North Korean cyber threats

On 15 April, US authorities issued guidance on mitigating the cyber threats posed by North Korean state actors, which includes a summary of recent attempts to steal and launder money from financial institutions and cryptocurrency exchanges to support Pyongyang's nuclear and ballistic missile programmes.

The 12-page advisory from the FBI and Departments of State, Treasury and Homeland Security includes an overview of possible UN and US sanctions against individuals and entities that engage in transactions linked to North Korean designated entities or cyber activities.

Recommended measures

- Sharing North Korean cyber threat information through government and/or industry channels
- Complying with US law enforcement requests for information regarding North Korean cyber threats
- Identifying forfeitable assets requested by US law enforcement or court orders and cooperating with efforts to seize those assets
- Giving "special attention" to business relationships and transactions with North Korean companies, financial institutions and representatives
- Terminating correspondent banking relationships with North Korean lenders
- Developing and maintaining effective anti-money laundering (AML) programmes
- Identifying and reporting suspicious transactions, including those conducted, affected or facilitated by cyber events or illicit finance involving crypto-assets
- Undertaking awareness training on common social engineering tactics
- Developing cyber incident response plans
- Implementing policies on information sharing and network access
- Segmenting networks to minimise risks
- Maintaining regular backup copies of data

State Department press release

Guidance
HKMA encourages remote on-boarding and simplified due diligence during Covid-19 crisis

The Hong Kong Monetary Authority (HKMA) sent a letter to all authorised institutions on 7 April, to provide guidance on money laundering and terrorist financing (ML/TF) risk management during the pandemic.

Amongst the measures proposed to meet the challenges presented by the pandemic, the HKMA suggests that firms use remote on-boarding and simplified due diligence as well as the use of financial technology where a lower ML/TF risk is identified.

Key observations and recommendations

- The use of FinTech provides opportunities to manage social distancing. More than 10 banks have launched remote account opening services since 2018
- Where lower ML/TF risks are identified, HKMA allows simplified due diligence measures – specifically, authorised firms should “effectively understand” the risks involved when opening accounts “solely for the purpose of the Government’s HK$10,000 cash payout scheme” and apply the lowest level of customer due diligence as “commensurate with the circumstances”
- Firms should remain vigilant to emerging ML/TF risks and ensure that they focus on priority areas and effectively mitigate risks through information sharing and suspicious transaction reporting to the Joint Financial Intelligence Unit (JFIU)
- HKMA encourages public-private information and typologies sharing to help prioritise and address Covid-19 related fraud risks

Philippine central bank ‘relaxes’ KYC rules for banks during Covid-19 lockdown

The Philippine central bank announced on 1 April that it has “relaxed” know-your-customer (KYC) requirements for financial institutions until 30 June to facilitate the delivery of welfare funds to individuals under the Covid-19 community quarantine.

Bangko Sentral ng Pilipinas stated that banks are not required to obtain valid identification documentation for customer onboarding and transactions during the three-month period “since the accounts involved are considered as low risk”. Firms are however expected to obtain “the required minimum information” from new clients and to perform risk-based customer due diligence (CDD).

Financial institutions should mitigate money laundering and terrorism financing risks from new accounts by ensuring

- Customers reside or conduct business in a quarantined area
- Customers certify that they have no valid ID
- Customer account activities are subject to ongoing monitoring

Central Bank press releas...
Arab Monetary Fund issues digital identity and e-KYC guidelines

The Arab Monetary Fund (AMF) published on 27 April a set of guidelines on digital identity and electronic know-your-customer (e-KYC) processes for the Arab region, which sets out the need for reliable ID systems, underlines existing cybersecurity and money laundering/terrorism financing risks and proposes a list of action points for regulators in the region.

The guidelines describe the benefits of using a tiered e-KYC regime to reduce fraud, carry out identity checks more effectively and reduce customer due diligence (CDD) costs.

The guidelines have been drafted by the Arab Regional Fintech Working Group, based on responses provided by regulatory and supervisory authorities in 18 Arab countries, which highlighted that the overall implementation of digital ID systems in the region is still in the early stages. In addition to this, 10 of the respondent Arab countries have implemented an e-KYC model, among which Bahrain and the United Arab Emirates are the most advanced.

Key action points for Arab regulators

- Set up a unique and interoperable digital ID framework and provide regulatory clarity to support digital innovation
- Establish a risk based CDD regime to comply with AML/CFT regulations and address financial inclusion objectives
- Issue standards for the use of ‘non-government’ backed ID systems and ensure minimal information sharing during CDD procedures
- Implement a strong governance model to manage the digital ID and CDD regime
- Collaborate with regional and international bodies and regulators

FATF extends all mutual evaluations and follow-up deadlines in the wake of the pandemic

The Financial Action Task Force (FATF) announced on 28 April that it is temporarily suspending all assessment and follow-up deadlines due to the "severe challenges" posed by the Covid-19 pandemic. As a result, all high-risk jurisdictions subject to increased monitoring or calls to action will be given a four month extension on their current deadlines.

Notable exceptions are Mongolia and Iceland, which have voluntarily requested to continue with their current schedules. FATF statements on Mongolia and Iceland are due to be published in June. Going forward, FATF stated that it will review deadlines further when necessary.

FATF explained that despite the challenges posed by the pandemic it continues to remain vigilant in combatting financial crime and is actively monitoring the impact of the crisis on measures to combat illicit financing.
FATF President outlines actions to fight illicit finance and fraud during Covid-19 pandemic

The Financial Action Task Force (FATF) President Xiangmin Liu issued a statement on 1 April on measures to combat illicit finance amid the Covid-19 outbreak, calling on financial services providers to remain vigilant to emerging money laundering and terrorist financing risks and able to detect and report suspicious activity.

According to FATF, Covid-19 related crimes might include financial fraud, fraudulent investment offers, phishing schemes, fake advertising or trafficking in counterfeit medicines. In addition to this, malicious cybercrime, fundraising for fake charities and medical scams are likely to increase. To respond to the ongoing challenges, FATF encourages governments to work with financial institutions to use the flexibility built into FATF's risk-based approach.

FATF’s Covid-19 related recommendations include:

- Address weaknesses in national anti-money laundering/counter financing of terrorism (AML/CFT) systems and make risk-based supervision a priority.
- Encourage the use of technology, including Fintech, Regtech and Suptech, in line with the FATF Guidance on Digital ID, and explore using digital identity.
- Explore the appropriate use of simplified measures where there is a low ML/TF risk.
- Apply a risk-based approach to ensure that legitimate non-profit organisations (NPO) activities are not delayed, disrupted or discouraged without reason.
- Establish mechanisms by which victims and businesses can report Covid-19 related fraud.

UK’s FCA sets out its anti-money laundering work in letter to Commons committee

The UK Financial Conduct Authority’s (FCA) Interim Chief Executive Christopher Woolard sent a letter to the House of Commons Treasury Select Committee on 11 April providing an overview of the FCA’s activities in the field of anti-money laundering (AML) supervision during Andrew Bailey’s tenure as chief executive between July 2016 and March 2020.

The letter notes that the FCA has identified some improvements in AML controls among larger firms as part of its supervisory activity, but the overall picture remains mixed, with more efforts necessary in specialist sectors such as investment management, e-money and capital markets. Since July 2016, the FCA has imposed fines of £334,540,148 on firms and individuals for AML-related failures.

Other key points:

- To respond to its expanding remit and better target firms at greatest risk of money laundering, the FCA aims make greater use of intelligence and data.
- The FCA is working with other UK agencies and the Financial Action Task Force (FATF) to minimise regulatory barriers to innovation.
- Since 2017 the FCA has communicated with over 400 small firms, including payment institutions, in relation to the management of AML risks within their sector.
- The FCA’s Office for Professional Body Anti-Money Laundering Supervision (OPBAS) continues to monitor all AML strategy plans received in 2019 from professional body supervisors.

See FCD portal
Brazil’s BRF settles US securities fraud lawsuit for $40m, discloses Iran transactions

Brazil-based BRF SA disclosed in a US securities filing on 24 April that it has agreed to a $40 million settlement of a securities fraud lawsuit alleging the firm’s senior executives bribed regulators and politicians to subvert inspections of its meatpacking plants as part of “an unprecedented and massive case of food fraud”.

The class action suit by shareholders, which was filed in March 2018, alleges that the Brazilian food processing company repeatedly made false statements to investors about its compliance with legal requirements and international standards governing food products and failed to disclose its alleged bribery scheme.

BRF also disclosed in its annual report to the US Securities and Exchange Commission (SEC) that, in the year ending 31 December 2019, a non-US affiliate of the company received €467,959 in payments from an Iranian company affiliated with the government of Iran. BRF stated that it believes the transactions, which form part of an ongoing single contract for agricultural commodities, “comply in all material respects” with all applicable US sanctions against Iran, but noted that “such laws are complex and continue to evolve rapidly”.

EU and Mexico agree final elements of trade agreement containing anti-corruption provisions

The European Union and Mexico agreed on 28 April a framework for the reciprocal opening of public procurement markets as part of a trade agreement that includes anti-corruption provisions to counteract bribery by government officials, money laundering through opaque entities and corruption in trade and investment.

The EU and Mexico will sign and ratify the finalised trade agreement, which was reached in principle in April 2018 to ensure 99 percent of products traded are duty free.

Aperio Analysis

A particularly interesting aspect of this agreement is that it is the first time the EU has negotiated provisions to combat and prevent corruption in trade and investment in the scope of a trade agreement. The objectives of the provisions are to prevent corruption in trade and investment, notably by promoting integrity in the private and public sector, enhancing internal controls, external auditing and financial reporting as well as to strengthen the fight against corruption through international conventions.
Luckin Coffee Inc’s internal fraud probe identifies fabricated transactions

The multi billion-dollar Chinese coffee startup, Luckin Coffee Inc, announced on 2 April that it has formed a Special Committee to oversee an internal investigation into allegations that Director and Chief Operating Officer, Jian Liu, and several other employees, engaged in misconduct, including fabricating transactions.

The internal probe was prompted by short-selling activist firm Muddy Waters, which took a short position on the company after receiving an anonymous 89-page report that claimed Luckin Coffee was inflating its sales figures.

Luckin Coffee has since suspended Jian Liu and the employees implicated in the misconduct and has suspended and terminated contracts and dealings with the parties involved in the fabricated transactions.

At this stage of Luckin Coffee’s internal investigation the aggregate sales amount associated with the fabricated transactions from the second quarter of 2019 to the fourth quarter of 2019 amounts to around ¥2.2 billion (£16.3 million). Certain costs and expenses have also been found to have been substantially inflated during this period.

Reuters reported on 3 April that China’s securities regulator has confirmed that it is investigating claims of accounting fraud at Luckin Coffee Inc.

Luckin Coffee published a statement on 3 February in response to the allegations in which it claimed that the anonymous report which was made public on 31 January by Muddy Waters contained misleading and false information.

FCA eases CDD checks for small UK businesses seeking government-backed Covid-19 loans

The UK’s Financial Conduct Authority (FCA) announced on 27 April that regulated firms administering government-backed loans to small businesses affected by the coronavirus pandemic do not need to conduct additional due diligence checks on existing customers if they do not pose a higher risk of financial crime.

Authorised firms are required to conduct customer due diligence (CDD) for new clients seeking funds under the government’s coronavirus business interruption loan scheme (CBILS) and bounce back loan scheme (BBL), but may apply simplified due diligence if the money laundering and terrorist financing risks are low.

The UK’s Financial Conduct Authority (FCA) announced on 27 April that regulated firms administering government-backed loans to small businesses affected by the coronavirus pandemic do not need to conduct additional due diligence checks on existing customers if they do not pose a higher risk of financial crime.
OECD recommendations for countering public sector fraud and corruption during pandemic

Recommendations include

**Short-term**
- Establishing a central price and supplier tracking system for key products and services to help identify red flags, collusion, price gouging and counterfeits
- Establishing specialised oversight bodies to conduct audits and identify fraud and abuse in crisis-related spending
- Analysing potential corrupt patterns involving procurement of personal protective equipment (PPE)
- Favouring existing collaborative procurement instruments whenever possible to avoid awarding contracts without competition

**Long-term**
- Using or expanding existing e-procurement platforms to record transactional information on procurement of emergency items
- Creating a database to analyse bidding patterns and identify potential red flags
- Allowing auditors and oversight bodies remote access to all procurement records to enable them to continue their investigations and identify emerging integrity risks

OECD report

EU pensions supervisor expects members to effectively manage fraud risks during pandemic

The European Insurance and Occupational Pensions Authority (EIOPA) issued a statement on 17 April on principles to mitigate the impact of Covid-19 on the occupational pensions sector, which outlines EIOPA's business continuity expectations and the impact on national authorities and pension scheme members posed by the increased fraud risk.

EIOPA expects national competent authorities (NCAs) and the EU's institutions for occupational retirement provision (IORPs) to adhere to its principles in a risk-based and proportionate manner. According to the statement, NCAs should expect IORPs to consider and manage effectively the increased risk exposure to fraud and other financial crimes caused by the disruption to society, which includes cybersecurity and data protection issues related to remote working.

In addition, NCAs should monitor the liquidity positions of IORPs in the current volatile markets and encourage more flexibility to safeguard pension rights. Deadlines for the provision of occupational pensions information to EIOPA were extended by two weeks for reports regarding the first quarter of 2020 and by eight weeks for year-end 2019 annual reporting.

EIOPA statement
Czech Republic warns of imminent large-scale cyberattacks against healthcare system

The Czech Republic’s Cyber and Information Security Office (NUKIB) issued cybersecurity recommendations on 17 April after warning on 16 April that a large-scale campaign of “serious” cyberattacks was expected in the “coming days” against the healthcare sector’s information and communication systems and other major targets. The NUKIB stated that it assessed the threat level as “probable to very probable”.

The US State Department warned in a 17 April statement that responsible states will be held accountable for “malicious” cyber activities and called on the suspected actor to “refrain” from attacking the Czech Republic’s healthcare system or similar infrastructure elsewhere.

UK’s NCSC launches campaign to combat cyber threats related to Covid-19

The UK’s National Cyber Security Centre (NCSC) launched on 21 April a cross-governmental ‘Cyber Aware’ campaign to promote behaviours to mitigate cybersecurity threats, the ‘Suspicious Email Reporting Service (SERS)’ to help assess and take down malicious content, and guidance for individuals and organisations hosting online video conferences, particularly in the context of the emerging scams seeking to take advantage of the pandemic.

The ‘Cyber Aware’ campaign provides recommendations for remaining vigilant and staying secure online during the pandemic, including: (1) creating a separate password for emails, (2) create strong passwords using three random words, (3) turning on the two-factor authentication (2FA) feature, and (4) updating devices and using the latest versions of software.

The SERS can be used by anyone who receives a suspicious email. The NCSC will analyse the suspect email and the websites it links to, in order to block the account that the email came from, remove the links to the malicious websites and raise awareness about commonly reported emails and methods used.

The NCSC’s guidance on the secure use of video conferencing services provides the steps to be taken in order to use the service safely, such as: (1) downloading the video conferencing software from trusted sources, (2) make sure the video conferencing account is protected with a strong password, and (3) keeping the meetings and calls private and making sure it is known exactly who is joining the call.

The NCSC also announced that it has already removed more than 2,000 online scams related to coronavirus in the last month, including 471 fake online shops selling fraudulent coronavirus related items, and 832 advance-fee frauds.
EU and UN launch joint initiative to return illicitly obtained assets to Eastern Partnership Countries

The EU and United Nations Interregional Crime and Justice Research Institute (UNICRI) launched on 6 April a programme to help Eastern Partnership Countries – namely Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine – trace and confiscate assets linked to organised criminal activity.

The programme will provide specialised training, peer-to-peer mentoring and legal advice to ensure inter-institutional and cross-border coordination in the Eastern Partnership region, specifically in financial crime investigations. The EU has committed €1.5 million to the initiative, which will cover a three-year period.

Lawrence Meredith, Director for Neighbourhood East at the European Commission, said that the initiative marks “a significant step forward in the EU’s support for Eastern Partnership countries in addressing their needs to counter many different forms of organised criminal activity, including drug trafficking, human trafficking and migrant smuggling.”

The UN estimates that approximately two to five percent of global GDP (€725 billion – €1.8 trillion) is laundered worldwide every year.

Aperio Analysis

The Eastern Partnership has been created to encourage cooperation between the EU and those post-Soviet countries that wish to see themselves as affiliated with Europe, rather than Russia. Crucially, the arrangement did not guarantee future EU membership which, arguably, has limited the initiative’s achievements to date. The region continues to be a sensitive topic, as Russia would see any strengthening of its links with the EU as a threat to its interests, and several existing EU members states openly oppose the idea of the six countries’ membership. To an extent, the efforts to return illicitly obtained assets to the communities of the Eastern Partnership countries will test the region’s ties to both Russia and the EU. The initiative is crucial for the EU too, as several recent cases have shown that illicit funds often flow to Europe from Russia through countries such as Moldova. However, for this to be successful, serious political will and commitment are required on all sides, and for a much longer period than three years.

UK regulators issue statements on compliance with senior managers regime during pandemic

The UK’s Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) published on 3 April a joint statement setting out their expectations of how dual-regulated firms should comply with the senior managers and certification scheme (SM&CR) during the Covid-19 pandemic.

The regulators stated that individuals performing senior management functions such as compliance oversight and money laundering reporting officers (MLRO) should only be furloughed as “a measure of last resort”.

The FCA separately announced on 3 April its expectations of how solo-regulated firms should manage their risks, allocate managerial responsibility and record governance changes during the global health crisis.
UK’s NCA announces new SAR glossary codes for reporting coronavirus-related fraud

The UK’s National Crime Agency (NCA) published on 29 April an updated booklet on suspicious activity reports (SARs) that contains three new glossary codes for reporting changes in patterns or behaviours in bank accounts or other suspicious activity connected to the Covid-19 pandemic.

The booklet states that the UK financial intelligence unit (UKFIU) implemented the new glossary codes in response to the increased threat of fraud by organised crime groups seeking to exploit the pandemic.

**The new glossary codes**

- Code “XXSATXX” for reporting suspected fraudulent use of the self-assessment tax refunds system
- Code “XXGPSXX” for reporting suspected fraudulent use of government priority schemes established to support businesses and individuals affected by the pandemic
- Code “XXCVDXX” for reporting other suspicious activity connected to Covid-19

UK’s FCA discloses 23 criminal investigations into breaches of Money Laundering Regulations

The UK’s Financial Conduct Authority (FCA) had four single-track criminal investigations and 12 dual-track criminal and civil probes into possible breaches of the Money Laundering Regulations 2007 as of 20 November 2019, according to a letter published on 28 April.

The regulator disclosed in a freedom of information (FOI) response that suspected compliance breaches by financial services firms included failures to comply with customer due diligence (CDD), ongoing monitoring and recordkeeping requirements.

The FCA has not yet launched a prosecution for a breach of the Money Laundering Regulations 2017.

The FCA separately revealed in a FOI response dated 14 November, which was also published on 28 April, that it had ongoing criminal cases against three individuals and dual-track investigations into one individual and three firms over suspected breaches of the Money Laundering Regulations 2017.

The regulator added that it has not yet prosecuted any firms for breaching the Money Laundering Regulations 2017 or for “failure to disclose” offences under the Proceeds of Crime Act (POCA).
UK FCA did not apply for any UWOs between January 2018 and November 2019

The UK’s Financial Conduct Authority (FCA) did not apply for any unexplained wealth orders (UWOs) between 31 January 2018 and 20 November 2019, according to a freedom of information (FOI) response published on 28 April.

The Criminal Finances Act 2017 amended the Proceeds of Crime Act (POCA) with effect from 31 January 2018 to introduce UWOs, which require respondents to explain how they obtained and paid for their property.

The financial regulator added in its letter dated 18 December 2019 that 39 restraint orders under POCA were in force against individuals subject to criminal investigation or prosecution. The orders prevent suspects from dealing with the assets pending a confiscation order.

UK’s FCA reveals that it referred 192 cases of suspected money laundering to NCA in 2018

The UK’s Financial Conduct Authority (FCA) disclosed in a letter published on 28 April, statistics on the number of suspicious activity reports (SARs) related to money laundering that it submitted to the National Crime Agency (NCA) over a three-year period.

The financial regulator stated in a 21 October response to a freedom of information (FOI) request that it made 192 SAR disclosures to the NCA in 2018, up from 155 reports in 2017 and 117 disclosures in 2016 related to suspected money laundering.
UK’s FCA discloses probes into two e-money firms over suspected AML breaches

The UK’s Financial Conduct Authority (FCA) had ongoing investigations into two e-money institutions (EMIs) and none into authorised payment institutions (APIs) for possible breaches of the Money Laundering Regulations as of 25 November 2019, according to a freedom of information (FOI) response published on 28 April.

The FCA stated that it had not closed any investigations or taken any enforcement actions against EMIs or APIs under the Money Laundering Regulations in 2019, noting that it may instead investigate harm or misconduct involving payment institutions and e-money firms under other relevant regulations.

Firms in tax havens barred from Covid-19 financial aid in Poland, Denmark and France

Polish Prime Minister Mateusz Morawiecki announced on 8 April that large companies will be able to access a PLN 25 billion (£4.8 billion) Covid-19 aid package provided they “pay taxes in Poland and not in tax havens”.

Similar announcements have since been made in Denmark and France.

On 18 April, the Danish Finance Ministry announced that Danish companies registered in countries on the European Union’s list of non-cooperative tax jurisdictions will not be eligible for financial aid. In addition, companies receiving more than DKK 60 million (£7 million) are restricted from paying out dividends or buying back their own shares until 2021.

During an interview on 22 April, French Economy and Finance Minister Bruno Le Maire said that companies headquartered or with subsidiaries in a tax haven will not be allowed to benefit from financial aid. “There are rules that must be followed. If you have benefited from the state treasury, you cannot pay dividends and you cannot buy back shares”, Le Maire added.

In response to these announcements, Tax Justice Network (TJN) published a report on 23 April on tax responsible rules for coronavirus bailouts, which argues that the EU’s blacklist of non-cooperative jurisdictions ignores some of the most significant tax havens, predominantly member states of the EU. Additionally, TJN calls for wider criteria for excluding companies from coronavirus bailouts, such as previous involvement in money laundering, tax evasion, profit shifting or other illicit financial flows scandals.

In a statement issued on 20 April, Tax Justice UK Executive Director Robert Palmer said: “The UK should follow Denmark and Poland’s lead and exclude tax haven companies from coronavirus relief. Companies that seek to dodge their obligations to society by cutting their tax bills shouldn’t expect a bailout when things go wrong. The UK should ensure that all bailouts come with conditions to ensure good business behaviour.”

Calls for stricter tax-related conditions for Covid-19 bailouts were also made by political opposition members in the German and Austrian parliaments on 21 and 22 April, respectively.
US DOJ publishes list of compliance monitors in corporate criminal fraud enforcement

The US Department of Justice (DOJ) published a list on 14 April identifying all corporate monitors actively engaged by companies as a part of criminal resolutions with the Criminal Division's Fraud Section, in a move that signals the DOJ's move towards increased transparency in corporate criminal enforcement and that corporate monitorships are now a mainstay of the DOJ's corporate enforcement policy.

The DOJ's monitor list names the companies and their monitors, noting the year when each monitorship began and the specific Fraud Section Unit overseeing the case. It is thought that the decision to publish the information may help identify trends in the Criminal Fraud Section's use of corporate monitors.

Vatican names new director of the Financial Information Authority amid ongoing scandal

The Holy See Press Office announced on 15 April the appointment of the new Director General and Vice Director of the Financial Information Authority (AIF), to replace Tommaso Di Ruzza, who was suspended in October 2019 as part of an investigation into suspicion of embezzlement, fraud, abuse of office, money laundering, misappropriation, self-laundering, corruption and abetment in the Secretariat of State’s purchase of a stake in a luxury residence in London.

The Vatican Secretary of State has named Bank of Italy official, Giuseppe Schlitzer, as the new Director General of the AIF. Federico Antellini Russo has been appointed to the position of Vice Director. During a press conference on 26 November 2019, Pope Francis said that Di Ruzza had been suspended due to "suspicions of poor administration". In addition to Di Ruzza's removal, Pope Francis decided not to renew the mandate of AIF president, René Brülhart.

Aperio Analysis

Schlitzer's appointment to the post of Director General of the AIF is significant. The decision to replace Di Ruzza and not renew the mandate of his superior, AIF president Brülhart, suggests that the pontifex maximus (Pope Francis) is no longer intending to compromise on transparency. Or, perhaps, that the ongoing Vatican probe into the 60 Sloane Avenue transaction, in which Di Ruzza is a suspect, is about to unearth a series of uncomfortable truths about the Vatican, and its foreign dealings. Yet, as with all Vatican matters, it remains to be seen whether or not the actual truth will be told.
US offers reward for information on financial networks of Hezbollah military commander

The US Department of State’s Rewards for Justice programme announced on 10 April a reward of up to $10 million for information on the activities, networks, and associates of Muhammad Kawtharani, a senior Hezbollah military commander who was designated as a global terrorist by the US in 2013. According to the US, Kawtharani is believed to have assumed a greater role in overseeing Hezbollah’s activities in Iraq since the death of Iranian commander Qasem Solemani.

It is alleged that Kawtharani facilitates the actions of groups operating outside the control of the Government of Iraq that have violently suppressed protests, attacked foreign diplomatic missions, and engaged in organised criminal activity. In addition to this, as a member of Hezbollah’s Political Council, Kawtharani is believed to have been involved in the promotion of Hezbollah’s interests in Iraq, which includes efforts to provide training, funding, political, and logistical support to Iraqi Shi’a insurgent groups.

Previously, the Islamic Revolutionary Guards Corp’s Quds Force was Iran’s primary liaison with its proxy Iraqi militias. However, after the assassination of Quds Force leader Qasem Soleimani, Hezbollah has taken over this role, largely led by dual Iraqi-Lebanese national Kawtharani. The US State Department designated Lebanon-based Shia Islamist political party and militant group Hezbollah as a FTO in 1997 and as a SDGT in October 2001. The US has a standing reward offer for information leading to the disruption of the financial mechanisms of Hezbollah, which reportedly generates $1 billion each year through direct financial support from Iran, international businesses and investments, donor networks, and money laundering activities. Kawtharani was designated by the US in 2013 for allegedly helping to transport fighters from Iraq to Syria, where Iran has been supporting President Assad. In recent months, the US has blamed Iranian-militias for several attacks on its bases in Iraq.

Iran’s Central Bank Governor comments on IMF loan request and possible use of INSTEX

The Governor of Iran’s Central Bank, Abdolnaser Hemmati, provided written answers to questions about Iran’s request for $5 billion in funding from the International Monetary Fund (IMF) to help combat Covid-19, which were published on 20 April. The answers to questions posed by Bloomberg, shed light on Iran’s hopes for securing the loans and the use of the EU’s special purpose vehicle INSTEX to facilitate the funds.

Hemmati states that Iran should be able to use its considerable foreign reserves, currently frozen under sanctions, to aid its Covid-19 relief efforts through INSTEX or the Swiss payment vehicle. In addition to this, the Governor suggests that this is a good opportunity to activate these new payment channels.

The Central Bank of Iran requested the loans from the IMF’s Rapid Financing Initiative on 6 March to help keep its economy afloat during the fight against Covid-19.
US to seek extension of arms embargo on Iran

US Secretary of State Mike Pompeo announced on 29 April that the US intends to take action to renew a conventional weapons embargo on Iran which is set to expire on 23 October, in line with UN Security Council resolution 2231 endorsing the Joint Comprehensive Plan of Action (JCPOA) on Iran's nuclear programme.

Pompeo urged France, Germany and the UK (known as the E3 countries) to ensure the arms embargo on Iran does not expire in October, adding that “in the event we can’t get anyone else to act, the United States is evaluating every possibility about how we might do that”. In response to criticism that the US is no longer part of the JCPOA, Pompeo said that resolution 2231 is “unambiguous” in its view that “the rights that accrue to participants in the UN Security Council resolution are fully available to all those participants”.

In an interview with Iran's state news agency on 29 April, Iran’s Permanent Ambassador to the UN Majid Takht-e Ravanchi rejected the US claims under the nuclear deal and said that adopting a new UN resolution to extend the arms embargo on Iran would violate resolution 2231 and international law.

US Senator Ted Cruz praised the US administration on 28 April for its plans to seek the renewal of the arms embargo on Iran and for considering the 'snapback mechanism', which would restore all Iran sanctions that have been lifted or eased since the adoption of the JCPOA. Cruz added that "Iran has consistently been in violation of nuclear restrictions before, during, and after the negotiation of the deal, and the Ayatollah is right now systematically advancing toward a nuclear weapon. It is well past time to reimpose international sanctions”.

EU extends advisory mission on security sector reform in Iraq until 2022

The EU Council decided on 7 April to extend the mandate of the Baghdad-based EU Advisory Mission in support of Security Sector Reform in Iraq (EUAM Iraq) until 30 April 2022, following an assessment of the National Security Strategy (NSS) and the support needed in the fight against terrorism, organised and financial crime, in particular corruption, money laundering and trafficking of cultural heritage goods.

For the first time, EUAM will coordinate a project cell for identifying and implementing projects. EUAM was launched on 16 October 2017 in response to a request by the Iraqi government and is mandated to advise officials of the Office of the National Security Adviser and the Ministry of the Interior regarding civilian related aspects of the NSS and other security sector reform issues.
Libra Association solicits Swiss payments licence for single currency stablecoins

Switzerland’s Financial Market Supervisory Authority (FINMA) announced on 16 April that it is processing a payment system licence application from the Libra Association, which intends to support both single currency stablecoins and the multicurrency Libra payment token.

FINMA warned that it will give “special consideration” to whether strict anti-financial crime standards can be upheld by the Geneva-based association. The Libra Association stated in an updated whitepaper on 16 April that it is developing a “comprehensive” risk management framework and “strong standards” for AML, CFT and sanctions compliance, in line with regulatory feedback.

Libra network participants would comprise: designated dealers; regulated virtual asset service providers (VASPs), including cryptocurrency exchanges and custodial wallet providers; and other individuals and entities seeking to transact or provide services through the network.

Libra’s proposed compliance measures include:

- Conducting risk-based due diligence on association members, designated dealers and VASPs
- Developing and periodically revising AML/CFT and sanctions compliance policies and procedures based on risk assessments and regulatory requirements
- Creating an internal audit function to periodically conduct independent reviews of the association’s compliance programmes

US Treasury issues sanctions guidance for humanitarian transactions with Iran, Cuba, others

The US Treasury Department’s Office of Foreign Assets Control (OFAC) published on 16 April consolidated guidance on key US sanctions exemptions, exceptions and authorisations for humanitarian aid or trade with Iran, Venezuela, Cuba, Syria, Crimea and North Korea in response to the Covid-19 pandemic.

The 10-page factsheet notes that US exporters of personal protective equipment (PPE) must comply with a temporary final rule by the Federal Emergency Management Agency (FEMA) requiring its explicit approval for certain PPE exports between 7 April and 10 August.
United Nations human rights chief calls for US to lift longstanding Sudan sanctions

On 28 April, United Nations High Commissioner for Human Rights Michelle Bachelet called for the US to remove sanctions against Sudan and for donors to “swiftly and generously” provide financial support to help counteract coronavirus in Sudan, which is ineligible for pandemic-related assistance from the International Monetary Fund (IMF) and World Bank.

Bachelet warned that the pandemic could be a “tipping point” for renewed instability and conflict in the Sudan, which remains on the US list of state sponsors of terrorism a year after ruler Omar al-Bashi was removed from power and now faces “acute” resource constraints on its transitional government.

The UN human rights chief added that a lifting of US sanctions, which were imposed against Sudan's previous government in 1993, would enable the nation to attract investment for economic reforms and access funds from international financial institutions.

Humanitarian exceptions to sanctions regimes need more clarification, states EU official

The EU’s High Representative for Foreign Affairs Josep Borrell stated on 20 April that the humanitarian exceptions to sanctions regimes should be fully utilised during the Covid-19 pandemic to ensure that essential supplies reach vulnerable people in the world’s poorest countries.

In support of statements by the UN Secretary-General António Guterres and UN High Commissioner for Human Rights Michelle Bachelet, Borrell added that more clarification on existing sanctions policies is needed as “many people do not believe that they can engage in humanitarian assistance to Iran or Venezuela without falling under the American sanctions”. In addition, a call for sanctions relief will be made again to assist with the most serious humanitarian crises.

According to Borrell, the breakdown in logistics chains and the difficulties in reaching vulnerable people will result in more deaths from hunger than from the disease itself. The EU High Representative also called for more coordinated action by the G20 and the international financial institutions, EU, China and the US to respond to the coronavirus pandemic.
National security leaders propose US adopts measures to up humanitarian trade with Iran

Two dozen US and European national security leaders issued a joint statement on 5 April calling on the US government to adopt sanctions measures that would increase humanitarian trade with Iran and help combat the Covid-19 pandemic.

According to the statement organised by the European Leadership Network and the Iran Project, existing humanitarian exemptions to US sanctions increase delays and the cost of Iranian imports of medicine, medical equipment and related raw materials and deter potential suppliers that fear overstepping sanctions limits.

The statement adds that the Trump administration’s sanctions on Iran are “the most extensive coercive economic measures ever imposed on a country” and that, given the military escalation between the US and Iran earlier this year, a lack of sanctions relief in response to the Covid-19 outbreak may “shut down chances completely” of a diplomatic engagement with Iran.

Signatories called on the US government to

- Allow exports of coronavirus-related medical devices and equipment through the humanitarian exemption under General License 8, which would enable Iran’s central bank to facilitate the transactions without exposing European and other banks to US sanctions
- Issue “comfort letters” to reassure EU and other non-US banks already conducting enhanced due diligence (EDD) that they will not “run afoul of OFAC” if they are involved in humanitarian trade with Iran
- Clarify that countries holding significant amounts of Iranian money in escrow from waivers granted for purchases of Iranian oil may use those funds to pay for humanitarian exports to Iran
- Provide regular updates on the US-sponsored Swiss Humanitarian Trade Arrangement (SHTA) and relax its stringent reporting requirements, which pose “a significant disincentive” to participation
- Express support for humanitarian trade between Europe and Iran through the Instrument in Support of Trade Exchanges (INSTEX)
- Increase staffing and other resources at the US Treasury Department’s Office of Foreign Assets Control (OFAC) to speed up the issuance of licences to manufacturers and non-governmental organisations that respectively seek to supply healthcare items and aid to Iran

US ‘encourages’ firms to disclose sanctions compliance concerns linked to pandemic

The US Treasury Department’s Office of Foreign Assets Control (OFAC) stated on 20 April that it “encourages” financial institutions and other businesses affected by the Covid-19 pandemic to get in touch soon if they anticipate delays in meeting regulatory deadlines for responding to administrative subpoenas, submitting licence reports or filing blocking and rejection reports.

OFAC stated that if a firm temporarily reallocates sanctions compliance resources in response to the pandemic and does so in a manner consistent with its risk-based approach, OFAC will evaluate this as a factor in determining the “appropriate administrative response” to an apparent violation that may occur during this period.
US authorities reportedly transacted with OFAC-listed Russian Direct Investment Fund

The US State Department announced on 1 April that the United States purchased from Russia coronavirus-related medical supplies, including ventilators and personal protection equipment (PPE), following a phone call between US President Donald Trump and Russian President Vladimir Putin on 30 March.

Half the cost of the shipment was reportedly paid by the state-owned Russian Direct Investment Fund (RDIF), which was added to the US Treasury Department’s sectoral sanctions list in July 2015 over its ties to US-designated Russian state bank Vnesheconombank (VEB), the Wall Street Journal reported on 2 April.

The State Department confirmed the shipment was delivered to the Federal Emergency Management Agency (FEMA) in New York City on 1 April.

MEPs call on the EU to maintain trade sanctions against Russia during the pandemic

Nineteen MEPs signed a 3 April letter calling on the EU’s representatives to “rebuff” any attempts to review or lift the bloc’s sanctions against the Russian Federation in response to the coronavirus pandemic.

The letter to EU Commission President Ursula von der Leyen, EU Council President Charles Michel and EU High Representative for Foreign Affairs Josep Borrell stresses that EU sanctions do not hinder Russian trade in medical supplies but rather limit its trade in arms, dual-use items and sensitive technology.

The cross-party lawmakers call on the EU’s leaders to ensure EU sanctions against Russia not only be maintained but “strictly linked” to the full implementation of the Minsk agreements for peace in Ukraine.

Aperio Analysis

The EU has been divided over Russian sanctions since their implementation, with some member states, such as Hungary, Slovakia, and the Czech Republic, opposing the sanctions for economic reasons and perhaps also due to their respective governments’ ideological or political affiliation to the Kremlin. However, the bloc would need serious reasons to lift the sanctions, as Russia’s aggression in Ukraine continues and lifting the restrictions could send the wrong message about the EU’s position regarding the sovereignty of post-Soviet states, some of which are now part of the Union. As the sanctions do not have a direct effect on Russia’s ability to tackle the Covid-19 outbreak, they are likely to remain in place. However, the Russian economy and healthcare system are not prepared to tackle a pandemic of this scale. Additionally, in response to the EU sanctions, Russia has introduced its own restrictions including a ban on the import of certain goods from EU members states. If Russia becomes unable to compensate for imports through domestic production, this could have serious economic, political and social implications, exacerbated by the pandemic.
OECD to issue guidance on combatting foreign bribery during pandemic

The Organisation for Economic Cooperation and Development’s (OECD) Working Group on Bribery announced on 22 April plans to examine the possible impact of the Covid-19 pandemic on foreign bribery and to identify “solutions” for strengthening national anti-bribery systems.

The group warned that many of the detected cases of foreign bribery have occurred in the health sector and called on all countries to ensure transparency, integrity of public procurement and protection for whistleblowers and journalists to help counteract corruption, particularly that which could undermine responses to the pandemic.

FBI issues warning over money mule schemes exploiting Covid-19 pandemic

The US Federal Bureau of Investigation (FBI) issued a warning on 6 April about criminals taking advantage of the uncertainty and fear surrounding the Covid-19 pandemic to steal money, access personal and financial information, and use victims as money mules to move or hide illicitly obtained funds through “transfers, physical movement of cash, or through various other methods”.

The FBI highlighted the following schemes in which criminals may attempt to get individuals to send or receive money on behalf of others who they are not personally and professionally responsible for: work-from-home schemes where online job postings and emails from individuals promise easy money for little to no effort; and individuals claiming to be located overseas asking to send or receive money on their behalf.
EBA’s Covid-19 supervisory statement stresses the need to prevent cybercrime

The European Banking Authority (EBA) issued a statement on 22 April on additional supervisory measures during the Covid-19 pandemic, which calls on financial institutions to ensure digital operational resilience, adequate ICT capacity and the security of their online services to better prevent cybercrime.

In its statement, the EBA highlights the importance of operational resilience in preventing both cybercrime and disruptions caused by malign actors targeting remote workers and businesses. In addition, financial institutions and supervisors are expected to ensure effective crisis communication measures with internal and external stakeholders regarding potential cybercrime activities.

The EBA reminds financial institutions that its guidelines on ICT and security risk management, issued on 28 November 2019, will become effective on 30 June. Under the guidelines, EU credit institutions, investment firms and payment services providers need to ensure appropriate ICT and security risk management. The EBA also calls on competent authorities to cooperate with their supervised institutions in prioritising ICT related activities and business continuity management.

Reserve Bank of India requires regulated entities to periodically review ML/TF risk assessments

The Reserve Bank of India (RBI) wrote a letter to all regulated entities on 20 April informing them that a new section has been added to the Master Direction (MD) on KYC requiring all regulated entities to conduct money laundering (ML) and terrorist financing (TF) risk assessments periodically.

The RBI highlights that the internal risk assessment carried out by regulated entities should be commensurate to the size, geographical presence, and the complexity of the activities and/or structure of the business. Furthermore, the risks identified should be mitigated and managed through a risk-based approach, which includes policies, controls and procedures approved by the Board.

Regulated entities are expected to complete their first internal risk assessment following the amendment by 30 June, which should be reviewed periodically thereafter.
US FinCEN updates institutions on Bank Secrecy Act reporting obligations during Covid-19

The US Treasury Department’s Financial Crimes Enforcement Network (FinCEN) provided on 3 April additional information to financial institutions on meeting their Bank Secrecy Act (BSA) obligations during the Covid-19 pandemic. FinCEN has set out its expectations that obliged entities should continue to abide by the anti-money laundering and countering the financing of terrorism (AML/CFT) requirements and ensure risk-based compliance during the coronavirus outbreak.

FinCEN acknowledges the ongoing challenges in meeting certain BSA obligations and reporting deadlines, and recognises that there may be some reasonable delays. Financial institutions are encouraged to contact their regulator regarding any potential BSA compliance concerns caused by the Covid-19 pandemic.

Key measures

- Implementation of the new FinCEN ruling of 10 February on currency transaction report (CTR) filing obligations for sole proprietorships and legal entities operating under a “doing business as” (DBA) name is suspended until further notice
- Paycheck Protection Programme (PPP) eligible financial institutions under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) of 27 March will not be required to carry out re-verification of existing customers in line with the BSA requirements, unless otherwise indicated
- FinCEN reminds financial institutions of the existing legal exceptions to beneficial ownership requirements for non-PPP loans
- FinCEN will continue to assess the BSA obligations and will issue further information, once the CARES Act has been implemented
- FinCEN advises financial institutions to remain alert to malicious or fraudulent transactions, in line with its 2017 advisory regarding disaster-related fraud
- FinCEN reminds institutions of its 16 March advisory, which alerted financial institutions to investment scams and insider trading

Global Witness warns of possible tax fraud and gold smuggling via DRC gold refinery

On 23 April, Global Witness announced that its investigation into Congo Gold Raffinerie (CGR) determined that the DRC-based gold refinery has an “invalid” processing licence and may be a front for obtaining tax breaks and legitimising exports of untraceable, semi-refined gold.

The anti-corruption advocacy group also claimed its investigation uncovered evidence that CGR is owned by “opaque” offshore entities and is linked to alleged gold smuggler Karim Somji and former DRC president Joseph Kabila.
Turkish FIU issues new AML reporting rules

The Turkish Banking Association (TBB) announced on 14 April that the Financial Crimes Investigation Board (MASAK) has introduced new measures to combat money laundering and terrorist financing (ML/TF), in line with the Financial Action Task Force (FATF) recommendations to better address key financial crime risks, particularly in connection with Covid-19 related fraud and cybercrime.

Under the new rules, regulated entities in the Turkish financial sector are required to report payments between TRY 100,000 (£11,590) and TRY 1 million (£115,900) or its equivalent in foreign currency to MASAK’s online system on the day the transaction is made. In addition, payments above that threshold will need to be reported to MASAK one day before actual processing.

Corporate transactions and payments between financial institutions are currently excluded from the new reporting requirements. In its latest mutual evaluation report on Turkey, published on 16 December 2019, FATF recommended that Turkey improve the implementation of sanctions related to terrorism and foster the development of a more thorough understanding of TF risks in the banking sector.

Portuguese court seizes NOS shares indirectly owned by Angola’s Isabel dos Santos

Portugal-based Sonaecom SGPS SA, which holds half of ZOPT SGPS SA’s share capital, announced on 4 April that a Lisbon court has ordered the seizure of half of ZOPT’s 52 percent shareholding in NOS SGPS SA, which is indirectly owned by two companies controlled by Isabel dos Santos, Unitel International Holdings BV and Kento Holding Ltd.

Unitel and Kento reportedly denounced the court’s preventative seizure of their indirect holding of 26 percent of NOS’ share capital as “abusive” efforts by the Angolan state to seize funds allegedly stolen by dos Santos, who is wanted by Angolan authorities on suspicion of money laundering, Jornal Economico reported on 5 April.

On 22 January, Angolan prosecutors accused dos Santos, the daughter of Angola’s ex-president, of conspiring to embezzle $1 billion from state oil firm Sonangolduring her time as chairperson between June 2016 to November 2017, the BBC reported. An Angolan court froze the assets of dos Santos, her husband Sindika Dokolo and Banco de Fomento Angola’s Chairman Mário Leite da Silva on 23 December for allegedly causing more than $1 billion in state losses.
UK’s FIU issues guidance on Covid-19 red flags of fraud and money laundering

The UK’s National Crime Agency (NCA) published on 30 April guidance from the financial intelligence unit (UKFIU) on trends and developments in fraud and money laundering linked to the Covid-19 pandemic.

The guidance, which draws on suspicious activity reports (SARs) received, states that the pandemic is being exploited to further facilitate existing fraud methodologies and to account for unusual cash deposits and money movements indicative of possible money laundering.

Examples of suspected fraud include:

- Sudden movement of funds from an individual savings account, possibly to fraudulently claim government compensation for Covid-19 loss of earnings
- Individuals or businesses taking payment for, but not supplying, personal protective equipment (PPE)
- Refunds claimed for fake bookings cancelled due to Covid-19

EU calls on every country to combat malicious cyber actors operating from within its borders

The EU’s High Representative Josep Borrell issued a declaration on behalf of the European Union on 30 April, condemning the malicious cyber activities being targeted at operators of essential services during the Covid-19 pandemic, which includes significant phishing, malware and distributed denial-of-service (DDoS) attacks being directed at healthcare providers and operators of critical infrastructure.

The EU requests that every country exercise due diligence and takes appropriate action against all malicious actors conducting activities from its territory, consistent with international law and the reports of the United Nations Groups of Governmental Experts (UNGGEs) on Information and Telecommunications in the Context of International Security.

The declaration explains that in view of the situation, the European Union and its member states will reinforce their cooperation to respond to malicious cyber activities.
UK’s FCA issues six-month extension to strong customer authentication deadline

The UK’s Financial Conduct Authority (FCA) announced on 30 April that it is extending until 14 September 2021 the deadline for implementing strong customer authentication (SCA) for e-commerce, citing the “exceptional circumstances” of Covid-19.

The six-month extension of the 14 March 2021 deadline allows firms more time to comply with the revised detailed phased implementation plan and critical path, which is being coordinated by trade association UK Finance, and to continue preparatory activities such as end-to-end testing.

EU Council adopts conclusions on South Sudan, warns further sanctions might be imposed

The Council of the European Union adopted on 30 April conclusions on South Sudan, which states that the “EU stands ready to adopt further restrictive measures” if the peace process in the country is undermined or the widespread violations of human rights continue. The conclusions also call on the UN Security Council to renew and enforce the arms embargo to ensure current security arrangements are being observed.

The EU Council expects the new South Sudanese government to ensure greater accountability and transparency, fight corruption, adhere to international financial standards and develop a comprehensive framework on future international cooperation.

The EU warned of further "restrictive measures" against South Sudan in case of continuing human rights violations.

The conclusions indicate that the EU strongly supports the setting up of transitional justice institutions and encourage the government to take the lead in establishing the Hybrid Court for South Sudan to help end the culture of impunity.

The conclusions welcome the formation of South Sudan’s Revitalised Transitional Government of National Unity as a crucial step towards long-lasting peace and stress the importance of holding free general elections and the respect for the rights of journalists, civil society and humanitarian workers.
EU anti-fraud agency recommends penalties against MEPs over ‘financial irregularities’

The European Anti-Fraud Office (OLAF) announced on 30 April that lawmakers from two EU member states breached European Parliament rules by transferring approximately €1.2 million from their EU salaries and allowances to their national parties between 2014 and 2019.

OLAF recommended that the European Parliament introduce “appropriate sanctions” such as disciplinary action and recovery of funds from the MEPs involved in these “financial irregularities”.

UN experts call for lifting of US sanctions on Cuba to help combat the pandemic

In a joint statement published on 30 April, UN human rights experts called on the US to lift the economic sanctions and financial embargo on Cuba, which is obstructing the humanitarian response to the Covid-19 pandemic in the country.

The joint statement explains that the US embargo on Cuba and the US sanctions on other countries seriously undermine international cooperation to combat the pandemic and provide humanitarian support. The UN experts note that the US government’s “lack of will” to suspend sanctions may lead to a higher risk of such suffering in those countries targeted by its sanctions.

More specifically, the UN experts claim that the US embargo has created a “cumbersome and expensive licensing process” for the export and re-export of goods to Cuba, which hinders the purchase of medical supplies. Despite updates to the Department of the Treasury’s Office of Foreign Assets Control (OFAC) Fact Sheet on 16 April, which provides guidance on humanitarian exemptions, the procedures have not been eased, reads the statement.
LEGISLATION

UK Treasury introduces Brexit financial services regulations, amends AML regulations

The UK Treasury laid before Parliament on 21 April the Financial Services (Miscellaneous Amendments) (EU Exit) Regulations 2020, which address "failures" of retained EU law to operate effectively and other "deficiencies" arising from the UK’s withdrawal from the European Union.

The draft regulations include several amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 that would come into effect on 31 December.

The Treasury stated in an explanatory note that it has not conducted a full impact assessment on the draft regulations as "no, or no significant, impact on the private, voluntary or public sector is foreseen".

The UK Money Laundering and Terrorist Financing (Amendment) Regulations 2019, which came in force on 10 January, updated the Money Laundering Regulations 2017 in line with the EU’s Fifth Money Laundering Directive (SMLD) and Financial Action Task Force (FATF) standards.

EU financial groups call for deferral of cross-border tax reporting obligations under DAC6

The European Banking Federation (EBF) and a group of nine other banking and insurance associations sent a letter to the European Commissioner for Economy Paolo Gentiloni on 20 April requesting that the deadline for the mandatory disclosure obligations under the revised cross-border tax directive (Directive on Administrative Cooperation, known as DAC6) is extended until 1 July 2021 due to a series of significant challenges, including the Covid-19 pandemic. DAC6 is due to come into force on 1 July 2020 as part of efforts to increase tax transparency and counter tax avoidance and evasion.

The letter cites enactment delays by some member states, the lack of detailed guidance on DAC6 implementation, as well as the impact of the coronavirus pandemic on the development of the required reporting software. According to the letter, the EU-wide deferral of domestic reporting requirements to July 2021 would give financial institutions more time to introduce new disclosure processes once workforce levels and IT capacity have been restored. The signatories also ask for an extension of the retrospective reporting deadline of 31 August and a further review of the DAC6 implementation status at the end of September.

Under the DAC6 2018 amendments, all EU intermediaries, including accountants, advisers, lawyers and banks, that sell reportable cross-border tax arrangements to their clients and "relevant" taxpayers will need to report information on these arrangements in their home member state.
UK export control unit revises application and remote compliance measures during Covid-19

The UK’s Export Control Joint Unit (ECJU) announced on 9 April interim arrangements for licence applications during the coronavirus pandemic to allow businesses more time to respond to requests for further information (RFIs) and to enable them to submit the required information, documentation and signatures electronically.

The ECJU separately announced on 9 April that it had revised its remote compliance measures to allow businesses exporting controlled items to submit digital copies of consignee undertakings and applications for Ministry of Defence (MOD) authorisation.

The notice also states that, ahead of their remote compliance assessment, businesses should complete a pre-visit questionnaire and itemise their licensable exports from the preceding two years.

UK's HMRC issues amended export guidance for personal protective equipment

The UK's HM Revenue and Customs (HMRC) published on 28 April updated guidance on exporting personal protective equipment (PPE) during the coronavirus pandemic, to reflect the revised EU regulations.

The UK guidance clarifies that economic operators will temporarily need a licence to export PPE outside the EU, European Free Trade Association (EFTA) member states and certain other territories and sets out the export control process. In cases where the proposed export is a humanitarian emergency, the Department of Health and Social Care (DHSC) will issue an export licence. In any other situations, DHSC will consider whether the shipment poses any threat to PPE availability in the EU and whether it satisfies a legitimate need for medical use in the destination country.

On 23 April, the European Commission (EC) adopted a revised implementing regulation on PPE export control, which reduces the number of controlled items, adds a PPE export control exemption regarding Western Balkans countries, and includes the possibility to process export control procedures in an expedited manner. The EC regulation entered into force on 26 April.
US BIS amends technology export controls in relation to China, Russia and Venezuela

The US Department of Commerce’s Bureau of Industry and Security (BIS) published on 27 April two final rules and one proposed rule amending the US export regulations to prevent attempts by Russia, China and Venezuela to obtain US technology that could be used in the development of weapons, military aircraft or surveillance technology.

Through the adoption of the two final rules, BIS has eliminated certain licence exceptions and added new controlled items in the field of telecommunications, aerospace, information security, semiconductors, sensors and lasers in relation to the three countries. Taking effect on 29 June, the new rules impose an additional requirement on companies to file declarations for all US exports to the destination countries irrespective of the value of the shipment.

Key actions

- The expansion of military end use and military end user (MEU) licence requirement controls on China, Russia and Venezuela by including exports to MEUs in China, amending the MEU definition and adding 17 new export control classification numbers
- The removal of a licence exception for exports, reexports, or transfers (in-country) to civilian end users (CIV) in the three countries
- A BIS proposal to amend the Export Administration Regulations (EAR) by eliminating certain provisions of the Licence Exception Additional Permissive Reexports (APR), which remains open for consultation until 29 June

US government to review national security-controlled exports to certain countries

The US Commerce Department’s Bureau of Industry and Security (BIS) issued on 28 April a final rule removing the licence exception for civil end users (CIV) and requiring businesses to obtain from 29 June a licence to export national security-controlled items in the Commerce Control List (CCL) to “countries of national security concern”.

The amendment to the Export Administration Regulations (EAR), which allows the US government to review such transactions prior to export, reexport or in-country transfer, is due to the “increasing integration” of civilian and military technology development in countries of concern, which makes it “more difficult” for industry to assess whether or not items are intended for military use.
US Treasury issues General License 8F on transactions with Venezuela’s PDVSA

The US Treasury Department’s Office of Foreign Assets Control (OFAC) issued on 21 April General License 8F, which supersedes General License 8E and imposes narrower restrictions on five companies’ transactions with US-designated Petróleos de Venezuela SA (PDVSA).

General License 8F narrows the previous licence’s exemptions under the Venezuela Sanctions Regulations and stipulates that these cover transactions and activities that are ordinarily incident and necessary to the “limited” maintenance of certain “essential” operations, contracts or other agreements in Venezuela.

It also stipulates that the exemptions only cover such transactions and activities that:

- Are for safety or the preservation of assets in Venezuela;
- Involve PDVSA or any entity in which PDVSA owns a 50 percent or greater interest; and
- Were in effect prior to 26 July 2019 and authorised until 1 December 2020

The general licence covers the following entities and their subsidiaries:

- Chevron Corporation
- Halliburton
- Schlumberger Ltd
- Baker Hughes, a GE Company
- Weatherford International PLC

OFAC issues Venezuela-related General License on PDVSA bonds

The US Treasury Department’s Office of Foreign Assets Control (OFAC) issued on 10 April General License (GL) 5C “Authorising certain transactions related to Petróleos de Venezuela, S.A. (PDVSA) 2020 8.5 percent bond on or after July 22, 2020” and amended Frequently Asked Question (FAQ) 595.

GL 5C has been issued pursuant to Executive Order (EO) 13835 of 21 May 2018, as amended by EO 13857 of 25 January 2019, and authorises all transactions related to, the provision of financing for, and other dealings in the PDVSA 2020 8.5 percent bond, on or after 22 July.

According to amended FAQ 595, between 24 October 2019 and 22 July 2020, there is no effective authorisation in place and transactions related to the sale or transfer of Citgo (a PDVSA subsidiary) shares in connection with the PDVSA 2020 8.5 percent bond remain prohibited, unless specifically authorised by OFAC.
US Treasury extends general licence for Nynas AB amid plan to end Venezuelan ownership

The US Treasury Department’s Office of Foreign Assets Control (OFAC) announced on 3 April the extension until 14 May of the general licence that authorises transactions with Sweden-based Nynas AB, which is undergoing a restructuring to terminate its ties with US-sanctioned Venezuelan oil firm PDVSA.

OFAC has confirmed that it is ready to “swiftly initiate its internal process for the removal of sanctions applicable to Nynas” when the proposed reorganisation is executed, according to a 12 March statement from Nynas.

Nynas published on 21 January a preliminary plan to change its ownership after US sanctions against PDVSA, whose subsidiary PDV Europa owns a 50.001 percent stake in Nynas, resulted in the firm filing for reorganisation on 13 December.

European Commission confirms new export authorisation scheme for PPE

The European Commission confirmed on 24 April a new scheme for authorising exports of personal protective equipment (PPE) under Implementing Regulation (EU) 2020/568, which comes into force on 26 April and applies for 30 days.

On 14 April, the EU’s executive body proposed a partial renewal of export restrictions introduced on 15 March to ensure the adequate supply of medical products in the European Union during the Covid-19 pandemic.

The new scheme

- Reduces the list of products that require export authorisation to masks, spectacles and protective garments
- Extends the geographical exception to the Western Balkans
- Requires member states to swiftly authorise exports for humanitarian purposes
- Includes measures to ensure transparency and consistency of member states’ decisions to grant or reject export authorisation requests
US updates exemptions on personal protective equipment export restrictions

The US Federal Emergency Management Agency (FEMA) filed a notice of exemptions on 17 April that amends rules on export controls of personal protective equipment (PPE) during the Covid-19 pandemic, clarifying and allowing some leniency for PPE exports in certain situations, predominantly where PPE is being shipped to US persons or businesses overseas.

The new exemptions outlined in the notice:
- Shipments to US commonwealths and territories (e.g. Puerto Rico and US Virgin Islands), Canada and Mexico (where these are the final destinations), and to overseas US military, foreign service posts and embassies
- Donations of PPE by not-for-profit or non-governmental organisations to foreign governments or charities
- Intra-company transfers by US companies from domestic facilities to company-owned or affiliated foreign facilities
- Materials exported solely for assembly in medical kits destined for US sale and delivery
- Sealed, sterile medical and diagnostic testing kits where only a portion of the kit is covered by PPE export restrictions
- Diplomatic shipments from foreign embassies and consulates to their home countries
- In transit merchandise, with a foreign shipper and consignee
- Shipments by or on behalf of the US government, including the military

US agency implements export restrictions on medical equipment to counteract Covid-19

The US Homeland Security Department’s Federal Emergency Management Agency (FEMA) filed on 7 April a temporary final rule establishing from 10 April export restrictions on personal protective equipment (PPE) for 120 days in response to the Covid-19 pandemic.

The rule implements President Donald Trump’s memorandum of 3 April requiring the allocation of scarce medical resources for domestic use, in line with Executive Orders 13909, 13910 and 13911.

Under the rule, US Customs and Border Protection (CBP) will temporarily detain all shipments of covered materials until FEMA determines whether to permit the exports in part or full, purchase the items, or allocate them for domestic use.
Germany Federal Ministry of Justice publishes revised draft corporate sanctions bill

The German Federal Ministry of Justice (BMJV) officially published its revised draft corporate sanctions bill on 22 April, which aims to strengthen the legal provisions around corporate crimes. The new bill aims to allow for corporate crimes in Germany to be prosecuted as a criminal offence rather than a mere “administrative offence”.

Despite these tougher sanctions, the law adopts a preventive approach by creating incentives for companies to implement and follow compliance measures, with companies potentially being able to avert a sanction or reduce the fine if they cooperate with the authorities.

This corporate sanctions bill is an updated version of a previous bill, published “unofficially” by the BMJV in August 2019, which would have granted German courts the power to dissolve a company in “particularly severe cases” – though this power has been removed in the latest iteration of the bill.

Armenian lawmakers adopt new law to introduce unexplained wealth orders

Armenian lawmakers adopt new law to introduce unexplained wealth orders

Armenia’s Parliament adopted on 16 April a law that would allow prosecutors to obtain unexplained wealth orders for property worth more than AMD 25 million (£42,000) that is suspected of having been acquired with illicit funds since 1991.

The draft law, which was adopted in full at its second reading, states that property of illegal origin acquired by a third party is not subject to confiscation if the current owner did not know about the illicit origins and used legal income to obtain the property.
OFAC issues amended North Korea Sanctions Regulations


The changes brought in by the new amendments include the incorporation of blocking and correspondent account sanctions provisions and a new prohibition “applicable for persons that are owned or controlled by a US financial institution” overseas as well as a series of related exemptions. In addition, the definition of luxury goods has been amended, and several other definitions have been edited and an interpretive provision has been revised.

The North Korea Sanctions Regulations were issued on 4 November 2010 and have been amended several times. The latest set of amended Regulations took effect on 10 April.

OFAC adjusts monetary penalties for inflation

The US Department of the Treasury’s Office of Foreign Assets Control (OFAC) published on 8 April a final rule adjusting the maximum amount for civil monetary penalties (CMPs) according to inflation, pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990 (FCPIA Act), as amended by the 1996 Debt Collection Improvement Act and the 2015 Federal Civil Penalties Inflation Adjustment Act Improvements Act.

Each federal agency with statutory authority to assess CMPs is required under Section 4 of the amended FCPIA Act to adjust CMPs annually for inflation according to a formula provided in Section 5 of the FCPIA Act, in order to ensure the “deterrent effect” of CMPs.

US continues South Sudan national emergency

US President Donald Trump announced on 1 April the renewal for one year of the national emergency in relation to South Sudan. The South Sudan sanctions were declared on 3 April 2014, by Executive Order (EO) 13664, pursuant to the International Emergency Economic Powers Act (IEEPA), in view of the activities undermining the peace and stability of South Sudan and the region.

According to the US President’s letter to the Speaker of the House of Representatives and the President of the Senate, the situation in South Sudan, which has been marked by “widespread violence and atrocities, human rights abuses, recruitment and use of child soldiers, attacks on peacekeepers and obstruction of humanitarian operations” continue to pose “an unusual and extraordinary threat” to the US.

South Sudan and the region.

White House notice

US President’s letter
EU renews Myanmar sanctions regime

The EU Council adopted on 23 April a decision extending the restrictive measures against Myanmar until 30 April 2021. The EU Council also updated one entry on the list of 14 persons and entities designated over human right abuses.

The restrictive measures on Myanmar, which include an arms embargo and an embargo on equipment that might be used for internal repression, were imposed on 22 April 2013, when the wider set of measures of 28 October 1996 were lifted. The sanctions regime was strengthened on 25 June 2018, when the EU imposed additional measures targeting senior officers from the Myanmar Armed Forces (Tatmadaw) and the Border Guard Police responsible for systematic human rights abuses, in particular in Kachin, Rakhine and Shan states.

EU aligns Yemen sanctions regulations with UN

The EU Council adopted on 2 April a decision updating its restrictive measures to put into effect the amendments included in UN Security Council (UNSC) resolution 2511 regarding the granting of case-by-case sanctions exemptions for UN humanitarian workers in Yemen.

In implementing the amendments, the EU Council has decided that each EU member state will authorise the provision of technical or financial assistance and the release of certain frozen funds or economic resources, agreed by the UNSC Yemen Sanctions Committee “to facilitate the work of the UN and other humanitarian organisations in Yemen or for any other purpose consistent with the objectives of those resolutions”.

The Council decision includes an additional amendment to include sexual violence in armed conflict and the recruitment or use of children among the sanctionable human rights abuses under the international humanitarian law.

US to impose visa bans on countries that delay repatriation of foreign nationals

US President Donald Trump issued a memo on 10 April authorising the State Department to impose visa bans on individuals from countries whose governments deny or “unreasonably delay” the repatriation of foreign nationals who violate US laws.

The memo, which cites the national emergency Trump declared on 13 March in response to the coronavirus pandemic, adds that sanctions may be repealed if the Homeland Security Department determines a jurisdiction has resumed accepting its citizens without unreasonable delay.

---

Council Decision 2020/563
Council Implementing Regu...
Council Decision 2018/900...
EU Council Decision 2020/...
EU Council Regulation 202...
UN Security Council resol...
White House memo
Proclamation 9994
US president extends national emergency with respect to Somalia

The US President announced on 3 April the renewal for one year of the national emergency with respect to Somalia, which was declared on 12 April 2010 by Executive Order (EO) 13536, pursuant to the International Emergency Economic Powers Act (IEEPA).

The national emergency was issued to deal with the deterioration of the security situation and the violence in Somalia, acts of piracy and armed robbery off the coast of Somalia, as well as violations of the arms embargo imposed by the UN Security Council. To deal with that emergency, additional steps were taken in 2012 through the adoption of EO 13620, which addressed the illicit export of charcoal, the misappropriation of Somali public assets and acts of violence against civilians in Somalia.

In the accompanying letter to Congress, US President Donald Trump said that the US “is strongly committed to Somalia’s stabilization, and it is important to maintain sanctions against persons undermining its stability. The situation with respect to Somalia continues to pose an unusual and extraordinary threat to the national security and foreign policy of the United States”.

EU extends Iran human rights sanctions

The EU Council renewed on 7 April the restrictive measures in response to serious human rights violations in Iran until 13 April 2021 and updated the information regarding 82 designated former or current government officials and members of the judiciary.

The measures were first adopted on 12 April 2011 and consist of an asset freeze and a travel ban with respect to individuals responsible for directing the repression of peaceful demonstrators, journalists or human rights defenders, or individuals involved in serious violations of the right to due process, torture or the “the indiscriminate, excessive and increasing application of the death penalty”.

On 23 March 2012, in view of the ongoing human rights abuses in Iran, EU member states were also prohibited from exporting equipment or software to Iran which might be used for internal repression or for telecommunications monitoring or interception. Providing related technical or financial assistance and services to Iran is also banned. The Iran human rights sanctions were last extended on 8 April 2019.
US Congress votes to create subcommittee to track $2 trillion Covid-19 relief funds

The US Congress passed a resolution on 23 April to formally establish a new select subcommittee to track the $2 trillion in aid administered during the Covid-19 pandemic. House Speaker Nancy Pelosi delivered a statement in support of the new Select Subcommittee on the Coronavirus Crisis which will sit within the Committee on Oversight and Reform, to guard against fraud, waste and abuse, and examine the US Government’s response to the crisis.

The subcommittee will be tasked with reviewing:

- The efficiency, effectiveness and transparency of taxpayer funds and relief programmes to address the coronavirus crisis
- Reports of abusive practices related to the crisis
- The protection of whistleblowers

- Executive branch “policies, deliberations, decisions, activities, and internal and external communications” related to the Covid-19 pandemic

House resolution 935
House Committee speech
LITIGATION

**EY ordered to pay $11 million to whistleblower related to suppression of gold audit**

The UK High Court ordered on 17 April accountancy firm EY, formerly known as Ernst & Young, to pay $11 million in damages to former partner turned whistleblower, Amjad Rihan, who leaked documents showing that the firm covered up evidence of money laundering during an audit of Dubai’s biggest gold refiner – Kaloti Jewellery International – in 2013.

Justice Kerr ruled that EY had helped cover up the results of an audit of Kaloti’s business practices undertaken by Rihan, which found that Kaloti paid “billions of dollars in cash” for gold without verifying its origin in addition to buying gold bars from Morocco that were then coated in silver in order to bypass export restrictions. The audit also identified transactions with high-risk countries such as Sudan, DRC and Iran without proper due diligence having been carried out.

The High Court found EY had suppressed evidence of money laundering during its audit of Dubai’s largest gold refiner.

The High Court held that instead of reporting the audit findings or terminating its engagement with Kaloti, EY agreed measures designed to obscure the audit findings, and were responsible for suggesting to Kaloti that the audit reports be drafted in such a way as to obscure the reality of the Moroccan gold and the cash transactions. The Court found that by colluding in its efforts to conceal the findings of the Kaloti audit, EY had breached its professional duties under the Code of Ethics for Professional Accountants.

Rihan, who resigned in 2014, brought legal proceedings against four UK-based companies within the EY Network over claims that he was forced out of his job when he blew the whistle on the misconduct concerning the Kaloti audit. The court awarded Rihan a total of $10,843,941 and €117,950 in damages for past and future loss of earnings and loss of employment benefits.

**UK High Court ruling**

---

**Vijay Mallya loses UK appeal against extradition to India over alleged bank fraud**

The UK High Court dismissed on 20 April Vijay Mallya’s appeal against his extradition to India on fraud and money laundering charges.

The Indian government filed in 2017 an extradition request for Mallya, who may appeal the Court’s decision at the UK Supreme Court.

The former CEO of Kingfisher Airways is accused of fraudulently obtaining approximately £266 million in loans from six banks in 2009 and then laundering some of the proceeds.

Vijay Mallya reportedly filed an application on 4 May for the UK Supreme Court to prevent his extradition to India on fraud and money laundering charges after the UK High Court dismissed his appeal on 20 April, the Statesman reported on 5 May.

**High Court judgement**

**Statesman story**
Kazakh family wins challenge against three unexplained wealth orders in London court

The UK High Court Queen's Bench Division ruled on 8 April to overturn three unexplained wealth orders (UWOs), issued by the National Crime Agency (NCA) in May 2019, in relation to London properties worth more than £80 million, linked to the daughter and grandson of the former president of Kazakhstan Nursultan Nazarbayev.

In its UWOs, the NCA sought information from Dariga Nazarbayeva and her son Nurali Aliyev about how they funded the purchases of the three properties alleging that they were bought “as a means of laundering the proceeds of unlawful conduct by Rakhat Aliyev (RA)”, Nazarbayeva’s husband between 1983 and 2007 and Nurali’s father, who died in an Austrian prison on 24 February 2015 awaiting trial on murder charges. In deciding to discharge the UWOs, the judge found that there was “cogent” evidence that Nazarbayeva and Nurali Aliyev founded the three companies that own the London properties and are the ultimate beneficial owners (UBOs) of all of the properties.

In addition, the NCA’s assumption that RA was the source of the funds was “unreliable” and the NCA’s case was “flawed by inadequate investigation into some obvious lines of enquiry” and “failed to carry out a fair-minded evaluation of the new information provided by the UBOs”, in particular “in relation to the evidence of purchase on behalf of the UBOs, the absence of any link between RA and the three foundations”.

The Court said the NCA’s case was “flawed by inadequate investigation into some obvious lines of enquiry”

The NCA announced that it will be appealing against the judgment. The Director of the NCA’s National Economic Crime Centre Graeme Biggar said that UWOs are “new legislation and we always expected there would be significant legal challenge over their use”. He added that: “The NCA is tenacious. We have been very clear that we will use all the legislation at our disposal to pursue suspected illicit finance and we will continue to do so”.

NCA press release
London High Court ruling

Aperio Analysis

This latest case illustrates the inherent limitations of UWO legislation, relying as it does on links to serious crime (prior to his death, Nurali Aliyev’s father Rakhat Aliyev was accused of kidnapping and attempted murder – charges he denied as politically-motivated). The respondents successfully argued that the funds used to purchase the properties were not directly derived from Rakhat Aliyev. Yet both Nurali Aliyev and his mother Dariga Nazarbayeva, daughter of former president Nazarbayev and ex-wife of Rakhat Aliyev, have derived substantial financial benefits from their positions in the post-Soviet political regime. According to the Organised Crime and Corruption Reporting Project (OCCRP), in 2013 Nurali Aliyev disappeared permanently from the Forbes rich list, maybe due to then-president Nazarbayev’s displeasure over “the shocking display of wealth by a state official”. Despite the setback suffered by the NCA (subject to possible reversal on appeal), the case does however show the willingness of British authorities to crack down on purported money laundering even when it implicates representatives of ruling foreign elites, including from countries that maintain friendly relations with the UK. Dariga Nazarbayeva’s sudden dismissal from her role as speaker of the Kazakh Senate on 2 May also illustrates the ongoing risks to reputation created by UWOs.
Canadian mining company Teck Resources faces Cuban trafficking lawsuit in the US

The heirs of the former owner of a Cuban mining company, Roberto Gomez Cabrera, is suing Canada’s Teck Resources Ltd in the US District Court of the Southern District of Florida according to a court filing dated 17 April for “unauthorised mining activities and extraction of valuable minerals” from mines nationalised by Fidel Castro’s government. The complaint has been filed pursuant to the US Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996 otherwise known as the Helms-Burton Act by Herederos De Roberto Gomez Cabrera LLC.

The defendant claims that Cabrera’s company, Minera Rogoca SA, explored and mined several rich ore and mineral mines in the El Cobre, Sierra Maestra region of Cuba until the communist Cuban government took their property in 1960. After engaging in a joint venture to explore and develop significant land holdings in Cuba, Teck and another Canadian corporation, Joutel Resources Ltd agreed in 1996 to engage in mining activities with Cuban state-owned entity Geominera SA.

According to the plaintiffs, Teck Resources “knowingly and intentionally” commenced, conducted and used the confiscated property for commercial purposes, as well as profited from the Cuban government’s possessions of the property without the authorisation of Cabrera and his company.

The plaintiffs have demanded a jury trial and requested all recoverable compensatory, statutory, and other damages, as well as equitable relief and damages allowable under the applicable law.

Bitcoin transfers provide basis for federal jurisdiction in money laundering conviction

The US Ninth Circuit Court of Appeals upheld the money laundering conviction against Thomas Costanzo, a bitcoin broker convicted of money laundering in 2018, which was filed on 17 April, thereby finding that bitcoin transfers – even if they originate and are received in the same state – have a sufficient effect on interstate commerce to warrant a money laundering charge.

The key argument behind Costanzo’s appeal was that, since the bitcoin transfers at issue originated in and were received by individuals “physically located in Arizona”, they did not have the requisite effect on interstate commerce to support a money laundering charge. In rejecting this argument, the Court argued, first, that Costanzo advertised his peer-to-peer services on localbitcoins.com, a website based outside the US, and, second, that Costanzo transferred the bitcoin through a digital wallet that involved the use of the internet, which previous court rulings have suggested is “intimately related to interstate commerce”.

Court filing

Court of Appeals ruling
English High Court to hear PrivatBank’s fraud claim against former owners

The UK Supreme Court confirmed on 6 April that the English High Court has jurisdiction to hear PrivatBank’s $3 billion fraud and conspiracy case against its former owners, Igor Kolomoisky and Gennadiy Bogolyubov, and six English and BVI Bogolyubov companies, according to a 7 April statement from the Ukrainian lender.

PrivatBank separately announced on 3 April that it has filed a claim in a Cypriot court seeking $5.5 billion in damages from Kolomoisky and Bogolyubov, former executive Timur Novikov and Cypriot companies PrimeCap (Cyprus) Ltd and Duxton Holdings Ltd over their alleged involvement in a loan fraud and money laundering scheme between 2013 and 2016.

The combined amount claimed by PrivatBank against Kolomoisky and Bogolyubov in England, Cyprus, Israel and the US amounts to more than $10 billion.

PrivatBank press release ...
Press release (3 April)

Aperio Analysis

This new iteration in the PrivatBank saga may be a run-of-the-mill court event for the UK, but certainly carries a lot of significance for Ukraine where the key former beneficiary of PrivatBank, oligarch Igor Kolomoisky, is seen by many as the ‘power behind the throne’; which is currently occupied by the young and energetic President Vladimir Zelensky. Ukraine’s political scene has been dominated since its independence by a class of oligarchs who have invariably supported all successive administrations, creating massive conflicts of interest and stymieing efforts to combat grand political corruption. Besides a net gain (in case of recovery) or loss for the Ukrainian state budget, the outcome of the PrivatBank affair could be a turning point for the extent of oligarchic influence over Ukraine. In fact, in April 2019 a Ukrainian court supported Kolomoisky in recognising the 2016 nationalisation of PrivatBank as illegal. Parallel to London hearings, the Ukrainian parliament is debating a draft law whose purpose is to protect the state’s financial position from the likes of Kolomoisky in the case of nationalisation-related litigation.

CJEU rules Poland must suspend the activities of new judicial disciplinary board

The Court of Justice of the European Union (CJEU) issued a ruling on 8 April that Poland must immediately suspend the activities of the Disciplinary Chamber of the Supreme Court – the country’s new judicial disciplinary board – as it risks causing “serious and irreparable harm” to EU interests.

Case C-791/19 R was instigated by the European Commission, which brought the action before the CJEU over concerns that Poland’s new disciplinary regime does not guarantee independence and impartiality.

In response to the ruling, Poland’s Deputy Justice Minister, Sebastian Kaleta, tweeted that the CJEU had “no power” to “suspend [the] constitutional organs of any member states” and called the ruling a “usurping act violating Poland’s sovereignty”.

CJEU press statement
Poland’s Deputy Justice Minister

79
CONSULTATIONS

UK extends consultation on freeports

The UK's Department for International Trade (DIT) announced on 8 April that the consultation on the government’s plans to create up to 10 freeports across the UK as post-Brexit hubs for global trade and investment will be extended until 13 July.

According to the government, the extension will allow key stakeholders, such as ports, businesses and local government, more time to submit their views amid the Covid-19 pandemic.

The consultation, published on 10 February, includes the government’s proposals for developing a UK freeport model, which includes tax incentives. In response to the EU's concerns about the risk of illicit activity posed by freeports, the government stated in the consultation that it remains committed to tackling tax avoidance and evasion, aggressive tax planning and no-compliance and asks for the public’s views on what additional measures should be implemented.

The government will consider a further extension to the deadline in the event that businesses and communities are not able to fully engage with the consultation before 13 July.

Financial Stability Board launches consultation on managing global stablecoin risks

The Financial Stability Board published on 14 April proposals for G20 nations to manage the regulatory, supervisory and oversight risks posed by global stablecoin (GSC) arrangements such as Facebook’s ‘Libra’.

The public consultation on a common international approach to regulating and supervising the crypto-asset closes on 15 July; the final recommendations will be published in October.

The FSB recommends that GSC arrangements

- Comply with all applicable regulatory, supervisory and oversight requirements of each jurisdiction in which they seek to operate
- Have policies for managing the risks of money laundering, terrorist financing and cybercrime
- Disclose recovery avenues available to users who lose access to their wallet and private key due to a cyberattack or other operational incident
- Conduct due diligence on individuals involved in their management and control, as well as those who exercise significant power or discharge significant responsibilities in relation to the GSC's activities
- Provide users and stakeholders with “comprehensive and transparent” information on areas including governance arrangements, operation of the stabilisation mechanism and the investment mandate for reserve assets
FSB consults on cyber incident response and recovery toolkit for financial institutions

The Financial Stability Board (FSB) published on 20 April a consultation paper which proposes a toolkit of effective practices for cyber incident response and recovery (CIRR), aimed at assisting financial institutions in countering cybercrime and responding efficiently to cyber incidents, including malicious attacks and fraud.

The toolkit includes a series of options that organisations should consider depending on their specificities and the particular legislative, judicial and regulatory frameworks they operate in. The FSB also notes that national authorities may consider the toolkit in their interactions with financial institutions during their supervisory work. Governments can also play a role in responding to cyber incidents that might affect the stability of the financial system and in sharing information more widely to protect against threats.

The FSB invites comments on its report and on a series of additional questions, including the impact of the Covid-19 pandemic on companies’ cyber related activities, cyber incident analysis and the mitigation of data breaches and ransomware events. The consultation is open until 20 July and the final toolkit is due to be published in October.

FSB press release
FSB report summary
FSB report
PRESS AND MEDIA

Latvian anti-graft agency reportedly probing US Treasury allegations against Aivars Lembergs

Latvia’s Corruption Prevention Bureau (KNAB) has reportedly opened an inquiry into allegations by the US Treasury Department’s Office of Foreign Assets Control (OFAC) that Aivars Lembergs, formerly mayor of Ventspils, exploited and corrupted Latvian politicians and law enforcement officials, LETA reported on 22 April.

On 9 December, OFAC designated Lembergs and four Latvia-based entities he purportedly owned or controlled for allegedly misappropriating state assets, expropriating private assets for personal gain and engaging in corruption related to government contracts or the extraction of natural resources.

OFAC stated that Lembergs controls entities through political parties and “corrupt” politicians, and “systematically exploits” those entities and individuals for his own financial gain. OFAC also claimed that Lembergs used his influence over political party leaders to place certain government officials in key positions and also “leveraged and corrupted” law enforcement officials to protect his interests.

The Riga Regional Court has a longstanding case against Lembergs, who is being tried for alleged graft, money laundering, abuse of office and other crimes alongside his purported co-conspirators, his son Anrijs Lembergs and business partner Ansis Sormulis.

Brazil’s justice minister reportedly resigns over president’s alleged ‘interference’ in investigations

Brazil’s Justice Minister Sérgio Moro reportedly announced at a press conference that he is resigning due to “political interference” by President Jair Bolsono in replacing Federal Police chief Mauricio Valeixo, who was reportedly leading criminal investigations into Bolsonaro’s children, Reuters reported on 24 April.

Brazil’s Supreme Court subsequently approved a request by chief public prosecutor Augusto Aras to investigate the allegations of presidential interference in police probes, which may lead to corruption and identity fraud charges against Bolsono, who maintains his innocence, Bloomberg reported on 27 April.

Transparency International claimed in a statement dated 25 April that political interference in Brazilian oversight institutions has been a “consistent problem” in Bolsonaro’s government and called for society and institutions to “react firmly” to contain the “abuses of this government”.

Moro, a former judge, oversaw Brazil’s largest anti-corruption investigation, Lava Jato, which uncovered billions of dollars in bribes and resulted in convictions of dozens of businessmen and politicians, including former president Luiz Inacio Lula da Silva.
European Investment Bank to reportedly investigate whistleblower’s AML complaints

The European Investment Bank (EIB) has reportedly called for an inquiry into whistleblowing allegations that officials failed to comply with EU anti-money laundering (AML) rules by conducting adequate know-your-customer (KYC) checks before providing billions of euros in financing to projects around the world, according to internal records cited by the Luxembourg Times on 21 April.

A leaked email from the EIB’s former group chief compliance officer Gerhard Hütz to his team reportedly suggests that a combined €267 million in funding was given to Hungarian state-owned bus company Volán Buszpárt in January 2020 and a German motorway project in September 2019 without obtaining verification of documents. The bank reportedly confirmed that auditors identified “gaps” in its AML/CFT practices, partly related to an “incomplete adaptation” of its policies in line with the latest requirements under the EU’s Money Laundering Directive and the Financial Action Task Force’s (FATF) standards.

The EIB’s audit committee stated in an annual report published in July 2019 that implementation of the bank’s AML/CFT monitoring framework was “ongoing” and that it was “partially compliant” with requirements to conduct enhanced due diligence on politically exposed persons (PEPs).

Maltese banks unfreeze €12m belonging to Satabank clients suspected of wrongdoing

Maltese banks have reportedly released €12.1 million held by 25 Satabank clients subject to account freezing orders that expired without resultant prosecution, according to an EY report cited by the Times of Malta on 29 April.

Investigation and attachment orders were reportedly received for 54 Satabank customers that held €40 million in total in 2019.

The Malta Financial Services Authority (MFSA) appointed EY to manage Satabank’s assets and business in October 2018 after the lender’s licence was suspended.

As at the end of February, EY reportedly identified 570 suspicious transactions totalling €188.5 million that involved 999 Satabank customers who had sent and received €9.3 billion since opening their accounts.

Satabank is reportedly contesting an €3 million penalty imposed by the financial intelligence unit in July 2019 over alleged breaches of anti-money laundering (AML) rules.
Malta police reportedly accuse James Fenech of breaching EU sanctions against Libya

Malta police announced on 25 April charges against five men suspected of violating EU sanctions against Libya and laundering money. The men, who pleaded not guilty, were arrested after investigators received information that a Maltese registered company had exported two ships to Libya without licence authorisation.

Arms dealer James Fenech, who is reportedly among the accused, allegedly entered into a Libya transportation agreement with a United Arab Emirates company in June 2019 without obtaining authorisation from relevant authorities, the *Times of Malta* reported on 26 April.

Sanctions evasion charges have reportedly been announced against Fenech, four of his employees and Sovereign Charterers, a Malta-based company held under Fenech’s Unified Global Services Group (UGSG), *Malta Today* reported on 27 April.

A request to freeze assets linked to Fenech has reportedly been issued and accepted by the courts. Other companies within his UGSG group include Fieldsports, RAE Malta and Safety at Sea Logistics.

Maltese authorities are also reportedly investigating a network of Malta-based companies and their foreign business partners on suspicion they helped provide weapons, tactical supplies and military contractors to forces linked to Libyan military commander Khalifa Haftar, the *Times of Malta* reported on 28 April.

The United Nations-approved Libyan government accused Haftar, leader of the Libyan National Army (LNA), of seeking to stage a new coup d’état after he claimed his army had a “mandate” from the people to govern the country, *Al Jazeera* reported on 28 April.

Swiss prosecutors are reportedly set to drop one of two open corruption cases against Sepp Blatter, the former president of FIFA, which concerns allegations of corruption in the sale of World Cup TV rights to the Caribbean Football Union (CFU), according to a report by *Reuters* on 11 April.

"We confirm the Office of the Attorney General of Switzerland [...] considers the criminal investigation into the partial facts and allegations concerning the contractual relationship with the CFU to be complete and ready for conclusion," the OAG said in a statement to *Reuters*.

Blatter was accused of selling television rights to the CFU for the 2010 and 2014 World Cup games far below market value, a combined $600,000. The CFU was under the control of disgraced former FIFA vice president Jack Warner, who was banned from football for life by FIFA’s ethics committee in 2015 for multiple misconduct charges.

Blatter is currently serving a six-year ban from all football-related activity and still faces a second criminal investigation over an alleged payment of CHF 2 million (£1.6 million) to then president of UEFA, Michel Platini, in February 2011. Blatter denies all wrongdoing in the case.
Indian high court quashes government efforts to ban Deloitte and KPMG affiliate

The Bombay High Court reportedly quashed on 21 April efforts by the Indian government to impose a five-year ban on Deloitte Haskins & Sells LLP and KPMG's affiliate BSR & Associates for allegedly aiding fraud at a subsidiary of Infrastructure Leasing & Financial Services (IL&FS), Reuters reported.

Legal filings reportedly show the Indian government detected at least 22 violations of auditing standards by the firms, which likely face a Supreme Court appeal of the ruling.

Indian investigative agencies, regulatory bodies and ministry officials reportedly accused the audit firms of failing to raise red flags on misstatements in the accounts of IL&FS' subsidiary, IL&FS Financial Services (IFIN), Mint reported on 20 June 2019.

Austrian court dismisses fraud probe against Airbus, but bribery case continues

An Austrian court has dismissed a government complaint against European aircraft manufacturer Airbus as part of a probe into alleged corruption and fraud involving a 2003 Eurofighter jet contract, with the criminal court finding no basis for prosecution in the charges filed in February 2017 by Austria's Ministry of Defence, Reuters reported on 27 April.

The Austrian Ministry of Defence triggered a probe into Airbus and the Eurofighter consortium, which also includes Britain's BAE Systems and Italy's Leonardo, in February 2017, alleging that they had misled the state about the price, deliverability and equipment of the planes. Airbus and the consortium denied the accusations. The closure of this case does not impact a broader criminal investigation into suspected bribery involving the same deal that has been ongoing since 2011, a court spokeswoman reportedly confirmed.

Venezuela’s Maduro appoints US-designated Tareck El Aissami as oil minister

Venezuela's President Nicolás Maduro reportedly promoted to oil minister his former economy vice president Tareck El Aissami, who is subject to US asset freezes and criminal proceedings for alleged drug trafficking, Reuters reported on 27 April.

El Aissami was designated by the US Treasury in February 2017 as a drug trafficker and charged by US prosecutors in March 2019 with violating US sanctions and the Foreign Narcotics Kingpin Designation Act.
US reportedly plans to block IMF loan to Iran for Covid-19 response

The US State Department’s spokesperson Morgan Ortagus told reporters the US opposes any fulfilment of Iran’s request for a $5 billion loan from the International Monetary Fund (IMF), claiming Tehran will use the funds to finance terrorist proxy groups in the Middle East, the BBC reported on 7 April.

Iran’s central bank reportedly asked the IMF for an emergency loan from its Rapid Financing Instrument (RFI) in March to help deal with the Covid-19 pandemic, which has resulted in more than 62,000 infections and 3,800 deaths in the nation to date.

The US State Department issued a statement on 6 April claiming that US sanctions are not hindering the delivery of medical aid to Iran, whose healthcare services are “woefully underfunded” after its government allegedly spent more than $16 billion on funding terrorist proxies abroad since 2012. Iran’s priority is “access to cash, not medicine,” according to the State Department.

Indonesian anti-corruption body demands 12-years for ex-president of national airline

Indonesia’s Corruption Eradication Commission (KPK) charged Emirsyah Satar, former president director of the country’s national airline Garuda Indonesia, with bribery and money laundering, and demanded that he be handed a 12-year jail sentence for accepting bribes totalling Rp 49.3 billion (£2.6 million) from Airbus and Rolls-Royce in exchange for purchasing aircraft and machine parts, according to an article published in the Jakarta Post on 24 April citing an article published by Antara News – Indonesia’s national news agency.

The KPK accused Emirsyah of accepting bribes on five separate occasions during his tenure as President (between 2005 and 2014), and named two former senior Garuda staff members, Hadinoto Soedigno, and Agus Wahjudo, as alleged co-conspirators on the bribery charge.

Further, Emirsyah is accused of laundering the bribes through a variety of channels, including debt repayments and property schemes such as a home renovation project in South Jakarta, that also implicated Soetikno Soedarjo, the former president director of a retail holding company and the subject of a separate corruption trial, according to the Jakarta Post article.
Nigeria criticises US senator’s questions over repatriation of funds, US sets out safeguards

Reuters reported on 10 April that Nigeria’s Economic Financial Crimes Commission (EFCC) has criticised a letter sent by the US Senate Finance Committee Chairman, Senator Chuck Grassley, to the head of the US Justice Department’s anti-money laundering unit that calls for a review of the plans to return $320 million in embezzled funds to the Nigerian government that were stolen by the country’s former dictator, General Sani Abacha, during his five years in power in the 1990s.

The US Department of Justice recovered $320 million of illicit gains through the US courts, and in February the US reached an agreement with Nigeria and the British dependency of Jersey to repatriate the recovered funds to Nigeria. Senator Grassley wrote to the head of the US Justice Department’s AML unit on 1 April asking for proof that funds returned to Nigeria would go towards infrastructure projects.

Grassley’s letter states, “it seems odd that the (U.S.) DoJ would help facilitate the payment of $320 million to the Nigerian government without first insisting on proper safeguards to prevent the further misuse of funds,” further alleging that the EFCC “has served as an enforcement arm against anyone voicing opposition to the Buhari government,” calling into question the impartiality of the actions of the anti-corruption body.

In a written response to Grassley’s letter on 27 April, US Assistant Attorney General Stephen Boyd sets out the safeguards detailed in the trilateral agreement on the repatriation of the funds, which includes the making public of documents concerning the disbursement of the funds, the prohibition of certain expenditures that would benefit the alleged perpetrators of the underlying criminal conduct, and the independent audit and monitoring of projects financed with the repatriated funds.

In addition to this, Boyd explains that the agreement stipulates that should any of the parties to the agreement conclude that any of the returned funds have been used for an “ineligible expenditure” then a “claw-back” provision will obligate the Federal Republic of Nigeria to replace those improperly diverted funds.

Opaque Covid-19 procurement process gives millions to Slovenian gambling mogul

The Slovenian government has approved a €25.4 million contract with a company, Public Digital Infrastructure d.o.o., owned by Joc Pečečnik, a Slovenian gambling mogul and one of the country’s richest men, to provide “unspecified protective equipment” as part of a series of emergency measures – that bypass the normal open tender bidding process – to tackle the effects of Covid-19, according to a report published by the Organized Crime and Corruption Reporting Project (OCCRP) on 3 April.

The OCCRP article raises concerns about this decision, as neither Pečečnik nor any of his companies – including Public Digital Infrastructure – have prior experience in the healthcare sector. Further, three other companies that were awarded lucrative state contracts as part of the emergency tenders process do not appear to have the “kind of track record” that would successfully pass the usual tender process, as the total revenue of each of these companies in 2018 was only a fraction of the value of the government contracts, according to the OCCRP.
Libya’s illicit imports of jet fuel from UAE likely to violate the arms embargo, reports the FT

The UN Security Council’s Panel of Experts on Libya is investigating whether a shipment of 11,000 tonnes of jet fuel from the United Arab Emirates (UAE) to the city of Benghazi in eastern Libya, controlled by General Khalifa Haftar’s militias, violated the UN international arms embargo, according to an article published by the Financial Times (FT) on 20 April.

According to the FT, the fuel was supplied by the UAE-registered company Afrifin Logistics FZE, transported by the Liberian-flagged tanker MT Gulf Petroleum 4, operated by Gulf Shipping Services FZC, and offloaded in Libya on 16 March. The FT further reveals that documents whose authenticity could not be confirmed allege that the shipment was ordered by a company called Libyan Express Airlines.

UN Libya envoy Stephanie Williams reportedly said that: “We are very concerned about this incident given that the illicit import of jet fuel by the parallel eastern National Oil Corporation (NOC) would very likely be used to support LNA [Libyan National Army] air force operations, as the legitimate Tripoli-based NOC is already supplying sufficient amounts of jet fuel for commercial use”.

In a letter to the UN Security Council dated 29 November 2019, the Libya Panel of Experts mentioned that the consumption of jet fuel in eastern Libya rose in relation to the conflict dynamics despite commercial aviation activity being relatively constant, raising suspicions about possible illicit imports of aviation fuel.

Nigerian firm handling state records reportedly owned by man accused of fraud

Nigerian authorities have reportedly given state contracts to a company beneficially owned by Mahmood Ahmadu, who is wanted by the Economic and Financial Crimes Commission (EFCC) over February 2016 charges of procurement fraud and money laundering, the BBC and Premium Times reported on 8 April.

Reporters identified Ahmadu as the sole shareholder and ultimate beneficial owner of Online Integrated Solutions Ltd (OIS), which is in charge of collecting sensitive data from Nigerians and foreigners on behalf of the Nigerian Immigration Service, the Central Bank of Nigeria and the National Identity Management Commission.

Nigerian embassies in the UK and US reportedly instructed visa applicants to submit the relevant documentation to OIS and to pay both the government’s visa fee and OIS’ charges for processing their documents.