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 March issue of the Financial Crime Digest. To receive the publication direct to your inbox every month, please sign up here. We are currently developing an online platform, which provides more comprehensive coverage of financial crime developments. If you would like more information on the new platform or our services please email info@aperio-intelligence.com

Aperio Intelligence’s next webinar ‘The impact of Unexplained Wealth Orders on the UK’s financial and property sectors’ will take place on 12 May. Our expert panel will discuss the role UWOs have played as an investigative tool in civil recovery proceedings, their impact in the UK, and offer predictions for post-Brexit civil recovery of the proceeds of crime. Register here.

EDITOR’S PICKS

ENFORCEMENT
16 March 2021
UK FCA launches criminal proceedings against NatWest for AML violations

REPORTS AND SPEECHES
30 March 2021
UK’s Crown Prosecution Service publishes first ever Economic Crime Strategy

SPECIAL FEATURE
31 March 2021
US reversal of Dan Gertler licence underscores challenges to anti-corruption efforts in the DRC

CONSULTATIONS
18 March 2021
UK consultation on restoring trust in audit, includes proposal on fraud prevention

DATES FOR THE DIARY

APRIL
8
UK Payment Systems Regulator’s call for views on APP scams closes

APRIL
9
FATF consultation on guidance on proliferation financing risk assessment closes

APRIL
20
Call for input on mitigating the unintended consequences of the FATF Standards closes

APRIL
20
FATF consultation on draft guidance on a risk-based approach to virtual assets closes
UK FCA launches criminal proceedings against NatWest for AML violations

According to 16 March reporting by Reuters, the customer in question was gold and jewellery dealer Fowler Oldfield, which was purportedly liquidated in 2016 following a police raid. As of December 2020, according to the company’s liquidators, seized company assets remain in police custody.

Reuters reporting on 19 March claims that NatWest informed the news agency that the criminal proceedings against it are related to another case involving 13 individuals who have been charged with money laundering, including two former Fowler Oldfield directors and former gold dealer James Stunt, whose gold trading company Stunt and Company was also liquidated.

The FCA’s charges mark the first instance of the MLRs 2007 being used to prosecute a bank, with no individuals being charged as part of the case.

NatWest is due to appear at Westminster court on 14 April.

The UK’s Financial Conduct Authority (FCA) announced on 16 March that it is filing criminal charges against National Westminster Bank Plc (NatWest) for alleged violations of the Money Laundering Regulations (MLR) 2007. Specifically, the FCA alleges that the bank’s systems and controls failed to adequately monitor or scrutinise large cash deposits into one of its UK incorporated customer accounts.

According to the FCA, the violations relate to a single NatWest customer who, between 2011 and 2016, purportedly accepted “increasingly large cash deposits” that apparently totalled £264 million out of £365 million in total deposits into the customer’s accounts. It is alleged that the bank failed to adhere to MLR regulations 8(1), 8(3) and 14(1).

Aperio Analysis by Gunita Thethy

The NatWest case is linked to a separate case brought by the Crown Prosecution Service, which filed charges against 13 people linked to the same NatWest accounts for money laundering offences in the UK. Aside from Fowler Oldfield, this includes two of its former directors, Gregory Frankel and Daniel Rawson, and former gold trader James Stunt, who runs a Mayfair-based gold bullion business and was a one-time supplier to Formula One. The FCA’s decision to pursue criminal proceedings against NatWest for alleged money laundering, rather than a civil action, is unprecedented. It serves as a clear warning to banking and financial services firms that if the case is serious enough, the FCA will not hesitate to take this type of action. Further, if successful in April, the FCA could be encouraged to bring more such prosecutions.
Swiss bank Rahn+Bodmer enters $22 million settlement over helping US clients evade taxes

The US Department of Justice (DOJ) announced on 11 March that Swiss private bank Rahn Bodmer Co has entered into a $22 million deferred prosecution agreement (DPA) over criminal charges that it conspired to help US clients evade their tax obligations, file false federal tax returns and defraud the US Internal Revenue Service (IRS).

According to the information filed by the US Attorney’s Office for the Southern District of New York, the bank helped 340 US customers avoid paying $16.4 million in taxes between 2004 and 2012, with the relevant undeclared assets under management topping $550 million in 2007. To help US account holders hide assets, the firm reportedly set up “numbered” or “pseudonym” accounts to conceal identities, opened accounts in the names of non-US corporations, trusts and legal entities and held bank statements in Switzerland.

In addition, the bank allegedly transferred the undeclared assets of some US taxpayers from accounts held in the names of sham foundations based in Liechtenstein to new accounts in the names of new sham foundations incorporated in Panama, after a tax information exchange treaty between Liechtenstein and the US was agreed in December 2008. When UBS Group AG and other Swiss banks took measures to curb offshore tax evasion, the bank allegedly onboarded some of their former clients and undertook actions to hide their offshore wealth.

The bank also allegedly opened “escrow” accounts to facilitate the transfer of undeclared US assets held in gold and other precious metals on behalf of a Swiss lawyer and helped accountholders with the repatriation of assets to the US through incremental payments and the routing of funds to a diamond dealer in Manhattan.

According to the DOJ, the reduced penalty amount took into consideration that the bank conducted an internal investigation, provided the US authorities with the required evidence and implemented remedial measures.

Under the terms of the DPA, the bank has accepted responsibility for its conduct and agreed to cooperate fully with US agencies. In addition, it has committed to provide upon request all information required from Swiss banks taking part in the Programme for Non-Prosecution Agreements or Non-Target Letters, in relation to accounts closed between 2009 and 2019. If the bank fully complies with the terms of the DPA, the US government will defer prosecution for three years and will then dismiss the charges.

---

Pension fraud suspect extradited to the UK

The UK’s Pensions Regulator (TPR) announced on 20 March that Alan Barratt, a pension schemes trustee, has been extradited from Spain in connection with a £13.7 million pensions fraud criminal case.

According to the regulator, Barratt and two other individuals, Susan Dalton and Julian Hanson, abused their position as trustees of pension schemes between 2012 and 2014, allegedly persuading 245 savers to transfer their savings into 11 pension schemes that were administered by the defendants.

Barratt has been released on bail and the case was adjourned until 13 April at Westminster Magistrates’ Court. None of the three defendants have entered a plea agreement.

On 11 March, the TPR issued draft guidance for public consultation on its new competence to investigate and prosecute individuals who avoid employer debts to pension schemes or who threaten savers’ pensions.

---

DOJ press release
Agreement

TPR press release
TPR notice (30 August 201...)
TPR press release (11 Mar...)

---
OFAC reaches settlement with Nordgas over alleged Iran sanctions violations

The US Department of the Treasury’s Office of Foreign Assets Control (OFAC) announced on 26 March that Italy-based gas boiler systems and applications components manufacturer Nordgas s.r.l has agreed to pay $950,000 to settle potential civil liability for purported violations of sections 560.203 and 560.204 of the Iranian Transactions and Sanctions Regulations (ITSR). OFAC agreed to suspend $650,000 of the settlement.

According to OFAC’s notice, between March 2013 and March 2017, Nordgas deliberately re-exported 27 shipments of air pressure switches procured from an unnamed US-based company, causing the company to conduct the exports indirectly. The components totalling $2,526,783 were intended for ten customers in Iran. According to media reports, the associated company is UniControl Inc, which has also recently agreed to settle with OFAC ITSR violation allegations involving shipments of similar components during the same period.

When agreeing to the partial suspension of $650,000 of the settlement, OFAC noted Nordgas’ cooperation and its implementation of enhanced compliance commitments.

OFAC assessed the case as egregious considering the fact that Nordgas assured the US company that the items would only be re-exported to Italian affiliates, after it had been informed that they would violate US sanctions if sent to end-users in Iran. In addition, Nordgas employees used deceptive replacement terms for Iranian end-users in correspondence and trade documentation with the US company and requested that the term “Made in USA” be removed from the switches to conceal their origin.

When agreeing to the partial suspension of $650,000 of the settlement, OFAC noted Nordgas’ cooperation with OFAC, its implementation of enhanced compliance commitments, including the submission of a report to OFAC on an annual basis for 5 years describing steps taken to meet the commitments.

Aperio Analysis by James Tytler

This action clearly demonstrates the extraterritorial reach of US secondary sanctions and OFAC’s ability to enforce compliance, even against SMEs; Nordgas is an Italian electronics manufacturer based in rural Northern Italy, with a few dozen employees. The case against Nordgas was clear cut; the company wilfully and explicitly violated US sanctions against Iran by both attempting to conceal the US-origin of the goods, and also misrepresented their intended destination to UniControl. However, the fact that UniControl also reached a settlement with OFAC, despite having self-reported the potential violations, indicates the lengths all parties must go to in order to avoid culpability. Claiming ignorance or turning a blind eye is not sufficient. OFAC found that UniControl had failed to act on red flags indicating that its products were not being exported to European customers, as indicated by Nordgas, but were in fact destined for Iran. This case highlights the need for extreme vigilance with regard to any transactions with a potential Iranian nexus, even if attempts are made to conceal it.
OFAC reaches settlement with UniControl over apparent Iran sanctions violations

The US Treasury Department’s Office of Foreign Assets Control (OFAC) announced on 15 March that Ohio-based UniControl Inc has agreed to pay $216,464 to settle its potential civil liability for apparent violations of the Iranian Transactions and Sanctions Regulations (ITSR).

According to OFAC’s enforcement release, UniControl allegedly exported a total of 21 shipments of air pressure switches between 2013 and 2017 to two European companies “with reason to know that the goods were intended specifically for supply, transshipment, or reexportation to Iran”. For two out of the 21 shipments, OFAC states, UniControl “had actual knowledge” that they would be sent onwards to Iran.

The warning signs that UniControl reportedly received and allegedly failed to respond to included requests to remove “Made in USA” labels from its products, customer interest in the Iranian market, the inclusion of Iran by the European company as an authorised sales territory, engagement by UniControl employees with Iranians during at least two trade shows in Europe, and obfuscated end-user requests by the European trader.

OFAC noted in reaching the settlement amount, the non-egregious nature of UniControl’s alleged activities as well as the company’s voluntary disclosure of the apparent violations to OFAC. According to OFAC, the company has also invested in and strengthened its trade compliance procedures.

US BIS enters settlement with Comtech Xicom Technology over alleged unlicenced exports

The US Department of Commerce’s Bureau of Industry and Security (BIS) announced on 19 March that it has reached an administrative settlement with satellite communications equipment supplier Comtech Xicom Technology over purportedly engaging in exporting controlled traveling wave tubes to Russia, the United Arab Emirates (UAE), and Brazil, without the required export licences.

According to the BIS order, between December 2015 and March 2017, Comtech Xicom exported traveling wave tubes totalling $153,945 on three occasions. The company made the exports in violation of Section 766.3 of the Export Administration Regulations which classifies the items as controlled for national security reasons and require a licence or other authorisation for export.

In addition, it is alleged that the shipments were exported after compliance personnel incorrectly stated that the exports to the UAE and Russia did not require a licence and made an incorrect determination as to the licence requirements of the shipment to Brazil.

As part of the agreement, Comtech Xicom will pay a $122,000 penalty as a condition for the granting, restoration, or continuing validity of any export licence.
US BIS fines German company for exporting US aircraft parts to Iran's Mahan Air

Under the Freedom of Information Act (FOIA) programme, the US Commerce Department’s Bureau of Industry and Security (BIS) made public on 5 March an order imposing a civil penalty of $51,921 on German company MSI Aircraft Maintenance Services International GmbH & Co over apparent Iran sanctions and export control violations.

According to the BIS order, MSI conspired with an unnamed German company between 2011 and 2012 to supply US parts and components to privately owned Iranian airline Mahan Air, a designated entity in the US since October 2011, without being authorised to do so by the US authorities. To be able to order and purchase aircraft parts from a US manufacturer, a MSI employee falsely indicated that they were destined for end-users in Thailand and Afghanistan.

In addition to the financial penalty, MSI is subject to a three-year denial of export privileges, which will be waived if the company cooperates with BIS and OFAC, pays the fine within the agreed deadline, complies with the reporting requirements and abstains from further violations of US export rules.

On 22 December 2020, BIS included Germany-based Maintenance Services International (MSI) GmbH, known under the aliases MSI Aircraft Maintenance Services International GmbH & Co KG and MSI International GmbH and Company, among the 77 entities added to the Export Administration Regulations (EAR) Entity List. According to BIS, these entities are subject to additional licence requirements, in view of their involvement, or their risk of becoming involved, in activities that are contrary to the national security or foreign policy of the US.

Russian national and his company plead guilty to violating US export controls

The US Department of Justice (DOJ) announced on 30 March that Russian national, Oleg Vladislavovich Nikitin, and his company KS Engineering, have pleaded guilty to charges of violating US national security laws, orchestrating a scheme to evade export control regulations.

Nikitin, the general director of Russia-based KS Engineering, admitted that he conspired with employee Anton Cheremukhin and an Italian company GVA International Oil and Gas Services and its employees, Bruno Caparini, Gabrielle Villone and Dali Bagrou, to evade US export regulations, in violation of the International Emergency Economic Powers Act (IEEPA) and the Export Control Reform Act.

It is alleged that Nikitin conspired to acquire a power turbine for $17.3 million on behalf of a Russian state-controlled company from a US-based manufacturer. The turbine was to be used on a Russian Arctic deepwater drilling platform, and the shipment or transfer of such equipment to Russia requires a licence from the US Department of Commerce.
John Wood Group reaches settlement in Scotland over Unaoil-related Kazakhstan bribery

British engineering and consulting company John Wood Group plc announced on 16 March that its subsidiary WGPSN (Holdings) has reached a £6.46 million settlement with Scotland’s Civil Recovery Unit concerning a Kazakhstan bribery probe involving Monaco-based consultancy Unaoil and offshore and onshore oil facility contracts.

While part of a joint venture, WGPSN’s subsidiary, PSNA Limited, won two Kazakhstan tenders in 2008 and 2010. Between 2012 and August 2015, the joint venture paid Unaoil almost $9 million with only “limited evidence of legitimate service being provided”, according to the Crown Office and Procurator Fiscal Service (COPFS) within the Scottish Prosecution Service. Wood acquired the business in 2011, years before the bribery allegations were reported in the media in 2016. Following the media allegations, the British company conducted an internal investigation and submitted the findings to the COPFS. The sum that WGPSN will pay represents the dividends and retained profits from the two contracts.

In its 2020 year-end results, John Wood Group revealed to investors it is increasing by $150 million the amount previously allocated for settling the allegations in Scotland and another bribery case it is exposed to in the US and Brazil. The second probe concerns allegations of illegal payments made by Unaoil on behalf of clients to secure contracts in several countries, including for the benefit of engineering and project management company Amec Foster Wheeler plc, which Wood acquired in 2017.

Former Unaoil CEO Cyrus Ashani and his brother, Saman, the COO of the company, pleaded guilty to US charges of offering millions of dollars in bribes to government officials all around the world. In December 2020, the Texas Southern District Court issued a continuance order, with sentencing scheduled for 13 September 2021. Four Unaoil managers have already been sentenced in the UK over Iraq bribery allegations after a five-year Serious Fraud Office (SFO) investigation.

Ten Iranian nationals charged with conspiring to evade US sanctions on Iran

The US Department of Justice (DOJ) announced on 19 March that 10 Iranian nationals have been charged with conspiring for almost 20 years to violate the Iranian Transactions and Sanctions Regulations, the Iranian Financial Sanctions Regulations and the International Emergency Economic Powers Act.

It is alleged that the accused conspired to evade US sanctions by disguising over $300 million worth of transactions carried out on behalf of the Iranian government. The defendants allegedly made false representations to US financial institutions and used over 70 front companies located in the UAE, Hong Kong, Canada and San Fernando Valley in the US to facilitate the transactions. The transactions included the purchase of two oil tankers valued at $25 million each.

The complaint filed in October 2020 also seeks a $157,332,367 money laundering penalty from the defendants who are still at large.
UK Gambling Commission fines In Touch Games Ltd over AML and customer breaches

The UK Gambling Commission announced on 17 March that it has issued a formal warning and imposed a £3.4 million fine on mobile casino operator In Touch Games Ltd for failing to comply with its social responsibility, anti-money laundering (AML) and customer interaction obligations.

According to the regulator, In Touch Games neglected its AML obligation to conduct “appropriate levels of enhanced customer due diligence”, while its risk assessment failed to consider risks associated with customers using a payment provider which also acted as a cryptocurrency exchange. In addition, the company failed to conduct reviews of source of funds information upon the Commission’s request.

The notice states that In Touch Games failed to put its customer interaction procedures and policies into action for seven customers whose activity indicated problem gambling concerns, and did not use all sources of information to ensure effective decision-making and deliver effective customer interactions for those clients. The Commission concludes that the company “should have given more consideration to placing mandatory limits on customer accounts”.

In Touch Games has also been ordered to appoint an independent auditor to assess its compliance with the Commission’s Licence Conditions and Codes of Practice.

UK Gambling Commission fines Casumo for AML and social responsibility failings

The UK Gambling Commission announced on 25 March that it is fining Maltese gambling platform operator Casumo £6 million for a range of anti-money laundering (AML) regulatory lapses and social responsibility failings which resulted in significant customer losses. As a consequence, Casumo will also be required to undergo extensive auditing of all transactions since 1 July 2020 at the company’s expense and has been issued with an official warning.

The Commission found that Casumo did not implement necessary procedures to intervene when customer activity appeared problematic, such as when a customer lost £1.1 million during a three-year period without the company engaging in a responsible gambling interaction. The company further failed to follow Commission guidance on customer interaction, as was apparent when one customer lost £89,000 in five hours and another lost £59,000 over 90 minutes.

The failings included:
- Significant sums deposited by customers without AML checks taking place
- Evidence of Source of Funds (SOF) not checked against bank statements and proving insufficient
- Incomplete bank statements accepted without necessary assessment
- Identification documents not verified
- SOF included winnings from other gambling platforms without follow-up
- Effective control, policy, and procedure implementation not ensured or reviewed
UK Gambling Commission fines five casinos for AML and social responsibility violations

The UK Gambling Commission announced on 30 March that it has fined or reached regulatory settlements with five casinos after assessments revealed failures to follow anti-money laundering (AML) and social responsibility obligations. All five casinos’ operating licences are also under review as part of the enforcement actions.

Casino operators Clockfair Ltd and Shaftesbury Casino Ltd are to pay settlements of £260,000, while Double Diamond Gaming Limited will pay a £247,000 settlement, with all three committing to reviewing and updating their AML policies and procedures.

Clockfair was found to have allowed multiple customers to gamble for nearly two years after triggering company AML red flags through substantial deposits and significant losses, in one case originating from a high-risk jurisdiction. Both Clockfair and Shaftesbury were found to have in multiple instances failed to screen for politically exposed persons (PEPs) or financial sanctions.

Les Croupiers Casino Limited is set to pay a £202,500 regulatory settlement for multiple AML failings, including not undertaking checks to establish source of funds for customers with significant deposits and losses as well as failures to record reasons for setting high daily loss limits for a customer with questionable business fund sources.

A&S Leisure Group Limited is being issued with a warning and a £377,340 fine for failing to maintain proper policies to prevent ML and TF, record sufficient information on customer interactions to gauge if customers should be flagged as high-risk for gambling problems, and interacting in a timely manner with customers experiencing significant harm or losses. The Commission also notes that A&S cooperated with investigators and did not attempt to conceal the breaches.

US orders UK national to pay $571 million over fraudulent Bitcoin trading scheme

The US Commodity Futures Trading Commission (CFTC) announced on 26 March that the US District Court for the Southern District of New York has ordered UK national Benjamin Reynolds to pay $571 million in fines for defrauding customers between May and October 2017 of Bitcoin valued at around $143 million.

According to the CFTC, Reynolds has tricked over one thousand customers worldwide into purchasing Bitcoins from third party vendors and depositing the virtual currency with his UK-based company Control-Finance Ltd. In addition, the defendant allegedly falsely represented to customers that their Bitcoin deposits were traded in virtual currency markets to generate profits. An affiliate marketing network was created, which relied on falsely promising payments of profits, rewards and bonuses to encourage existing customers to refer new customers to Control-Finance Ltd.

The judgment is the result of a 2019 CFTC enforcement action filed against Reynolds and his company Control-Finance Ltd for fraud and misappropriation of virtual currency.
Former Honduran Congressman given life sentence in the US for drug trafficking

Former Honduran congressman Juan Antonio Hernández Alvarado, also known as Tony Hernández, was sentenced on 30 March to life in prison in the US Southern District of New York for his role in a vast drug trafficking conspiracy between 2004 and 2015.

The ex-politician, who is the brother of President Juan Orlando Hernández, was convicted in October 2019 for conspiring to import cocaine into the US, possessing and conspiring to possess machine guns and destructive devices, and making false statements.

According to Judge Kevin P. Castel, Hernández is responsible for manufacturing and distributing 185 tonnes of cocaine, as part of a "state sponsored narco-trafficking" scheme.

In addition, the former congressman exercised control over members of the country’s armed forces and sold ammunition to drug traffickers, according to a 30 March Department of Justice (DOJ) press release. Hernández reportedly acted as a middleman between narcotraffickers and top-level politicians, including by delivering a $1 million bribe to the country's president on behalf of the ex-leader of the Sinaloa cartel Joaquín Archivaldo Guzmán Loera. Hernández has also been ordered to forfeit $138.5 million.

The current Honduran head of state is himself subject to a criminal investigation in the US for allegedly accepting bribes from drug trafficker Geovanny Daniel Fuentes Ramírez, in exchange for offering him protection from arrest and extradition. According to the DOJ, the politician directed Fuentes Ramírez to collaborate directly with Tony Hernández to export drugs. The chief of state is identified as ‘CC-4’ in a February court filing in the case against Fuentes Ramírez. President Hernández has repeatedly rejected the allegations.

Ex-trader pleads guilty to price manipulation

The US Department of Justice (DOJ) announced on 25 March that former oil trader Emilio José Heredia Collado has pleaded guilty to conspiracy to engage in commodities price manipulation between September 2012 and August 2016.

According to documents filed before the US District Court for the Northern District of California, Heredia and his co-conspirators sought to unlawfully enrich themselves by manipulating oil benchmark prices and directing other traders to submit bids and offers through oil price benchmark publisher S&P Global Platts, for intermediate fuel oil 380 CST at the Port of Los Angeles.

The defendant allegedly directed his co-conspirators to submit the fuel oil order in the final minutes of daily trading, known as the “Platts window”, for the purpose of artificially affecting the evaluation mechanism.

According to media reports, the defendant is a former employee of Swiss commodity trading and mining company Glencore Ltd. Bloomberg reported on 23 March that the company confirmed in a statement that “one of Chemoil’s – and later Glencore Ltd – former employees in the US has been charged with conspiracy to manipulate the price of fuel oil in the LA market between 2012 and 2016”.

On 25 March, the US Commodity Futures Trading Commission (CFTC) issued an order imposing a $100,000 civil monetary penalty to settle parallel charges against Heredia, for violating the Commodity Exchange Act and the CFTC regulations. In addition, the order permanently bans the defendant from trading commodity interests.
Former Mexican governor pleads guilty to money laundering in the US

The US Department of Justice (DOJ) announced on 25 March that former Mexican governor and presidential candidate Tomás Yarrington Ruvalcaba pleaded guilty to accepting over $3.5 million in bribes and laundering the proceeds through real estate in the US.

According to the DOJ, Yarrington admitted to receiving bribes from Mexican individuals and private companies which sought to secure business with the state of Tamaulipas between 1999 and 2005, when he was governor. Yarrington allegedly used the illicit funds to purchase property in the US, including real estate and vehicles, which he acquired through nominee buyers to hide his ownership.

Yarrington was charged in 2013 in the US for allegations of racketeering, drug smuggling, money laundering and bank fraud, and was extradited in 2018 after he was captured in Italy while travelling using false identification documents. As part of his plea agreement in the US, Yarrington has agreed to forfeit an illegally purchased condominium in Port Isabel.

Former Venezuelan official pleads guilty to bribery and money laundering in the US

The US Department of Justice (DOJ) announced on 22 March that dual US-Venezuelan citizen Jose Luis De Jongh Atencio, a former procurement officer and manager at Citgo Petroleum Corporation’s Special Projects Group, has pleaded guilty to conspiracy to commit money laundering, in connection with an international bribery scheme, in violation of the Foreign Corrupt Practices Act (FCPA).

Citgo is a Houston-based subsidiary of Venezuelan state-run oil company Petróleos de Venezuela S.A. (PDVSA). According to the DOJ, De Jongh accepted over $7 million in bribes between 2013 and 2019 from businessmen Jose Manuel Gonzalez Testino and Tulio Aníbal Farias Perez and others, in exchange for assisting them and related companies in securing contracts with Citgo and PDVSA. The defendant admitted to transferring bribe payments from Testino and Farias to bank accounts of shell companies in Switzerland and Panama, which he controlled, as well as falsifying invoices.

As part of his plea agreement, De Jongh has agreed to forfeit more than $3 million seized from his accounts, as well as 15 properties.
North Korean national extradited to the US over sanctions evasion allegations

The US Department of Justice (DOJ) announced on 22 March that North Korean national Mun Chol Myong has been extradited to the US over allegations of laundering money through the US financial system as part of a scheme to provide luxury items to North Korea. Mun faces six counts of money laundering.

Mun and others are accused of conspiring to fraudulently access the US financial system between April 2013 and November 2018. Mun allegedly defrauded US banks to evade counter-proliferation sanctions imposed by the US and the UN on North Korea and laundered money in transactions amounting to more than $1.5 million. It is also alleged that Mun was affiliated with the Reconnaissance General Bureau, North Korea’s primary intelligence organisation, which is subject to US and UN sanctions.

The indictment alleges that Mun and his conspirators used a web of front companies and bank accounts registered to false names and removed references to North Korea from international wire transfer and transactional documents. As such US correspondent banks were allegedly deceived into processing US dollar transactions for the benefit of designated entities.

According to the DOJ, this the first ever extradition of a North Korean national to face charges in the US.

US CFTC reaches settlement with Coinbase over false reporting and wash trading allegations

The US Commodity Futures Trading Commission (CFTC) issued a 19 March order filing and settling charges against cryptoasset exchange company Coinbase Inc, ordering it to pay a $6.5 million civil monetary penalty after a former employee engaged in wash trading on the company’s GDAX platform. According to the regulator, the firm itself “recklessly delivered false, misleading or inaccurate” transaction reports and failed to disclose that it was trading between two of its own programmes.

Between January 2015 and September 2018, the company used two automated trading programmes, Hedger and Replicator, that at times generated matching orders with one another. According to the order, the digital asset transactions, including in Bitcoin, may have given misleading impressions about asset volumes and liquidity levels, while the company allegedly failed to disclose that it was operating multiple programmes from multiple accounts.

Separately, between August and September 2016, an ex-employee was found to have engaged in deception by placing matching buy and sell orders on the GDAX platform for a Litecoin/Bitcoin trading pair that matched each other as wash trades to send misleading information about the trading activity to the market. Coinbase is “vicariously liable” for the former employee’s conduct, states the order.

The company disclosed the CFTC allegations in its 17 March filing with the US Securities and Exchange Commission (SEC), amending its previous statement from 25 February relating to a proposed public direct listing on the Nasdaq stock exchange. The firm settled the charges without admitting or denying them.
US sentences founder of private jet firm over Venezuela sanctions evasion

The US Department of Justice (DOJ) announced on 17 March that Victor Mones Coro, the founder of US-based private jet company American Charter Services (ACS), has been sentenced to 55 months in prison for violating US sanctions against senior Venezuelan leaders, pursuant to the Foreign Narcotics Kingpin Designation Act (Kingpin Act).

According to the DOJ, Coro was involved in a scheme to enrich himself by using his company’s planes and employees to provide charter flights to former Venezuelan vice president Tareck Zaidan El Aissami Maddah and Venezuelan businessman Samark Jose Lopez Bello to countries of strategic importance for Nicolás Maduro, such as Russia and Turkey. In addition, Coro arranged over 20 Venezuelan domestic flights to assist Maduro’s 2018 re-election campaign.

Coro and his associates, including Venezuela’s current Superintendent of Cryptocurrencies Joselit Ramírez Camacho, falsified invoices and flight records and used code names and encrypted messaging applications for communication purposes. In addition, Coro received cash transferred from Venezuela to the US and accepted wire transfers from companies linked to the sanctioned Venezuelan individuals. In November 2019, Coro pleaded guilty to violating the Kingpin Act.

El Aissami and Bello were designated by the US Department of the Treasury’s Office of Foreign Assets Control (OFAC) as specially designated narcotics traffickers in 2017 and were charged in March 2019 with criminal violations of the Kingpin Act and US sanctions.

US DOJ charges two individuals in Ecuadorian bribery and money laundering scheme

The US Department of Justice (DOJ) announced on 2 March that two Ecuadorian individuals have been charged with one count of conspiracy to commit money laundering for their alleged role in a bribery scheme involving the Ecuadorian Social Security Institute of the National Police (ISSPOL), in violation of the US Foreign Corrupt Practices Act (FCPA).

According to the complaints filed in the Southern District of Florida, investment advisor Jorge Cherrez Miño paid almost $4 million in bribes to ISSPOL public officials between 2014 and 2020, including risk director John Robert Luzuriaga Aguinaga. In exchange for the bribes, Cherrez secured investment business for him and several companies that he controlled, which brought him nearly $65 million in profits from the fraudulent scheme.

Cherrez allegedly paid bribes to Luzuriaga directly, or through payments made to his relatives, as well as through transfers to US bank accounts of Cherrez’s investment companies for which Luzuriaga owned a debit card.

According to the DOJ, the two Ecuadorian citizens allegedly laundered the illegal proceeds through Florida-based entities and bank accounts, “including numerous US investment fund companies incorporated in Florida with Cherrez as an officer or director”.

Luzuriaga was detained on 26 February and an arrest warrant has been issued in Cherrez’s name, who is currently thought to be in Mexico.
UK Financial Reporting Council to investigate Deloitte over Lookers accounts

Deloitte revealed in June 2020 that it will resign as auditor after Lookers finalised the publication of its 2019 audited financial statements. The company announced last year that a Grant Thornton UK LLP investigation into potential fraud revealed that the company overstated its profits for several years. The inquiry produced evidence of cash expenses fraud, resulting in a loss of £327,000.

The FRC probe will be conducted by its Enforcement Division under the audit enforcement procedure. The announcement follows the UK car dealership’s statement on 2 March that the UK’s Financial Conduct Authority (FCA) is ending its investigation without imposing any fines. While not pursuing penalties, the FCA reportedly made clear its concerns to the company’s board, concerning Lookers’ “historic culture, systems and controls”.

UK FCA fines and bans trader for market abuse

Between July 2018 and May 2019, Horn reportedly executed 129 wash trades by engaging in an abusive strategy aimed at ensuring daily trading of a minimum of 13,000 shares of McKay Securities plc, for which Stifel served as a financial advisor and corporate broker. The FCA notice states that in instances where less than 13,000 shares were traded before the market closed for the day, Horn “would make up the shortfall by executing wash trades with himself”, in order to ensure that McKay remained in the Financial Times Stock Exchange All Share Index.

The FCA notes that Horn contributed to market manipulation by providing “false and misleading signals”, which led other participants to consider investing in McKay shares based on the fictitious volume of reported trades as a result of wash trading. Horn’s initial £100,000 financial penalty was reduced to £52,500 due to the “high level of cooperation” during the FCA investigation and his willingness to settle the case.
UK FCA orders Dolfin Financial (UK) Ltd to stop regulated activities over misconduct concerns

The UK’s Financial Conduct Authority (FCA) announced on 12 March that it has imposed restrictions on wealth management company Dolfin Financial (UK) Ltd, due to misconduct concerns, which include concerns relating to its Tier 1 investor visa services and financial crime controls.

The restrictions imposed stop the company from conducting any regulated activities and “prevent it from reducing the value of its assets, or any of the client money or custody assets it holds”, without prior approval from the FCA. Dolfin will continue to hold client money and custody assets in accordance with the regulator’s rules, but clients will not be able to trade, transfer of withdraw money held in accounts managed by the company without the FCA’s consent.

The regulator imposed voluntary restrictions on Dolfin’s regulated activities on 24 December 2019, when it commissioned a Skilled Persons Review to assess how the company operates its investor visa activities. In light of the review, the FCA concludes that it is “in the interest of protecting the UK financial system to stop the firm from carrying out regulated activities”.

Deloitte PLT agrees to £57 million settlement in Malaysia over 1MDB scandal

Malaysia’s Ministry of Finance announced on 3 March that it has reached a MYR 324 million (£57.3 million) resolution with audit firm Deloitte PLT to settle the auditor’s fiduciary responsibilities in reviewing the accounts of 1Malaysia Development Berhad (1MDB) and its former unit SRC International Sdn Bhd between 2011 and 2014.

Finance Minister Tengku Zafrul called the agreement a “milestone” in the country’s ongoing efforts to hold accountable those involved in the 1MDB corruption scandal. The announcement follows AMMB Holdings Berhad’s (AmBank) global settlement in February worth MYR 2.83 billion (£501 million) with the Malaysian authorities.

On 1 March opposition MP Tony Pua called on the Malaysian government to scrutinise the role international auditors played in the scandal, including Deloitte and KPMG, against whom Pua filed complaints with the Malaysian Institute of Accountants in 2015 for “filing of fraudulent 1MDB financial statements”.

Malaysia’s former prime minister Najib Razak was convicted in July 2020 of abuse of power and money laundering, among other charges, for his role in the 1MDB scandal, after it was found that he had illegally moved money from SRC International into his AmBank accounts while holding office as the country’s prime minister.
Central Bank of Ireland fines investment firm J&E Davy for conflict of interest failings

The Central Bank of Ireland (CBI) announced on 2 March that Irish investment firm J&E Davy has been reprimanded and fined €4,130,000 for breaches of the European Communities (Markets in Financial Instruments) Regulations 2007 (the MiFID Regulations) related to conflicts of interest concerning personal account dealing between 2014 and 2016.

The company’s failings related to a transaction that a group of employees made in a personal capacity with a Davy client. The company was found to have failed to supervise the personal account dealings of a consortium of 16 employees, including a group of senior executives, who personally profited from the sale of Anglo Irish Bank bonds of a Davy client in November 2014, structuring the bond transactions to bypass the compliance system.

With respect to the transaction, CBI found Davy in breach of conflict of interest obligations due to its failure to take all reasonable steps to identify the conflict of interest between the consortium of its employees and the client in the transaction.

The CBI also found that Davy lacked an adequate personal account dealings framework to prevent potential conflicts of interest when employees enter into personal transactions. In addition to this, Davy’s weak internal control mechanisms and its failure to ensure that its compliance function had access to all relevant information in relation to the transaction resulted in Davy’s inability to detect the transaction as part of its ongoing monitoring.

Moreover, Davy also failed to disclose the full extent of the wrongdoing by providing misleading details and withholding information, which was treated as an aggravating factor in the case. Following the CBI’s investigations, two independent reviews were conducted and a revised conflicts of interest policy as well as personal account dealing rules were introduced by Davy in May 2016.

ING France fined over AML/CFT shortcomings

France’s Prudential Supervision and Resolution Authority (ACPR) published on 2 March its decision to impose a €3 million fine on ING Bank France for failing to comply with anti-money laundering (AML) and countering the financing of terrorism (CFT) regulations, following an investigation by the French regulator between September 2018 and February 2019.

ACPR found that ING’s money laundering/terrorism financing risk classification was “incomplete and inoperative” and that the bank failed to assess risks based on the client’s sector of activity, mainly in the real estate, automotive, pharmaceutical and business services sectors.

According to the ACPR, customer due diligence was not adapted to the profile of the client and failed to take into account the nature and risks associated with the customer’s sector of activity, including in the case of politically exposed persons (PEPs).

In addition, ING failed in its obligation to report suspicious activity to the French financial intelligence unit Tracfin, although the bank identified cases where transactions did not match the client’s income. The ACPR did however declare ING’s mechanism for asset freezing effective and “well founded”.

ING stated in a press release that it is committed to strengthening its risk assessment mechanisms and enhancing its customer due diligence and transaction monitoring system in order to “detect and prevent the financial system from being misused for criminal activities”.

ACPR decision
ING press release
EU authorities reportedly crack encrypted communications service being used by criminals

Europol and Eurojust announced on 10 March that a tri-national European enforcement effort has yielded the de-encryption of the communication tool Sky ECC and monitoring of roughly 70,000 of the tool’s approximately 170,000 users since February, resulting in raids and arrests in Belgium and the Netherlands and “the collection of crucial information on over a hundred planned large-scale criminal operations”.

According to press releases from the EU law enforcement agencies, the coordinated effort to unlock Sky ECC’s encrypted messages also involved investigative authorities in France and “will assist in expanding investigations and solving serious and cross-border organised crime for the coming months, possibly years”. Europol and Eurojust state that the investigation began in Belgium following the seizure of mobile phones from suspected criminals that showed the frequent use of Sky ECC. Twenty percent of Sky ECC’s users, which is purportedly operated in the US and Canada and uses European servers, are based in Belgium or the Netherlands. The two agencies report that the authorities have thus far accessed hundreds of millions of Sky ECC messages.

According to a 9 March statement, the company denies that any authorised Sky ECC devices have been hacked or cracked by Belgian and/or Dutch authorities, stating that “SKY ECC maintains, after thorough investigation, that all such allegations are false”, but did acknowledge a connection interruption to its servers on 8 March.

The company claims that authorised distributors in both countries notified Sky ECC that “a fake phishing application falsely branded as SKY ECC was illegally created, modified and side-loaded onto unsecure devices, and security features of authorised SKY ECC phones were eliminated in these bogus devices”. The company also notes that it is not cooperating with investigators nor has it been contacted by the authorities, denying that it is a “platform of choice for criminals” and stating that it has a zero-tolerance policy on criminal activity.

Peru prosecutor charges presidential candidate Keiko Fujimori with money laundering

Peruvian prosecutor José Domingo Pérez announced on 11 March that he has charged presidential candidate Keiko Fujimori and 41 other individuals with money laundering, organised crime, obstruction of justice and perjury, following a two-year investigation into alleged corruption.

Peru’s opposition leader is accused of receiving $1.2 million in illicit campaign funding from Brazilian construction company Odebrecht SA during her first presidential campaign in 2011. In addition to this, the prosecutor asked for the dissolution of Fujimori’s political party Popular Force and filed charges against the company MVV Bienes Raíces SAC, owned by Fujimori’s husband Mark Vito Villanella.

In 2019, Fujimori was placed under pre-trial arrest for 13 months over related allegations, but she was released following a decision by the Constitutional Tribunal of Peru. On 29 January 2020, an appeals court ordered Fujimori to return to prison for an additional period of 15 months.
The UK’s Crown Prosecution Service (CPS) launched on 30 March its Economic Crime Strategy, setting out a five-year plan to combat financial crime and ensure correct and timely prosecution, as part of its aim to contribute to improving criminal justice outcomes concerning economic crime.

Launched at a roundtable meeting with government departments, police and criminal justice partners, the strategy highlights fraud as the most common crime typology in the UK, with 86 percent of reported fraud being cyber-enabled.

Underlining that the number of economic crime victims has increased to 800,000 a year, the CPS seeks to establish how prosecutors can better support all types of victims, from the most vulnerable, who are “exploited and left with unaffordable personal losses”, to businesses, whose impacted viability “leads to significant losses to taxpayers”, according to Max Hill QC, Director of Public Prosecutions.

The strategy highlights fraud as the most common crime typology in the UK, with 86 percent of reported fraud being cyber-enabled.

According to the CPS, economic crime like fraud, terrorist financing, market and regulatory abuse, bribery and corruption, money laundering and sanctions, is perpetrated by exploiting social situations and national disasters, and targets various victims, including individuals, organisations and the public sector. The strategy reflects the steps that the CPS is committing to take to ensure the system has the capability to tackle the threat of economic crime effectively.

Commitments include

- Training and supporting all legal staff across the CPS to ensure a good understanding of the implications of new technology on economic crime and provide prosecutors with the tools to prosecute the most complex economic crime cases
- Harnessing the opportunities of technology to support effective prosecutions, while also balancing the rights of a fair trial with the right to privacy
- Supporting more virtual hearings for economic crime cases, to help reduce the backlog of cases and give victims and witnesses more efficient access to justice
- Ensuring that asset recovery and ancillary orders are successfully pursued in all economic crime cases, domestic and international proceeds of crime are recovered, and international deployments are used to tackle such cases where they also impact domestic casework
- Supporting in the creation of the first Economic Crime Court and the use of more Nightingale Courts for fraud cases

CPS press release

CPS Economic Crime Strategy
UK HMRC AML supervision assessment

The UK’s HM Revenue & Customs (HMRC) published on 17 March its annual report assessing anti-money laundering (AML) supervision of the more than 30,000 businesses in nine sectors it oversees for compliance with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The self-assessment is stipulated by the Economic Crime Plan 2019-2022 to ensure supervisory compliance with the law and professional body supervisor standards.

The self-assessment states that HMRC’s "performance overall is currently broadly in line" with the relevant money laundering regulations and the OPBAS sourcebook. There are however areas for improvement. The report also includes (Annex A) a summary of key statistics for the past five years, including interventions and outcomes.

The report finds that HMRC has recently improved and formalised its risk assessment process for supervised businesses and is making efforts to increase supervisory intervention staff and improve productivity through enhanced training. The department has recently made efforts to improve registration time that has already been shown to have a significant impact, including streamlining registration and perimeter function policing. While information sharing is limited due to tax confidentiality laws, the self-assessment finds that HMRC does share information with supervisors as much as it is legally able to do so.

Promptly sharing new information about emerging risks with supervised businesses is another priority in which HMRC is already taking steps to improve. Lastly, the self-assessment notes that HMRC "has been adopting a tougher approach to sanctions for several years" which has been made easier by the recently released sanctions framework. The report states that it is "expected that the changes, together with the new sanctions framework, should result in efficiency savings and more penalties being issued going forward”.

HMRC intends to review the progress made to further improve its performance in a follow-up self-assessment over the course of the next 12 months.

---

UK government to invest £100 million in new HMRC Covid-19 fraud taskforce

UK Chancellor of the Exchequer Rishi Sunak announced on 3 March in the 2021 Budget speech to parliament that HM Revenue & Customs (HMRC) will set up a taskforce to investigate fraud targeting Covid-19 support schemes.

Sunak said that £100 million will be invested into the taskforce, which will consist of 1,265 HMRC staff members who will investigate fraud targeting the government’s furlough payments scheme as well as a “clamp down on tax avoidance and evasion”.

The UK’s 2021 Budget states that the new taskforce represents one of the largest responses to fraud risk by HMRC and that the government will raise awareness about any enforcement action in order to deter financial crime.
UK Integrated Review includes financial crime reforms and corruption sanctions regime

The UK government published its Integrated Review of Security, Defence, Development and Foreign Policy titled ‘Global Britain in a competitive age’ on 16 March, which sets out the government’s strategic vision for the UK’s international role in the next decade and national security policy objectives up to 2025, including tackling financial crime with more financial investigators, suspicious activity report (SAR) reforms, and increased funding to fight money laundering (ML) and other aspects of serious and organised crime (SOC).

The Integrated Review also indicates that the UK will launch a second global sanctions regime on corruption in 2021, and that there will be further use of the UK’s Magnitsky-style sanctions regime to promote UK values, combat cyber and terror threats, and counter chemical weapons proliferation.

On sanctions, the Review declares that the UK “will remain the most engaged non-regional partner on denuclearization by North Korea and on sanctions enforcement”. Regarding other state threats, the Integrated Review states that the UK will continue to put diplomacy at centre stage and utilise sanctions and international coalitions to respond to threats, particularly Russia. In responding to cybersecurity threats from individual or state actors, the UK intends to increase its Active Cyber Defence to tackle “the most pernicious forms of cybercrime, such as ransomware, including by blocking malicious online activity at scale”.

The Review also indicates that the UK will launch a second global sanctions regime on corruption in 2021, complementing the Magnitsky-style human rights sanctions regime, which will enable the UK to prevent those involved in corruption from utilising the UK financial system. The UK will also look to work proactively with allies with similar sanctions regimes, such as the US and Canada. There is also acknowledgement in the Review that the UK’s departure from the EU will allow for a swifter and more agile sanctions response. In a 22 March response to a parliamentary question on anti-corruption sanctions, Minister of State for Asia Nigel Adams stated that work is currently underway to consider adding such a sanctions regime, with a parliamentary update to follow.

In responding to financial crime, the UK will overhaul the existing SARS regime to ensure that the most crucial information informs police investigations into potential ML and other SOC-related financial activity. Furthermore, the UK aims to bolster the National Economic Crime Centre (NECC) and enhance the powers of the National Crime Agency (NCA) to better respond to such threats as cybercrime, fraud, and terrorist financing. This will include a £83 million investment into strengthening economic safety, of which £63 million will be directed specifically at tackling economic crime, including through SARS reforms. As is recommended by the independent review on SOC, released on the same day, the Integrated Review commits to recruiting 300 new police officers in the next year that will be exclusively dedicated to SOC investigations as part of the bolstering of regional organised crime units.
UK government releases Independent Review of Serious and Organised Crime

The UK’s Home Office published on 16 March an Independent Review of Serious and Organised Crime (SOC), which assesses current capabilities and funding needs for combatting SOC, including illicit financing and fraud, and finds that SOC threats are increasing both in scope and complexity. The Independent Review was commissioned in 2019 and undertaken by Sir Craig Mackey and offers a range of recommendations for increased innovation and collaboration by law enforcement and the government.

The review finds that law enforcement and the private sector are constrained in their ability to address SOC “with a set of tools that has not adapted to the evolving nature of crime, relying instead on a traditional view”.

Mackey calls for enhanced learning and innovation when it comes to being able to duplicate successful SOC investigations and prosecutions as part of a wider “substantial transformation proposal to restructure” government and law enforcement cooperation through what Mackey terms a “campus model” for connectivity.

The UK government also published on the same day ‘Global Britain in a Competitive Age’, an Integrated Review of Security, Defence, Development and Foreign Policy, which describes the government’s vision for the UK’s role in the world over the next decade and the actions that will be taken to 2025.

Recommendations from the Independent Review include:

- Establishing a UK Crime Campus (UKCC) within the National Crime Agency (NCA) and Regional Crime Campuses (RCC)
- Creating enhanced functions for the NCA that can be made available through the UKCC, including simplified funding for investigations and a single performance framework for investigative outcomes and threat levels
- Creating enhanced functions for regional organised crime units in coordination with the UKCC to ensure local priorities are granted and that risk assessments are shared more widely
- Strengthening NCA capabilities and UK work with foreign partners

UK OFSI quarterly asset freezing report

The UK Treasury’s Office of Financial Sanctions Implementation (OFSI) published on 19 March its quarterly report to parliament on the operation of the UK asset freezing regime between 1 October and 31 December 2020, mandated by UN Security Council resolution 1373.

During the reporting period, a new public designation was made under the Islamic State of Iraq and the Levant and Al-Qaeda regime (ISIL-AQ) regime, while three other designations were renewed under the Terrorist Asset-Freezing etc Act 2010 (TFA).

The OFSI notes that the UK government froze £9,000 in funds in six accounts under the TFA regime during the reporting period. In addition, £24,000 was frozen in three accounts under EU Regulation (EC) 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combatting terrorism, while £75,000 was frozen in 38 accounts under the ISIL-AQ regime.

Between October and December 2020, one licence was issued under the ISIL-AQ regime, while four general licences remained in force.
UK report on Xinjiang urges government to ensure supply chains are free from forced labour

The UK’s Business, Energy and Industrial Strategy (BEIS) Committee published its report on 17 March to parliament on Uyghur forced labour in Xinjiang province, urging the government to enhance its anti-modern slavery requirements in the Modern Slavery Act 2015 to ensure that products resulting from forced labour stay out of the UK’s supply chain. The recommendations include creating a working group within the BEIS Department that would produce a blacklist of companies that fail to prove that their supply chains are not linked to Uyghur abuse.

The Committee expresses concern that companies still cannot guarantee that their supply chains are free from forced labour

The report draws on Committee interviews with numerous entities, including Hennes & Mauritz AB (H&M), Nike Inc, TikTok, North Face Apparel Corp, and Boohoo.com UK Limited.

The Committee expresses its deep disappointment with The Walt Disney Company’s refusal to provide testimony on the matter, noting it finds that the company must face unanswered questions about its conduct in Xinjiang province relating to the production of its Mulan motion picture.

It further asserts that Boohoo’s minimal data about its supply chain linking China and the UK is unacceptable and urges corporations to conduct independent reviews of their due diligence policies.

The recommendations include

- The BEIS Department should commit to full transparency on how Official Development Aid is being used in China to ensure it is not used in connection with human rights abuse
- The Department should assess targeted sanctions options against international businesses and Chinese corporations involved in Uyghur forced labour and other human rights abuse
- The Department should publish a supply chain review of projects in China supported by the Newton Fund, including exact funding amounts for all organisations in China receiving support
- The UK government should strengthen supply chain transparency obligations and introduce steep financial penalties for non-compliance
- The Department should review the Company Directors Disqualification Act (1986) and determine if Modern Slavery Act 2015 breaches should disqualify company registration or director duties moving forward

The Committee goes on to express concern that companies still cannot guarantee that their supply chains are free from forced labour, despite widespread media reports of human rights abuses in Xinjiang.
UK committee report on UK-EU security and justice cooperation expresses concern

The UK House of Lords European Union Security and Justice Sub-Committee published on 26 March a report which examines the provisions in part three of the Trade and Cooperation Agreement (TCA) and establishes detailed arrangements to facilitate UK-EU cooperation in terms of policing and criminal justice measures.

The report underlines that the UK’s loss of access to the Schengen Information System leaves the most significant gap in terms of operational capacity.

The TCA was signed on 24 December 2020 by the UK and EU, creating a single framework covering a wide range of areas of economic activity and cooperation. Part Three of the TCA is centred on law enforcement and judicial cooperation in criminal matters and describes the arrangements established to enable effective cooperation on a range of policing and criminal justice measures.

The report welcomes provisions establishing further collaboration on protecting fundamental rights, the rule of law, and personal data. Additionally, the report commends the provisions on sharing of passenger record data between the UK and the EU, and for continued UK access to EU databases covering fingerprints and criminal records, as well as the agreement on extradition arrangements. The paper also highlights that the UK has agreed to continue its involvement with the EU’s policing and justice agencies, Europol and Eurojust, which reflects its commitment to maintaining a close relationship on law enforcement and criminal justice with the EU. As a result, the UK will continue to share data and expertise, but will no longer have a role in the management of the agencies.

However, noting the inevitable consequence of the agreement that it no longer ensures the “same level of collaboration” exercised pre-Brexit, the report underlines that the UK’s loss of access to the Schengen Information System (SIS II) leaves the most significant gap in terms of operational capacity, meaning that law enforcement officers no longer have immediate access to real-time information about the movement of criminals, missing persons and objects of interest. Furthermore, the report warns that the alternative system which the agencies will use instead, Interpol’s I-24/7 database, does not provide the same information at the same speed, as it is dependent on the willingness of EU states to re-upload the same information contained in SIS II.

The report further calls for caution on assessing the effectiveness of the part three arrangements, underlining vulnerabilities which might be caused by: (1) the complexity of the provisions, many of which are untested; (2) the provision covering justice and security which states that if either side “denounces” the European Convention on Human Rights, cooperation will stop or be suspended; (3) potential misalignments of UK and EU data protection rules, which could lead to the suspension, or even termination of the TCA; and (4) the operational effectiveness of the extradition arrangement, which replaces the European Arrest Warrant, which will need to be closely monitored.

The report is part of a series of five reports published by the House of Lords EU Committee which analyse the development of the UK-EU relationship, following the UK’s departure from the EU, and as established by the TCA. The other four reports focus on: (1) the institutional framework, namely the TCA’s provisions relating to governance and dispute resolution; and the impact of the TCA on (2) food environment, energy and health; (3) trade in services; and (4) trade in goods.

UK parliament press release...

Beyond Brexit: policing, ...
UK Independent Anti-Slavery Commissioner issues recommendations for law enforcement

The UK’s Independent Anti-Slavery Commissioner (IASC) released a report on 29 March urging law enforcement agencies to prioritise financial investigations of human trafficking and modern slavery. The paper asserts that the financial investigation components of these cases will likely yield more prosecutions due to financial evidence and increase the possibilities of victims receiving compensation.

Modern slavery is estimated to generate roughly $150 billion in annual profits, according to a 2017 International Labour Organisation estimate, with the paper urging law enforcement to make use of resources such as the Joint Money Laundering Intelligence Taskforce (JMLIT) and investigate suspicious activity reports (SARs) to better identify possible organised crime groups, understand group hierarchies, and identify victims. SARs can also be used to detect money laundering (ML) and trace it to criminal networks involved in trafficking.

IASC recommendations include:
- Utilising financial strategies early on in these types of cases and embedding financial intelligence officers in slavery and human trafficking task forces and investigation units
- Mapping and scoring organised crime groups early in the investigation and determining where financial investigation resources need to be allocated

UK Work and Pensions Committee urges FCA to step up fight against pension scams

The UK government’s House of Commons Work and Pensions Committee published a report on 28 March summarising the findings of its pension scams inquiry, urging the Financial Conduct Authority (FCA) to issue a plan to step up its fight against scams. The Committee also calls on the UK government to hold large tech corporations responsible for publishing and profiting from scam advertisements on their platforms, requesting that online harms be added to the Online Safety Bill.

According to the Committee, the true scale of pension scams is underestimated, citing the Pension Scams Industry Group’s estimate that almost £10 billion has been lost to such scams since 2015. To address this, the Committee stresses that Action Fraud should provide clear reporting guidance and effective tools for the industry, while online publishers should be required to ensure that any financial promotions that they communicate have obtained prior authorisation or are exempted from the financial promotions regime. The Committee also suggests Project Bloom be renamed the Pension Scams Centre and be offered dedicated funding and a pension scams intelligence database.

On 11 February, the Pensions Schemes Bill, which provides measures aimed at protecting consumers from pension transfer scams, received royal assent. According to the new provisions, pensions trustees and managers can block their constituents’ benefit transfer applications if they believe that the funds may be at risk of investment scams. The Committee welcomes the new act and recommends a review of the red and amber flags system be published within 18 months.

The government’s response to the Committee report is due by 28 May.
UK Finance fraud report calls for legislative measures to increase consumer protection

UK Finance published its "Fraud – The Facts 2021" report on 25 March, finding that financial institutions blocked £1.6 billion worth of fraud last year, roughly 67 percent of all fraud, but noting the rise in online scams during the Covid-19 pandemic, including the advertisement of phishing services and banking app impersonations for sale online. Unauthorised financial fraud losses involving payment cards, online banking, and cheques amounted to £783.8 million in 2020, five percent lower than the previous year. UK Finance urges the UK government to introduce legislative measures that will hold platforms responsible for fraudulent material posted on their sites and enhance consumer protection from scams.

In addition to card fraud typologies, the report covers a range of authorised push payment (APP) fraud, including CEO fraud, invoice and mandate scams, and investment scams, the latter of which rose 42 percent in value and 32 percent in volume from 2019. APP fraud increased by 5 percent to losses of £479 million, out of which £207 million was reimbursed. The number of CEO fraud cases increased by a quarter to 837, but losses dropped significantly to £10 million.

Scams in which criminals gained access to a customer’s bank account increased by almost 70 percent, to around 74,000 cases. The cost of unauthorised remote banking fraud rose to approximately £200 million, out of which £30 million was recovered. In addition, financial institutions were able to stop attempts to steal an estimated £400 million. The Dedicated Card and Payment Crime Unit in 2020 arrested more than 100 suspected fraudsters, some of whom allegedly engaged in pandemic-related fraud. UK Finance Economic Crime Managing Director Katy Worobec states in the report that the Banking Protocol, a bank branch rapid response programme, accounted for £45.3 million worth of fraud being halted and is currently being expanded to cover online and phone banking.

The report urges both large tech companies and the UK government to take more proactive measures in stopping fraud, noting that online platforms receive payment in some cases from fraudsters to post scam content. UK Finance urges the government to ensure that fraud and economic crime provisions are added to the Online Safety Bill to require big tech corporations to respond to current vulnerabilities being actively exploited by both individual criminals and organised crime networks.

UK Finance report summary
UK Finance fraud report

RUSI paper highlights rise in ransomware threats

RUSI published a paper on 29 March examining the impact of rising ransomware attacks on businesses. The paper, produced in conjunction with data collected by BAE Systems Applied Intelligence, considers emerging methodologies, including double extortion attacks, complications for businesses, such as paying ransoms to criminal groups subject to sanctions, and the role of cyber insurance. The report registers over 1,200 ransomware attacks against victims in 63 countries, with a 200 percent increase between June and October 2020, noting a correlation with the rise in remote working due to Covid-19.

RUSI notes that the size and scope of global ransomware attacks in 2020 was unprecedented, with many attacks involving double extortion attacks that both threaten the availability of information, also known as denial of business attacks, and the confidentiality of sensitive material, data, and/or intellectual property. While ransomware attack demands on individuals average at $500, the paper notes an instance of German IT company Software AG receiving a ransomware demand for $20 million.

RUSI press release
RUSI paper
FATF and Egmont Group publish report on trade-based money laundering risk indicators

The Financial Action Task Force (FATF) and the Egmont Group of Financial Intelligence Units released on 11 March a report on trade-based money laundering (TBML) risk indicators, with a view to helping private and public sector actors detect suspicious activity. The indicators have been developed based on a sample of the data received during a joint TBML project, presented in December 2020.

In terms of risk indicators, FATF stresses that private actors, such as banks and money value transfer services, designated non-financial businesses and professions, and small and medium businesses and large conglomerates, need to collaborate with public institutions to cross reference datasets. In addition, the list of indicators should be considered together with information available about a client gathered at different stages in the business relationship.

In a webinar hosted by the FATF on 18 March, project co-leader Tamara Pollard-Maier underlined that TBML is one of the most challenging types of illegal activities to investigate due to the wide range of goods that can be used in the process and noted that public-private partnerships represent “the most powerful weapon” to combat this type of financial crime. Australian Border Force inspector Daniel Strack underlined during the same event that investigations are severely complicated by the involvement of professional enablers such as lawyers in TBML.

Nedko Krumov, a senior officer within the Egmont Group Secretariat, emphasised that both reporting entities and investigators need to constantly update the technology they use, but advised against viewing this as the only solution. David Kane, the head of the World Customs Organisation’s anti-money laundering and combatting the financing of terrorism (AML/CFT) programme, stressed that the biggest challenge is identifying the point of conversion of money into goods. He also underlined that financial intelligence units (FIUs) need to find a balance between using top-tier technologies to go through large amounts of data and delivering diligent analysis and investigations.

Key TBML risk indicators include:

- Structural risk indicators, which include an unusually complex company structure, residence in a low-enforcement jurisdiction, an incompatibility between given address and the location of the business activity, the lack of an online presence, the absence of typical business activities such as payroll transactions, or senior staff appearing to obscure the actual beneficial owners

- Trade activity risk indicators, such as an inconsistency between executed operations and the stated line of business, involving numerous intermediaries from varied sectors, the use of economically unsound shipping routes, making transactions beyond the company’s financial capacity, or suddenly re-engaging in trades of high volume and value after a period of dormancy or immediately after the company’s creation

- Trade document and commodity risk indicators, which include contradictions between documents, vague descriptions of traded commodities, accepting prices that are unusually low or inconsistent with market value, using generic contracts for complex operations, or significant mismatches between the value of exports and the related financial inflows

- Account and transaction activity risk indicators, such as last-minute changes to payment arrangements, lack of correspondence between business activity and value of transactions, using accounts just for transactions to third parties without a clear commercial connection, or repeated transactions that are nearly below the reporting threshold

FATF/Egmont report
FATF press release
Egmont Group press release...
US FinCEN report on efforts to foster innovation and engage with compliance solutions

The US Treasury’s Financial Crimes Enforcement Network (FinCEN) issued a report on 26 March on its Innovation Hours Program (IH Program), which aims to shape and inform the regulator’s engagement with innovators of compliance solutions related to anti-money laundering (AML) and countering the financing of terrorism (CFT) pursuant to the Bank Secrecy Act (BSA) and amendments to the AML Act 2020.

FinCEN will establish formal BSA innovation security officer positions and two BSA advisory group subcommittees on innovation and technology as well as security and confidentiality.

Pursuant to its meetings with financial technology (FinTech) firms as part of the IH Program, FinCEN finds that financial institutions may not be sufficiently aware of technology solutions to address AML/CFT challenges, noting that reluctance to adopt new technologies may be linked to potential legal liability and data privacy concerns. Other identified concerns are associated with digital ID technology, maintaining the confidentiality of shared information, and a lack of anonymised financial data when reviewing criminal activity and transactions. FinCEN intends to host additional periodic workshops to facilitate innovation in the CVC area.

The report also includes the IH Program’s main achievements since inception, its impact on government policy and FinCEN priorities, and the program’s role in supporting the regulator’s plans to foster innovation. The IH Program was launched in 2019 as part of FinCEN’s broader 2018 Innovation Initiative, which focuses on ensuring US national security by promoting responsible financial services innovation to further the BSA’s purposes and its associated financial crime efforts.

On 23 March, the regulator held a virtual meeting to discuss BSA filing statistics for low dollar suspicious activity reports (SARs) in Arizona, New Mexico, Texas, Oklahoma, and Louisiana. The meeting gathered multiple stakeholders as part of the FinCEN Exchange to discuss SARs filing information and potential trends in suspicious activity.

---

Euro Banking Association issues report on CBDCs and stablecoins

The Euro Banking Association (EBA) published on 8 March a report on the recent developments in establishing central bank digital currencies (CBDCs) and stablecoins and how they can be integrated with the existing financial system. The report has been released for the use of EBA members only.

According to the factsheet accompanying the report, ongoing developments in the area of digital currencies could result in the further automation of payments and regulatory compliance, and may provide regulators with insights into financial flows and the management of risk. The EBA’s Cryptotechnologies, Smart Payments and Stablecoins Working Group stresses that the increased interest of public bodies in researching CBDCs should make technology companies and payment service providers (PSPs) alert to the possibility of using smart payments to expand their services.

According to the factsheet, the development of digital currencies could have an impact on both retail and wholesale payments, in domestic and cross-border transactions. The EBA advises companies to analyse compliance requirements and liquidity management practices to prepare for possible changes when using CBDCs or stablecoins.
ESMA report on the risks in the EU market for non-regulated cryptoassets

The European Securities and Market Authority (ESMA) published a 17 March trends, risks, and vulnerabilities report on the Covid-19 pandemic’s impact on financial markets, increased debt-related hazards, and risks associated with non-regulated cryptoasset investments. The EU regulator’s review includes discussions on the impact that regulatory requirements have on European money market funds (MMF) and the use of supervisory technology (SupTech) in providing retail investors with accessible information.

The ESMA reminds consumers that many cryptoassets remain outside the scope of financial regulations meant to offer safeguards and that perils persist amidst growing digitalisation, with increased cyberattacks and fraud during the pandemic. The ESMA highlights the growing need for operational and cyber resilience, welcoming the EU Commission’s 2020 digital finance package.

The ESMA identifies MMF vulnerabilities to structural risks, such as the pandemic-related liquidity shock of March 2020, and retail investor behaviour. The report highlights that, in some cases, the interaction between regulations requiring weekly liquid assets (WLA) to be above the 30 percent threshold and limited liquidity can prove problematic. When WLA sinks towards the limit, investors’ withdrawal requests can spike to avoid fees and gates, putting additional pressure on the funds.

Corporate Tax Haven Index published for 2021

The Tax Justice Network (TJN) published on 9 March its 2021 Corporate Tax Haven Index, a biennial ranking of jurisdictions according to their tax avoidance risk, which finds that the British Virgin Islands (BVI) is responsible for 6.4 percent of global corporate tax abuse risk.

The report notes that Organisation for Economic Cooperation and Development (OECD) members and their dependent territories are responsible for 68.3 percent of global corporate tax abuse risk. Three British Overseas Territories, namely the BVI, the Cayman Islands and Bermuda, rank first in the TJN’s Index, which also includes the United Arab Emirates (UAE) among the 10 largest enablers of corporate tax abuse. According to the report, “multinational corporations rerouted over $218 billion foreign direct investment through Netherlands and into UAE’s economy”.

The TJN alleges that the OECD failed to determine the majority of corporate tax havens evaluated by the index, claiming that countries classified as “not harmful” are responsible for $239 billion in lost corporate tax every year, while jurisdictions graded as “harmful” are accountable for only $5 billion.

TJN’s Tax Haven Index ranks all jurisdictions by their corporate tax haven index value and by their global scale weight. According to the latest Index, the top 10 enablers of global tax abuse are: the BVI, the Cayman Islands, Bermuda, the Netherlands, Switzerland, Luxembourg, Hong Kong, Jersey, Singapore and the UAE.
UN Panel of Experts report confirms probe into North Korean front company in the DRC

The UN Security Council (UNSC) released a report on 4 March by the UN Panel of Experts on North Korea which identifies North Korean activities taking place in the Democratic Republic of Congo (DRC) in apparent violation of UN sanctions, recommending two North Koreans and an apparent front company in the DRC be subjected to repatriation requirements.

The Panel of Experts investigation into North Korea sanctions evasion activities in the DRC cites and builds upon August 2020 and January 2021 reports by The Sentry, finding that statue construction company Congo Aconde SARL is a likely front company for North Korean state-controlled Korea Paeko Trading Corporation, an artwork exporter. Procuring statues from North Korea is banned pursuant to UNSC resolution (UNSCR) 2321 (2016).

The company reportedly built statues in two DRC provinces in 2018 and 2019, involving government contracts, with North Korean nationals Pak Hwa Song and Hwang Kil Su opening business accounts for the company in US dollars at a DRC branch of a Cameroon-based bank. The Sentry’s investigation, confirmed in the UN report, reveals that bank to be Afriland First Bank, which has also been identified by the US anti-corruption watchdog as an alleged laundering facilitator for US-designated Israeli mining billionaire Dan Gertler.

Three other individuals with known affiliations to the North Korean-controlled DRC company, Han Kyong Ho, Ri Yong Gwag, and Rim Chol, also opened accounts at Afriland, with the individual and business accounts registering over $400,000 in both deposits and withdrawals between February 2018 and September 2020.

The Panel of Experts reports that it is currently investigating Su’s involvement in projects in Cameroon and similar work by Korea Paeko Trading Corporation and affiliates in Rwanda, Nigeria, and Ghana.

In a 31 March response to the UN Panel of Experts report, The Sentry’s Senior Investigator John Dell’Osso said that the relative ease with which an apparent North Korean front company was able to set up US dollar bank accounts and access contracts in the DRC underscores the need for international bodies to help those involved with sanctions enforcement in the DRC and elsewhere in Africa.

EU to consider additional sanctions on Turkey

The EU High Representative for Foreign Affairs Josep Borrell published on 22 March a report on the state of play in the EU’s political, economic and trade relations with Turkey, which notes that the existing sanctions regime against Turkey’s illegal drilling activities in the Eastern Mediterranean could be extended and that additional restrictive measures could be imposed on entities and individuals.

The report was requested by the European Council in December 2020, when EU leaders asked for additional listings under the EU’s sanctions regime against Turkish unauthorised drilling activities in Eastern Mediterranean. The first designations under the sanctions regime were made on 27 February 2020 pursuant to Council Decision (CFSP) 2020/275 and targeted two executives of the Turkish Petroleum Corporation.

During an EU Council meeting on 25 March, EU leaders agreed that the EU is determined “to use the instruments and options at its disposal to defend its interests” in the Eastern Mediterranean.
RUSI details illicit North Korean oil networks

The Royal United Services Institute (RUSI) published a joint report with C4ADS on 22 March detailing the sanctions-evading oil network that supplies North Korea with refined petroleum products needed to maintain the country's economy and support its military and weapons of mass destruction (WMD) proliferation activities. The RUSI and C4ADS report finds that North Korea has been successful in its efforts to evade international sanctions and a UN Security Council (UNSC) cap on oil and petroleum product imports through organised crime networks and the black market in the region, which appears to have helped the country breach the UNSC import cap in 2020.

Singapore-based oil trading company the Winson Group is described in the report as being linked to likely ship-to-ship transfers of fuel that is suspected to be destined for North Korea.

A loosely organised criminal federation based along the coastal region of Fujian Province in China, particularly the city of Shishi, appears to be a hub for major actors involved in illicit North Korean fuel supply, with many of the same or similar organised crime organisations in the region linked to other regional smuggling operations, including tobacco, illicit wildlife products, and narcotics. The Singapore-based oil trading company the Winson Group is also described in the report as being linked to likely ship-to-ship transfers of fuel that is suspected to be destined for North Korea.

The report finds that diverging fuel regulations and pricing by nations in East Asia continue to allow fuel smugglers to redirect legal fuel supplies to North Korea, generating significant profits. Furthermore, Taiwan is presented as being a major throughway for fuel that ends up in North Korea, due in large part to relatively low petroleum prices. In addition to numerous fuel smuggling operations originating in Taiwanese ports or connected with physical addresses in Taiwan, the report notes that ship-to-ship transfers between legitimately flagged vessels carrying legally purchased fuel and ships that transport the smuggled fuel to North Korea often occur in Taiwanese waters.

The report's recommendations include:

- All nations should adopt similar anti-money laundering (AML) legislation to the US AML Act of 2020 in order to enact stricter suspicious activity reporting, promote information sharing, and expand monitoring of North Korean fuel smuggling
- Amend UNSC resolution (UNSCR) 2397 to allow for the seizure and impounding of vessels believed to be participating in North Korean fuel smuggling
- Investigate and target vessels and affiliated entities identified by member states, the UN Panel of Experts, and other organisations
- Allow Taiwan and other non-member states to participate in information sharing agreements to combat North Korean fuel smuggling
- Amend UNSCR 2375 to mandate that all member states prohibit their citizens or flagged vessels from participating in ship-to-ship transfers involving vessels bound for North Korea
- Create due diligence guidance for flag registry operations and ensure increased red flag reporting
- Financial institutions should diversify KYC and due diligence efforts to screen for risks involving shipping entities and fleet activities

| RUSI notice |
| RUSI report |
| UNSCR 2375 (2017) |
UN Panel of Experts finds Libya arms embargo “totally ineffective,” EU extends IRINI

The UN Panel of Experts on Libya published its final report on 17 March which describes the international arms embargo on Libya as “totally ineffective”, finding that multiple countries are routinely bypassing embargo security vessels to supply combative parties to the conflict with weaponry. The report also recommends that the UN Security Council (UNSC) authorise the UN Committee on Libya to begin designating embargo-violating aircraft in addition to ships, as well as engaging in flag de-registration, landing bans, and overt flight bans.

In its assessment of international sanctions on Libya, including the arms embargo, the Panel of Experts finds that member states supporting competing groups in the ongoing conflict are violating the embargo in a manner that is “extensive, blatant and with complete disregard for the sanctions measures” and “their control of the entire supply chain complicates detection, disruption or interdiction”. The report goes on to note “a persistent lack of transparency in beneficial and legal ownership”, identifying only a single case of non-compliance that resulted in asset freezes for an entity. For individuals, the report finds that asset freezes and travel bans thus far remain ineffective.

The report sheds further light on the network of shell companies that has been utilised by some, including Erik Prince, brother of the former secretary of education under the Donald Trump administration and former head of Blackwater USA, to provide equipment to the Libyan National Army (LNA) and other armed groups. In one example detailed in the report, Prince’s company is believed to have sold an aircraft used for reconnaissance and intelligence gathering to a Delaware-based company also under his control before it was sold to an Austrian company, registered in the Netherlands, and fitted with surveillance equipment. The aircraft was then sold to a company controlled by an associate of Prince that contracts with LNA Commander Khalifa Hafer, where it remained as of December 2020. Prince is accused directly in the UN report of violating or assisting others in violating the 2011 arms embargo.

Acknowledging the UN report’s concerns, EU High Representative for Foreign Affairs Josep Borrell announced on 21 March that the bloc will continue the Operation IRINI arms embargo naval enforcement mission for a further two years. Responding to the UN Panel of Experts report, Borrell stated that the findings are “fully consistent with our own assessment and confirms the need for an Operation like IRINI, the only actor implementing the arms embargo and serving at the same time as a deterrent” and adding that the findings indicate that efforts must be stepped up. In remarks to the press on 19 March, Borrell stated that the Operation has thus far conducted eight vessel inspections, leading to illegal cargo and illicit fuel seizures, made nearly 100 approaches, and haled vessels over 2,300 times.

On 26 March, the EU Council formally extended Operation IRINI until 31 March 2023 following the Political and Security Committee’s strategic review, adding more detailed provisions for disposing of arms and other items seized by the mission. Secondary tasks include monitoring illicit fuel exports from Libya, assisting in training the Libyan Navy and Coast Guard, and contributing to disrupting opportunities for trafficking networks with air patrols. The mission currently consists of four vessels and six aircraft along a nearly 1,800-kilometer coastline.
Switzerland’s FINMA annual report includes details on AML inspections

The Swiss Financial Market Supervisory Authority (FINMA) published its 2020 annual report on 25 March, announcing that the regulator carried out its full supervisory activity in addition to Covid-19 pandemic-related regulatory actions and declaring that Swiss financial institutions have continued to function robustly throughout the pandemic. The report notes, however, that some supervised institutions that it encountered in 2020 are not properly exercising appropriate due diligence concerning clients that pose money laundering risks.

Despite the pandemic lockdowns, FINMA reports that it conducted approximately 100 on-site bank supervisory reviews, a 6 percent increase from 2019. The authority also undertook 628 investigations and 33 enforcement proceedings. The report notes that while banks largely demonstrated over the past year that they took reporting obligations for suspicious activity seriously, FINMA found that some institutions inferred that instances of criminal proceedings being dropped led to an assumption that related assets were legal, leading to reminders that monitoring must continue in such cases to identify possible suspicious activity.

FINMA also reports that it identified some instances of Swiss financial institutions over relying on the stipulation that contracting partners subject to adequate levels of anti-money laundering and counter financing of terrorism (AML/CFT) can be deferred to for supervision. In these cases, FINMA found that some Swiss banks entered such relationships with institutions whose status as a bank was uncertain and were thus unable to provide beneficial ownership information when fraud, insider trading, or tax evasion suspicions involving offshore clients arose. The authority issued reminders to the relevant Swiss financial institutions that they must make such supervisory clarifications on a case-by-case basis, not only when general ML supervisory arrangements are assumed to be in place within a given foreign jurisdiction.

UK publishes annual terrorism report

The UK’s independent reviewer of terrorism legislation Jonathan Hall published on 23 March his report on the operation of the Terrorism Acts 2000 and 2006, which recommends that further consideration is given to whether law enforcement agents should receive additional powers to compel encryption keys in counter-terrorism investigations.

The document highlights a series of scenarios regarding the risks faced by aid agencies of committing terrorist funding offences in difficult jurisdictions, such as access fees or a monopoly on the supply of fuel either directly or through proxy companies. The report welcomes the progress made on developing a prosecutorial guidance by the Attorney General on the use of proscription offences against overseas aid agencies.

Hall recommends that the Home Office and the National Crime Agency consult with aid agencies and develop guidance on Section 21ZA of the Terrorism Act 2000 concerning the defence against terrorist financing offences based on consent in connection with humanitarian assistance.

The report notes that the investigation and prosecution of terrorism offences “looks and feels different in Northern Ireland from the rest of the UK” and recommends increasing transparency and public understanding of the approach taken towards countering Northern Ireland-related terrorism.
US State Department releases country reports on human rights practices

The US Department of State’s Bureau of Democracy, Human Rights and Labour released on 30 March its 2020 country reports on human rights practices, which provide detailed information about the human rights situation in nearly 200 countries and territories, and which require the imposition of sanctions against perpetrators of human rights abuses.

The reports include an assessment of human rights abuses against Uyghurs and other religious and ethnic minority groups in China’s Xinjiang region and condemn the authorities for “crimes against humanity” and “genocide”. In addition, the report on Russia notes that national security forces have been involved in numerous human rights abuses against opposition politicians, journalists and anti-corruption whistleblowers, and in relation to Ukraine’s Donbas region. Similar abusive practices were also identified in jurisdictions such as Belarus, Uganda and Venezuela.

During a press conference, the Secretary of State Antony J. Blinken emphasised the actions taken by the US with regard to the situation in Myanmar, including designations made against those responsible for the 1 February military coup. He stated that countries continue to “have significant investments in enterprises that support the Burmese military” and called for countries to block financial support.

According to Blinken, “the trend on human rights continue to move in the wrong direction” and more efforts are required for promoting and protecting human rights, including by imposing economic sanctions and visa restrictions on all human rights violators. Blinken notes that the pandemic has had a negative impact on individuals and groups that are particularly vulnerable to abuses and has enabled governments to restrict rights and fundamental freedoms and to “consolidate authoritarian rule”.

Blinken stated that the Department of State will continue to work with the US Congress in order to hold perpetrators accountable for abuses by applying existing legislation, such as the Global Magnisky Act and the Hong Kong Human Rights and Democracy Act, as well as by allowing new authorities to sanction human rights violators.

UK publishes cybersecurity breaches survey

The UK government released on 24 March its cybersecurity breaches survey 2021, revealing that 39 percent of businesses and 26 percent of charities reported experiencing a cyber-attack or cybersecurity breach during the past 12 months. The report also finds that businesses using security monitoring tools and running updated anti-virus programs have dropped by five percent, with the government urging businesses to adopt more resilient measures.

The survey results show that medium and large businesses and high-income charities were frequent targets of breaches or attacks in this period, at 65, 64, and 51 percent, respectively, as has been the case in previous reporting years. However, less businesses identified cyber intrusions this year than the previous year, which the report attributes in part to lower trading activity during the Covid-19 pandemic. Phishing attacks remain the most prevalent form of cyber-attack, followed by impersonation scams. Roughly one in four of the businesses and charities that reported attacks in the last year experienced at least one breach or attack per week.
UK FCA addresses market abuse forum

The UK’s Financial Conduct Authority (FCA) published on 8 March a speech that Enforcement and Market Oversight Executive Director Mark Steward delivered on 25 February to the Expert Forum: Market Abuse 2021 in which he shared recent successes and enforcement actions by the regulator.

Speaking via webinar, Steward told the forum about recent FCA activities, including the introduction of the Potentially Anomalous Trading Ratio (PATR) in September, a new market cleanliness measure which focuses “on the underlying trading behaviour around specified price sensitive announcements and assesses whether the behaviour can be deemed anomalous”. Other recent initiatives include a new short selling reporting approach that allows for short position reporting via the FCA’s Electronic Submission System (ESS). Steward said that this measure, as part of “the virtue of the transparency regime” in the UK, can help prevent market distortions, as short positions over 0.1 percent must be reported to the FCA and all positions over 0.5 percent must be publicly disclosed daily.

The FCA executive stated that the agency saw a 34 percent increase in transactions and transaction reports in 2020, despite Brexit and the Covid-19 pandemic, noting that it was accompanied by a reduction in suspicious transaction and order reports (STORs). Nevertheless, he also noted that STOR levels have returned “to levels we would expect to see” and is not concerned by the relatively low levels compared to previous years given “the unprecedented trading conditions”. Furthermore, Steward said that proactive surveillance as well as FCA investigation work has led to less trading by some individuals who had prompted large amounts of suspicious transaction and order reports.

FCA speech

Israeli geothermal operator Ormat Technologies allegedly engaged in corruption


According to Hindenburg, former Ormat employees and business partners have disclosed that the company routed sales of Guatemalan energy assets through an undisclosed related entity, Comercializadora Comertita, set up by a former employee of the company. The same entity was allegedly involved in funneling energy rights to government officials responsible for approving Ormat’s deal in Guatemala in 2003.

Additionally, in Kenya, the company purportedly obtained a public procurement contract after meeting with Ken Tarus, chief of Kenya Power and Lighting and former Kenyan president Daniel Arap Moi and paying contractors tied to corrupt government officials. Meanwhile, Honduras’ state energy company allegedly agreed to enter an uneconomical deal in 2010 with Geoplatanares PPA, a company later operated by Ormat, and was purportedly bribed to do so through an opaque entity, Bidle Trading Inc.

Ormat General Counsel Hezi Kattan, Chief Compliance Officer Doron Blachar, along with Board Member Ravit Barniv, have been under investigation in Israel since 2018 for their alleged involvement in bribing Kenyan and Guatemalan officials while in their previous positions at Israeli construction company, Shikun VeBinui Ltd.

Ormat issued a statement on the same day that Hidenburg’s claims “are inaccurate and filled with innuendo in an attempt to mislead investors”. Ormat stated that it is aware of claims being investigated in Israel regarding Barniv and Kattan, which relates to their conduct at another company.
US reversal of Dan Gertler licence underscores challenges to anti-corruption efforts in the DRC

The US Treasury’s 8 March revocation of an unpublished general licence granted to Israeli mining tycoon Dan Gertler closed a two month chapter that has brought heightened scrutiny upon the US government amid questions over reprieves issued in the final days of the Donald Trump administration. The billionaire miner has, according to the US government’s latest revocation and initial US Treasury’s Office of Foreign Assets Control (OFAC) December 2017 designation, “engaged in extensive corruption” in the Democratic Republic of the Congo (DRC), harnessing a partnership with former DRC president Joseph Kabila that allegedly caused losses to the DRC of “over $1.36 billion in revenues from the underpricing of mining assets that were sold to offshore companies linked to Gertler”. Investigative reporting, including by the George Clooney and John Prendergast US-based Africa-centric anti-corruption watchdog The Sentry, has detailed in recent years the flow of corruption proceeds through and out of the DRC and offered recommendations for policymakers to assist due diligence by financial institutions. Significant challenges to due diligence efforts by regional and multi-national banks in the DRC include the extensive and intricate web linking companies under Gertler’s control, local regional banks, DRC political leaders, a series of middlemen across Europe and the Middle East North Africa (MENA) region, and companies such as Switzerland-based Glencore plc engaged in the rare mineral trade.

The Financial Crime Digest spoke with The Sentry’s Sasha Lezhnev, Deputy Director of Policy and Lead Investigator for the Democratic Republic of the Congo and Megha Swamy, Deputy Director for Illicit Finance Policy and Lead Banking and Finance Investigator, in the days leading up to the Joe Biden administration’s reversal of the January reprieve. The two investigators discussed the Gertler case with Aperio and shed light on regional due diligence challenges as well as the likely positive changes brought by the Financial Action Task Force (FATF) standards, which the DRC has yet to adopt, and improved legislative efforts with the aim of a future free of corruption in the DRC’s financial services industry.

General licence granted during Trump’s final days in office

The 15 January general licence from OFAC granted Gertler and his entities a reprieve from his 2017 designation, allowing for financial institutions to legally unfreeze assets belonging to him or any designated entities associated with him and resume transactions for at least one year. The licence issuance reportedly came as a result of involvement by former Secretaries of Treasury and State Steve Mnuchin and Mike Pompeo, as well as lobbying efforts by Alan Dershowitz, the defence attorney best known for representing such figures as Jeffrey Epstein, Harvey Weinstein, and former US president Donald Trump. Lezhnev states it was likely “a combination of efforts that were done in a non-transparent
secret manner that is very disappointing and concerning”. Citing statements by former US Special Envoy to the DRC J. Peter Pham and former Assistant Treasury Secretary Marshall Billingslea, both Trump administration appointees, Lezhnev describes the reprieve as an action that “undermines US sanctions, national security, and national interests and really threatens to destabilize Congo at a very critical time when a new government is being formed”.

The New York Times reported in February on the outsized presence of Israeli lobbying efforts playing a significant role in Gertler’s reprieve, citing two 2001 UN reports linking Gertler to DRC efforts to gain access to the Israeli arms market in exchange for diamond exports, making Gertler and Kabila’s relationship an early example of conflict diamonds as a geopolitical concept. A spokesperson for Gertler, Aron Shaviv, who has denied Gertler’s engagement with any corrupt activities in the region, previously served as campaign manager for Israeli Prime Minister Benjamin Netanyahu’s successful 2015 re-election campaign, underscoring Gertler’s close ties to Israeli politics. Furthermore, Gertler himself served as Kabila’s official emissary to the US in 2002, with Kabila informing then-president George W. Bush that Gertler would represent the country’s interests in conveying “the true intentions and motivations of my country to rid itself of destructive occupation, corruption, and terrorism”, and stating that Gertler himself had convinced Kabila to collaborate with the US.

March reporting by Bloomberg indicates that then-Israeli Ambassador to the US Ron Dermer and Mossad Chief Yossi Cohen held multiple meetings with US officials making the case for Gertler. While close connections to US and Israeli politics were fundamental to Gertler gaining the licence in January, so too was his wider network in maintaining a steady flow of illicitly sourced funds through the international financial markets even after his 2017 designation.

Prior undermining of Global Magnitsky sanctions

Amid the lobbying efforts of Trump administration officials to grant Gertler a licence, anti-corruption watchdog Global Witness in July 2020 detailed the lengths to which Gertler and numerous associates have allegedly gone to evade US sanctions utilising shell companies and regional banks. In conjunction with the Platform for the Protection of Whistleblowers in Africa (PPLAAF), Global Witness’ report highlighted the role of a Kinshasa branch of the Cameroon-based Afriland First Bank as a conduit for the laundering of corrupt funds. In one instance, a known Israeli friend of Gertler’s, Shlomo Abibassira, allegedly made cash deposits totalling $6 million into a likely shell company, despite having no stated business interests in the region.

Lezhnev identifies a shift towards Europe following the 2017 and 2018 designations. “Gertler’s companies were set up in multiple jurisdictions”, he said. “As soon as US sanctions were put on he figured out a way to get paid in Euros, using banks in non-US locations”. According to Global Witness, Abibassira’s involvement netted $19 million in cash deposits, which reportedly made its way to one of three companies incorporated by Elie-Yohann Berros, a French citizen who is registered as the owner of another company bearing the same name as one of Gertler’s entities. A local businessman in the DRC reportedly set up ten companies and deposited €11 million after the 2017 designation, all of which point to Gertler as beneficial owner.

Aperio Intelligence France Branch Head and corporate intelligence analyst George Voloshin notes that “there was clear complicity in Congo and other places where alleged sanctions evasion originated through a network of proxies”. Global Witness claims that it was through these companies that such entities as Glencore, Sicomines, and the Eurasian Resources Group (ERG) could continue doing business with Gertler while being able to issue public denials of any connection. Voloshin told the Financial Crime Digest that through this step in the money chain, such networks can effectively undermine US sanctions regimes.

“The US Treasury can do nothing about it, apart from going after sanctions busters”, Voloshin adds. “The problem lies within FIs themselves, how well they manage sanctions risk and how good they are at curbing complicit behavior”. The foundation for these business operations, as is the demonstrated case with many of Gertler’s masked entities, is the ability to engage in transactions at the local banking level. Voloshin notes that while business operations in Europe by shell companies indirectly controlled by Gertler do not always constitute a US sanctions violation, the onus remains on FIs themselves to determine whether a violation is taking place.

“Those that process or are somehow engaged in facilitating transactions on his behalf must conduct proper DD to ensure that US sanctions are not breached”, Voloshin states. “The main risk is to inadvertently process USD transactions, which is only possible with the involvement of a US-based correspondent bank”.

Both Global Witness and The Sentry have pointed to loopholes in the regulatory framework and practices of DRC financial institutions that have allowed money launderers to take advantage of lax enhanced due diligence, AML checks, and KYC standards. Swamy adds that while the current financial landscape is concerning, she sees positive steps being taken, including clear indications from the DRC banking community that they want to improve. “We hear they are seeking resources both on the regulatory side and on the
banking side as well”, Swamy explains. “There is increased engagement at the global banking level as well on these issues”. This can partially be attributed to the influence of investigative reports by The Sentry and other organisations highlighting loopholes and raising the Congolese banking profile. Nevertheless, she notes, pointing to Afriland as a primary example, “there are deep rooted systemic issues that need to be addressed”.

Local banks have, at times, materially benefitted in the short term from the operations of shell companies laundering illicit proceeds. Afriland’s annual profits increased by nearly 350 percent in 2018 by maintaining more than a dozen Gertler-affiliated entity accounts, according to Global Witness. However, the processing of transactions by clients like Gertler and his network of affiliates by local banks also places such financial institutions in the crosshairs of de-risking by large multi-national banks based in Europe and North America.

Aperio reported on 25 January about the benefits that can result from international financial institutions engaging with local central African banks rather than withdrawing support and cutting ties. The Sentry’s investigators agree wholeheartedly, with Swamy stressing that “a functional, clean banking sector is crucial to any country’s economy”, describing de-risking in central Africa in particular as “a real problem and a real hindrance to access to banking service for a vast majority of the population and for businesses”. Critical to these efforts are managing and carefully highlighting risks so that multinational banks can adjust their own internal controls and conduct enhanced due diligence efficiently and effectively. Closer cooperation, Lezhnev states, is also key to supporting the “significant legitimate business sector in the DRC and the region and that needs responsible investment to continue to grow and really develop the country and help alleviate poverty”.

FinTech can also play a crucial role in the effectiveness of local banks in Central Africa, according to a 2019 International Monetary Fund (IMF) report which asserts that FinTech can remove information barriers, take pressure off correspondent banking relationships, and improve the security and transparency of payment systems. But technology alone will not bridge the gap between Central African banks and larger counterparts in the US and Europe.

The IMF recommends regional and national policymakers address such infrastructure challenges as internet and electricity access, confront the race between fast innovation and slower regulation, and apply FinTech-related benefits on a wider scale to develop digital economies and implement structural reforms.

**Paving the way to a corruption-free financial sector in Central Africa**

With challenges to due diligence and KYC efforts abundant in DRC-area financial institutions, Swamy points to a combination of political will, regulators, and banks as crucial for building a better AML framework as well as raising the integrity of the region. She adds that more communication and guidance from regulators is needed to start seeing improvements and asserts that technical assistance and public-private partnerships will also be key. In terms of recent successes in the region and potential for the DRC, Swamy points to FATF standards and mutual evaluation reports.

**The most significant consequence of this brief period in 2021 would likely have been felt by financial services firms, especially those holding funds belonging to Gertler or his designated entities**

Aperio Intelligence Head of Africa and ESG Simon Jennings concurs that steps such as implementing FATF standards are crucial to overcoming vulnerabilities to money laundering, corruption, and political influence. “Adopting international best practices like the FATF standards would not only help the financial sector implement effective AML measures, and controls with regard to politically exposed persons but, crucially, also facilitate the country’s engagement with the international financial system and support higher levels of foreign direct investment”, Jennings states.

As for new approaches under the Biden presidency, Swamy’s 31 March briefing by The Sentry urges the new US administration to harness provisions of the recent AML legislation package included in the National Defence Authorization Act (NDAA) to put greater financial pressure on corrupt actors in the region. Among these are opportunities for the Financial Crimes Enforcement Network (FinCEN) to engage in deeper public-private information sharing and implement a beneficial ownership registry to better identify those involved in money laundering facilitation. Furthermore, her briefing recommends that the US cast a wider net with future anti-corruption sanctions to target entire networks rather than individuals and, when possible, to synchronise those designations with allies for greater impact.
The Sentry’s 31 March briefing urges the new US administration to harness provisions of the recent AML legislation package to put greater financial pressure on corrupt actors in the region

A significant challenge that lies ahead on the road to corruption-free banking is raising awareness of the role global financial services play, often inadvertently, in supporting corrupt actors that take advantage of developing African economies and the link between global finances and crimes against humanity. Lezhnev states that educating the wider public about the international web involved in making corrupt proceeds laundering possible, as well as the role enhanced due diligence can play in preventing it, is a crucial element of reform. “It’s not some random African bank sending money to another random African bank”, Lezhnev adds. “Actually, it turns out that many of the corrupt transactions are done in US dollars and they go through a US correspondent bank and so there is a lot of connectedness. However, very few people know about that, so we’re trying to make people aware of those things”.

Gertler’s licence reversal by a new administration a mere two months after issuance represents a rare incident for OFAC, with Voloshin acknowledging that it is very uncommon for the Treasury Department to make such a quick turnaround. However, he asserts that the most significant consequence of this brief period in January, February, and March 2021 would likely have been felt by financial services firms, especially those holding frozen funds belonging to Gertler or his designated entities. “I imagine the US firms concerned lived through a pretty chaotic period as they had to unfreeze the funds and later freeze them again if they were still within US jurisdiction”, Voloshin states. “Depending on how smooth the process was, those that struggled to identify and re-freeze the assets within hours would want to embark on internal reviews to rectify relevant operational deficiencies”.

To ensure a more effective sanctions regime moving forward, Voloshin states that the US could exert greater pressure on Gertler, his network, and similar types of actors through imposing secondary sanctions, a move that would effectively isolate targets from the global financial system. But he is quick to note that secondary sanctions are not implied by the GLOMAG regime. Thus, as was the case following the 2017 designations, the burden remains on banks and financial service providers to carry out their own intelligence work to ensure that they are neither breaching sanctions regimes nor inadvertently supporting the movement of corrupt proceeds.

While any FI is free to conduct due diligence on their own, many engaging with customers in high-risk jurisdictions will find the benefits that come from working with financial intelligence firms such as Aperio that are home to regional specialists and expert at tracing financial webs. “Through its source networks in countries like the DRC, Aperio Intelligence conducts enhanced due diligence for a wide range of banking and corporate clients about high-risk customers and third parties”, Jennings states. “Our reports serve to inform clients’ decision-making or broader dialogue with regard to financial crime, sanctions and reputational risks”.

By David Shoup, Junior Editor at Aperio Intelligence
david.shoup@aperio-intelligence.com
EBA takes steps to address de-risking practices

The European Banking Authority (EBA) issued a press release on 22 March detailing its recent steps to address de-risking by financial institutions based on evidence gathered from its call for input.

The three regulatory instruments published by the EBA in March 2021 to address de-risking practices clarify that compliance with anti-money and counter terrorist financing (AML/CTF) obligations in EU law does not require financial institutions to refuse, or terminate, business relationships with entire categories of customers considered as presenting a higher ML/TF risk.

Through the issuance of the instruments, the EBA has also set out steps that financial institutions and competent authorities should take to manage the risks associated with individual business relationships.

The EBA launched a consultation on 17 March on changes to its guidelines on risk-based AML/CFT supervision.

The EBA states that it will continue to monitor and assess the scale, impact and reasons for de-risking, and consider the extent to which the current legal and regulatory framework is sufficient to address the problem.

The three instruments are

- The EBA published its 2021 Opinion on ML/TF risks in the EU financial sector on 3 March 2021, in which it observes that de-risking is a continuing trend that has implications from an ML/TF risk, consumer protection and financial stability point of view and sets out a number of actions competent authorities should take to understand the drivers, scale and impact of de-risking in their sectors.

- The EBA issued its revised ML/TF Risk Factors Guidelines on 1 March 2021, which clarify that the application of a risk-based approach to AML/CFT does not require financial institutions to refuse, or terminate, business relationships with entire categories of customers that are considered to present higher ML/TF risk.

- The EBA launched a consultation on 17 March 2021 on changes to its guidelines on risk-based AML/CFT supervision. The proposed guidelines require competent authorities to take stock of the extent of de-risking in their jurisdiction and address de-risking in their ML/TF risk assessments.
EBA publishes final revised guidelines on money laundering and terrorist financing risk factors

The European Banking Authority (EBA) published on 1 March final revised guidelines on money laundering and terrorist financing (ML/TF) risk factors, with revisions taking into consideration EU AML/CFT legal framework amendments as well as emerging risks. Addressing both regulatory authorities and financial institutions (FIs), the revised guidelines aim to support legal supervision efforts and customer due diligence (CDD).

CDD and business-wide risk assessment requirements are reportedly strengthened in the revised guidelines, with new clauses addressing the identification of beneficial owners, solutions for verifying customer identities, and compliance guidelines for FI enhanced CDD for transactions involving high-risk jurisdictions. Other new guidelines address crowdfunding platforms, account information service providers (AISPs), payment initiation service providers (PISPs), and currency exchanges. Corporate finance guidance and more detailed risk advice on TF is also included.

The EBA’s revised guidelines also highlight the need for supervisory authorities and FIs to enhance their understanding of tax crimes, as set out in the EBA’s report on competent authorities’ approaches to tackling market integrity risks associated with dividend arbitrage schemes.

Following the implementation and coming into force of Directive (EU) 2018/835 (the EU’s Fifth AML Directive) as of 10 January 2020, the new guidelines replace in full the previously issued EBA ML/TF guidance.

UK NCA guidance on filing good quality SARs

The UK National Crime Agency (NCA) published on 5 March updated guidance for anti-money laundering (AML) supervisors, including the self-regulatory organisations overseen by the Office for Professional Body Anti-Money Laundering Supervision (OPBAS), on how to improve the quality of suspicious activity reports (SARs).

The guidance, drafted in collaboration with OPBAS, is directed at all entities that must submit SARs under the Proceeds of Crime Act 2002 (POCA) and Terrorism Act 2000 (TACT). The document explains how regulated entities should justify, complete and structure their SARs, and how to refer to previous filings.

All reporters should

- Explain the suspicion in a clear and concise manner, include all relevant information in chronological order, and avoid jargon and acronyms
- Ensure service descriptions and technical details are accompanied by a brief synopsis
- Explain the reason for suspicion, including persons involved and their role, and insert a description of the property and estimated value
- Provide all the required details even where the reporter includes a previous SAR reference number

- Mention all the glossary codes/alert references that the reporter believes are relevant
- When seeking a defence against a principal money laundering offence, regulated entities need to detail how they came to know or suspect involvement in dealing with criminal property, what act they want to carry out, describe the asset in question and its location and provide information about the entity associated with it
ESMA suggests amendments to Transparency Directive in light of the Wirecard scandal

The European Securities and Markets Authority (ESMA) announced on 3 March that it has sent a letter to the European Commission (EC) with proposals to improve the enforcement of the financial information framework, in light of the Wirecard AG fraud case.

The ESMA suggests that Directive 2004/109 on harmonising transparency requirements in relation to information about securities’ issuers (the Transparency Directive) is amended to eliminate confidentiality requirements that prevent an effective exchange of information between national competent authorities (NCAs) and designated authorities. In addition, legislation should be revised to clarify which competent authority is ultimately responsible for enforcing the Directive.

In addition, the Directive should mandate all three European supervisory authorities to develop regulatory technical standards (RTS) on cooperation and information exchange between accounting enforcers, audit oversight bodies, prudential supervisors and anti-money laundering and countering the financing of terrorism (AML/CFT) supervisors.

The ESMA points out that the evaluation of the delegation and designation models should be made on a regular basis, while NCAs, designated authorities and/or delegated entities and their staff should be independent from market participants. In addition to this, delegated entities, designated authorities and NCAs should be empowered and the ESMA’s 2015 guidelines on alternative performance measures (APMs) should be qualified as part of the enforcement of the financial information framework.

On 1 March, the ESMA’s Securities and Markets Stakeholder Group (SMSG) published a series of recommendations to address the irregularities identified in the Wirecard case, which include a clear delimitation of accounting fraud-related competences between authorities and clarification of the circumstances under which a short selling ban or restriction can be enacted. Additionally, the ESMA should improve the scrutiny of market manipulation allegations and issue a report “to pave the way for changes to the level 1 Short Selling Regulation”, while the EC should reconsider the auditors’ mission and framework.

UK publishes CRM Code review roadmap

The UK Lending Standards Board (LSB) published on 1 March a roadmap that outlines the activities the LSB will undertake in 2021 in relation to its review of the Contingent Reimbursement Model Code for authorised push payments (APP) scams (CRM Code).

The roadmap includes updates to the wording of the CRM Code, stemming from responses received to the consultation and signatories, publication of the CRM review report, the implementation of recommendations listed in the CRM report, a call for input with regards to emerging scams, expanding the scope to other business models and sending/receiving bank liability, as well as ongoing engagement with stakeholders.

The LSB also announced that it has begun work on a follow-up review in regards to the approach to the reimbursement of customers. The review’s outcomes are due to be published later this year.
FATF issues guidance on applying a risk-based approach to AML supervision

The Financial Action Task Force (FATF) published on 4 March new guidance on applying a risk-based approach to anti-money laundering and countering the financing of terrorism (AML/CFT) supervision, designed to help supervisors focus their resources on sectors where the risks are highest.

According to FATF, a robust risk-based approach includes appropriate strategies to address the full spectrum of money laundering and terrorism financing (ML/TF) risks, from higher to lower risk sectors and entities, and measures to effectively mitigate relevant risks on an ongoing basis, in line with national priorities.

The guidance encourages supervisors to improve their approach to detecting and preventing illicit financial flows by working across the government and together with the private sector to develop a better understanding of the assessed risks. Consistent with a risk-based approach, supervisors are expected to provide reporting entities with flexibility and clear communication of expectations in the Covid-19 context.

**An effective risk-based supervisory process should include**

- The implementation of a sound risk assessment which identifies and measures ML/TF risks, and enables effective supervisory intervention to address any elevation in risks, as well as emerging ML/TF risks
- Maintaining a good understanding of ML/TF risk exposure of the regulated sectors and entities by undertaking a supervisory risk assessment (SRA), in line with the national risk assessment
- Developing and implementing supervisory strategies, informed by the SRA, which sets clear objectives for AML/CFT supervision, provides adequate coverage and monitoring of all entities and sectors, and includes an approach to the application of supervisory tools
- Most supervisory resources should be allocated to the higher ML/TF risk areas, but supervisory strategies should describe the approach for areas of lower risk
- Providing guidance and feedback to entities on their AML/CFT policies, directing remedial actions and applying the sanctions toolkit in a dissuasive and proportionate manner
- Coordinating with other competent authorities, including the financial intelligence unit, law enforcement agencies and other regulators, as well as its foreign counterparts to share information

---

**UK to review wildlife crime laws and enforcement**

The UK Department for Environment, Food and Rural Affairs launched on 2 March an assessment of UK wildlife and forest crime law and enforcement, based on the International Consortium on Combating Wildlife Crime (ICCWC) toolkit.

The ICCWC will work with the UK until August to evaluate wildlife crime legislation, policing structures, criminal justice responses and prevention efforts, in line with its 2012 Wildlife and Forest Crime Analytic Toolkit. DEFRA’s Under-Secretary Rebecca Pow believes that there has been “tremendous progress [in] tackling wildlife crime” but there is more to be done to “reduce these horrific crimes”.

The ICCWC, formally launched in 2010, was established by representatives of the Convention on International Trade in Endangered Species of Wild Fauna and Flora, Interpol, the UN Office on Drugs and Crime, the World Bank and the World Customs Organisation.

---

**UK government press release**

**Wildlife and Forest Crime...**
UK OFSI revises guidance on monetary penalties for breaches of financial sanctions

The UK HM Treasury’s Office of Financial Sanctions Implementation (OFSI) published on 10 March updated guidance on monetary penalties for breaches of financial sanctions, which provides more clarity in relation to the government’s case assessment rules and penalty calculation procedures.

According to the guidance document, OFSI will continue to assess what level of penalty is reasonable and proportionate within the statutory maximum penalty and will make “a holistic assessment” of all the factors present in the case when deciding on the value of the penalty, not only based on the value of the breach.

OFSI clarifies that it will consider suspected financial sanctions breaches on a case-by-case basis and it may decide not to give voluntary disclosure reductions when the person in question has not made a complete disclosure.

The updated guidance removes previous provisions which recognised OFSI’s right not to impose a penalty in certain circumstances, such as when imposing a penalty has “no meaningful effect”, is perverse or runs against the public interest. The guidance became effective on 1 April.

Other key points

- In cases where there is no transaction value to be used in the penalty calculation process, OFSI will impose a penalty which is reasonable and proportionate to the facts, with a maximum permitted penalty of £1 million.

- When assessing an individual’s or a company’s knowledge of sanctions and compliance systems, OFSI will consider the nature of the work done, as well as their exposure to financial sanctions risk.

- Repeated, persistent or extended breaches by the same person will be qualified as an aggravating factor, especially when a person is unresponsive to previous warnings and continues to breach financial sanctions.

- The time period within which a penalised person can make representations regarding the proposed penalty, as well as requests for a ministerial review of the OFSI’s decision to impose a penalty has been extended to 28 working days.

- Penalty payments should be made within 28 working days of the date the penalty has been imposed.

Braskem discloses probe into allegations of improper payments involving project in Mexico

Brazilian petrochemical company Braskem S.A. disclosed in an 11 March filing with the US Securities and Exchange Commission (SEC) that it has hired an independent US law firm to assist the company in carrying out an internal investigation into alleged improper payments in relation to an ethylene project in Mexico.

Braskem states the allegations were first published in Mexican news reports and “included in the testimony presented by the former CEO of Pemex to the Office of the Attorney General of Mexico.” As the investigation is still ongoing, Braskem is unable to estimate when it will conclude.
UK regulators published Digital Regulation Cooperation Forum workplan, FCA to join

The UK Competition and Markets Authority (CMA) announced in a press release on 10 March that it has published the Digital Regulation Cooperation Forum (DRCF) workplan for 2021/22, highlighting three main priorities for the coming year. Formed by the CMA, the Information Commissioner’s Office (ICO) and the Office of Communications (Ofcom) in July 2020, the Financial Conduct Authority (FCA) will join the DRCF on 1 April 2021, to collectively ensure the effective and efficient regulation of the digital and online landscape.

The roadmap set out in the workplan aims to improve cooperation and coordination between the regulators as well as to establish a coherent regulatory approach to the digital and online landscape by focusing on three priorities: (1) responding strategically to industry and technological developments; (2) developing joined-up regulatory approaches; and (3) building shared skills and capabilities.

The first priority on responding strategically to industry and technological developments will include the establishment of joint strategic projects and horizon scanning for potential and future regulatory gaps. The DRCF identifies four emerging trends and technological developments in online services which it considers have implications for the regulatory objectives of its members and for which a coordinated approach to regulation is required. The identified emerging trends and technological developments in online services are: (1) design frameworks; (2) algorithmic processing; (3) digital advertising technologies; and (4) end-to-end encryption.

UK Pensions Minister calls for support from pension schemes to combat scams

UK Pensions Minister Guy Opperman issued an 11 March letter to 90 pension schemes in the country requesting that they share data relating to pension investment scams with the Pension Scams Industry Group (PSIG) to give the voluntary industry group greater insight into the impact of scams on pension investments.

Opperman stated in the letter that although “the measures contained in the Pension Schemes Act are a significant step forward, we need government, the individual and industry to tackle this together”, noting that “better data-sharing is a vital first step”. He also cited PSIG figures that roughly 5 percent of pension-related transfers are concerning. Opperman further referenced recent testimony by an Aviva executive that “95 percent of scams are from cloned investment sites resulting in a loss on average of £54,000”.

PSIG-gathered data is used to support the efforts of the Project Bloom taskforce that coordinates anti-scam and fraud activity targeting pensions. PSIG Chair Margaret Snowdon was quoted in a UK government notice as stating that the group currently has 51 participating pension schemes, which is not enough to fully “benefit from each other’s experience and spot trends early”. Ninety significantly sized pension schemes reportedly do not share data with the PSIG or with the Project Bloom taskforce.

To share data with the PSIG, pension scheme trustees can apply online via the combatting pension scams webpage. According to the government notice, the Pension Schemes Act will shortly allow for trustees to red flag certain transactions, who may, in some cases, be required to demonstrate they have read guidance prior to transfer approval.

UK government notice

Combatting pension scams ...
UK Finance and Cifas reveal uptick in money mule activity amongst "Generation Covid"

UK Finance published on 10 March new data from the national fraud prevention service Cifas which reveals a 5 percent increase in money mule cases targeting 21- to 30-year-olds in the past year, recording 17,157 such instances which account for 42 percent of money mule activity in 2020.

Money mules are reportedly targeting young people and others seeking work during the Covid-19 pandemic through fake job advertisements on social media and employment websites. UK Finance warns job seekers to exercise caution when viewing or responding to any offers that purport to promise easy and fast means of earning money and noting that money mule activity is often associated with serious crimes including human and drug trafficking and terrorism. Such offers, sometimes labelled as "money transfer agents" or "local processors", will often involve targets being prompted to provide their bank accounts, transfer incoming funds, and being offered a portion of the proceeds. UK Finance and Cifas launched the "Don't be fooled" online campaign in 2019 to educate young people about the personal and legal risks they can incur by accidentally becoming money mules.

Meanwhile, money mule cases involving UK residents under 21 dropped 12 percent last year to 8,791. UK Finance suggests that this drop may be attributed to teenagers spending more time with their parents and being less at risk of falling prey to criminal activities. Overall money mule cases are 27 percent higher than in 2017, but 2020 saw a slight decrease from the previous year. The UK Finance press release notes that it and Cifas "are calling for fraud and economic crime to be included in the upcoming Online Safety Bill" to make online platforms accountable for fraudulent content posted on their sites. UK Finance's Managing Director of Economic Crime Katy Worobec added that "online platforms must take swift action to detect and take down content being used to promote money muling activity" as "criminals are cruelly preying on 'Generation Covid' and those struggling to find work at this difficult time".

US SEC issues risk alert on issues related to broker-dealers suspicious activity reporting

The US Securities and Exchange Commission’s (SEC) Division of Examinations issued a risk alert on 29 March detailing broker-dealers’ obligations to monitor and report suspicious activity. The alert also includes findings from SEC examination staff on the adequacy of firms’ anti-money laundering (AML) compliance programmes.

According to the alert, some broker-dealers lack “reasonably designed” policies, procedures, and internal controls to identify suspicious activity, such as red flag provisions and automated monitoring. The SEC division adds that some broker-dealers also lack reporting systems even when dealing with large daily trading volumes, while their reporting thresholds are higher than $5,000. The SEC asserts that some firms fail to implement their policies and procedures, conduct adequate due diligence, and report suspicious activity.

The regulator finds that due to weak policies and procedures or failures to implement them, some broker-dealers do not conduct or document due diligence or report “known” suspicious activity indicators, especially in cases involving low-priced securities. Additionally, firms often submit suspicious activity reports that do not detail information on “key aspects” such as cyber-intrusion methods or do not report concerns on low-priced securities’ suspected promoters and issuers. The SEC reminds firms that failure to properly report suspicious activities or maintain records constitute violations of the AML regulations.
US FinCEN notice on antiquities and art trading

The US Financial Crimes Enforcement Network (FinCEN) issued a 9 March notice to financial institutions (FIs) about the Anti-Money Laundering (AML) Act of 2020 in relation to antiques and art trading as well as information resources about ongoing illegal art and antiques trading. The notice further provides suspicious activity report (SAR) instructions related to the trade and encourages FIs to continue filing SARs related to suspicious transactions.

Antique trading regulations are now amended under the AML Act’s Section 6110(a) to include individuals “engaged in the trade of antiques” under the definition of FIs, with Bank Secrecy Act (BSA) obligations to take effect when FinCEN implements relevant regulations. Section 6110(c) requires a joint study by coordinated government department heads including the Treasury Secretary and Secretary of Homeland Security to assess ML and terrorist financing (TF) in the art trade. This study is intended to include analysis of which markets should be subjected to regulations and whether regulations should center on any specific high-value art trades and purchaser identification.

The notice also warns FIs about art and antiques-related crimes such as looting or theft, illicit archaeological excavations, smuggling, and the sale of stolen items. Crimes related to art and antiques, FinCEN warns, may involve ML, sanctions violations, transnational organised crime groups, and cultural persecution of groups or individuals.

For SARs filing in relation to the trade in art or antiques, FIs are instructed to reference “FIN-2021-NTC2” in SAR field 2 and the SAR’s narrative section. They should also select SAR field 36(z), which corresponds to “Money Laundering – other” and denote art, antiques, or both. Contact information, including IP and email addresses and phone numbers, should also be listed in the narrative section for purchasers and sellers, intermediaries or agents, volume and dollar amounts of the transactions, and beneficial ownership information.

US FinCEN issues Marijuana banking update

The US Financial Crimes Enforcement Network (FinCEN) issued on 8 March an update that provides statistics on the suspicious activity reports (SARs) filed regarding Marijuana-related businesses (MRBs) and depository institutions (DIs) reporting services for MRBs through 31 December 2020.

The update offers explanations about why SAR filings related to MRBs declined from November 2019 and states that the decline leveled off in the middle of 2020, as have the number of DIs providing services to MRBs.

DIs actively banking MRBs experienced a short-term decline between the first and second quarter of 2020, with FinCEN noting that the short-term decline coincided with the issuance of guidance by the regulator and other financial supervisory agencies on financial services to MRBs. FinCEN notes that the Covid-19 pandemic may have added to the decline as many MRBs have temporarily closed and reduced staffing at DIs may have caused delays in sending SARs beyond the 90-day filing timeframe.

FinCEN received 170,975 SARs as of 31 December 2020 with keywords or phrases relating to MRBs.
US BIS updates advisory on North Korea’s ballistic missile procurement activities

The US Department of Commerce’s Bureau of Industry and Security (BIS) published on 11 March a revised advisory on the Democratic People’s Republic of Korea’s (DPRK) ballistic missile procurement activities, which highlights key procurement entities and deceptive techniques and provides information concerning designated entities and individuals.

According to the guidance document, individuals or entities violating the North Korea Sanctions Regulations could face monetary penalties of up to $307,922 or twice the value of the underlying transaction and may be subject to criminal proceedings. The most common DPRK procurement tactics include agents who are members of overseas networks operating from consulates and embassies or from trade offices, especially in countries such as China, Russia, Belarus or Ukraine. In addition, North Korea allegedly collaborates with Chinese and Russian foreign-incorporated entities, which purchase the items and ship them back after repacking and mislabelling them.

The US authorities call on individuals who are subject to US jurisdiction and foreign persons conducting transactions which involve the US to employ a risk-based approach to sanctions compliance, with a focus on management commitment, risk assessment, internal controls, testing, auditing and training. In addition, entities operating with goods identified by the UN Panel of Experts are advised to strengthen their due diligence mechanisms to ensure that the DPRK and its associated entities are not beneficiaries of such products.

The first North Korea advisory was issued on 1 September 2020 in cooperation with the US Department of State’s Bureau of International Security Non-Proliferation and the Department of the Treasury’s Office of Foreign Assets Control (OFAC).

Egmont Group holds workshop on financial investigations into wildlife crime

The Egmont Group’s Centre of FIU Excellence & Leadership (ECOFEL) organised on 10 March an online panel discussion on the public-private partnerships on wildlife crime related financial investigations, which discussed best practices and challenges in sharing intelligence in criminal investigations.

The event was organised in the context of ECOFELs Financial Investigations in Wildlife and Forestry Crime (FIWFC) project, targeted at reducing illicit financial flows linked to wildlife crime by enhancing financial intelligence units’ (FIUs) involvement in investigations. Participants included FIUs, international organisations, law enforcement agencies, financial institutions and other reporting entities.

As part of its FIWFC project, ECOFEL published on 12 January a report on financial investigations into wildlife crime, which called for the strengthening of partnerships between FIUs, environmental authorities and law enforcement to identify and tackle the laundering techniques associated with wildlife and forestry crime.

Egmont Group press release...
Workshop agenda
ECOFEL report
Egmont Group issues Covid-19 best practices guide for financial intelligence units

The Egmont Centre for Financial Intelligence Unit Excellence and Leadership (ECOFEL) released a Covid-19 best practices guide for FIUs on 18 March, which identifies emerging risks related to fraud, cybercrime, and corruption during the pandemic and offers a series of recommendations to FIUs on supervision, operational responses, contingency, and coordination. The paper follows virtual roundtables the group held with organisations including the Financial Action Task Force (FATF), Europol, Interpol, the UN Office on Drugs and Crime (UNODC), and the World Bank.

The guide notes increased corruption risks related to relaxed public procurement rules, hindered corruption investigations, non-bidding contracts, and emerging wildlife crime risks.

ECOFEL identifies some of the causes of increased fraud and cybercrime risk in the report as resulting from changes in supply and demand of pharmaceutical products such as Covid-19 tests and personal protection equipment, decreased mobility, and the increase in remote working, which includes 90 percent of banking and insurance workers working from home as of May 2020.

The paper also cites increased anxiety leading to increased vulnerabilities to exploitation, a decrease in illicit goods supplies, emergency procurement yielding increased opportunities for corruption, and a significant rise in government stimulus measures and financial aid distribution, which is the target of fraudsters.

Emerging fraud risks identified by ECOFEL and interviewed organisations include fraud related to Covid-19 medical supplies, soliciting donations for supposed research into Covid-19 cures, falsely claiming undue benefits, misappropriating public funds, increased CEO and cyber fraud, and increased use of illicit wire transfers. The paper recommends that FIUs advise entities to research charities before donating to them to avoid fraud.

In assessing cybercrime risks, the Egmont Group notes increased phishing emails, fake free money and prize offers, WhatsApp impersonation fraud, fake benefits agencies or medical product offers targeting the elderly and other vulnerable people, business email compromise scams, and ransomware. The group also notes increased corruption risks related to relaxed public procurement rules, hindered corruption investigations due to social distancing rules, non-bidding contracts, and emerging wildlife crime risks.

Recommendations include:

- Engage with public sector agencies, including prudential supervisors, to communicate about emerging risks through regular virtual meetings
- Communicate anti-money laundering and counter financing of terrorism expectations to reporting entities by requesting keyword usage in suspicious transaction reports (STRs) and suspicious activity reports (SARs) and engaging in daily screenings of FIU requests
- Engage with other FIUs and international organisations, consult with expert resources, and exchange Covid-19 operational information
- Ensure swift and prompt replies to requests from counterparts
- Monitor delays in receiving or processing STRs
- Proactively analyse transactions to screen for corruption
- Maximise off-site supervision when in-person visits are not possible
- Examine alternative methods for regulated entities to follow KYC requirements
- Ensure that FIUs have a contingency plan in place

Egmont Group announcement

ECOFEL best practices for FIUs summary
German government suspends Covid-19 aid for firms following fraud allegations

The German Ministry for Economic Affairs and Energy announced on 9 March the temporary suspension of Covid-19 financial support for companies as of 5 March, due to suspicions of personal protective equipment (PPE) fraud.

According to German authorities, the measure affects companies that applied for special financial assistance in November and December, and for other Covid-19 related bridge loans. The suspected fraud has been reported to the competent authorities and a criminal investigation is currently ongoing. The Ministry announced on 11 March that the programmes will be resumed shortly.

Two German members of the parliament, Nikolas Löbel and Georg Nüsslein, resigned on 7 March over face mask kickback allegations. The German media outlet Der Spiegel reported that Löbel confirmed that his company earned approximately €250,000 for brokering PPE contracts between a Baden-Württemberg supplier and two private companies. In addition, Nüsslein is accused of allegedly receiving over €600,000 to lobby for a face mask supplier.

On 29 March, Christian Social Union (CSU) member Niels Korte withdrew his Bundestag candidacy due to allegations of involvement in unlawful PPE contracts together with the German Ministry of Health. In addition, on 25 March Der Spiegel reported that the Munich Higher Regional Court issued an arrest warrant against an individual allegedly linked to the face mask scandal. Media reports claim that the arrested person is CSU-affiliated entrepreneur Thomas Limberger, who reportedly used his companies to secure face mask contracts with the German government.

Additional corruption allegations emerged on 18 March with respect to Tobias Zech, a representative of Bavaria’s CSU party in the Bundestag, who announced his resignation after Der Spiegel reported that he had allegedly accepted a “five-digit sum” in 2016 to lobby for a North Macedonian political party.

UAE bans Petrofac from bidding for contracts

The UK-based oil services provider Petrofac Limited announced on 15 March that it has been suspended by the Abu Dhabi National Oil Company (ADNOC) from bidding for new contracts in the United Arab Emirates (UAE) until further notice, as a result of the UK’s Serious Fraud Office (SFO) investigation into suspected bribery.

ADNOC’s decision follows the SFO’s 14 January announcement that the company’s former global head of sales David Lufkin has pleaded guilty under the UK Bribery Act 2010 to three additional charges of bribery in relation to UAE oil deals. According to the SFO, Lufkin made corrupt payments to UAE agents to influence the awarding of contracts worth $3.3 billion to Petrofac in 2013 and 2014. The former executive pleaded guilty to 11 charges in February 2019 for attempting to secure contracts worth of $4.23 billion in UAE and Iraq.

Petrofac will continue to work on two engineering, procurement and construction projects in UAE. According to the company statement, ADNOC’s decision will be periodically reviewed.
Australia's PRA closes Westpac AML probe

The Australian Prudential Regulation Authority (APRA) announced on 12 March that it has closed its investigation into Westpac Banking Corporation’s possible violations of banking regulation including anti-money laundering and counter terrorism laws.

The investigation was initiated by the APRA in December 2019 following AUSTRAC’s allegations involving Westpac. The APRA also sought to assess Westpac’s efforts to rectify and remediate the issues identified.

The APRA delegated certain powers to the Australian Securities and Investments Commission (ASIC) in 2020 to avoid both agencies investigating related matters concerning Westpac. The ASIC was conducting its own investigation into Westpac over potential corporate regulation violations.

Now, having considered the results of ASIC’s investigation, the APRA has decided to close its investigation. APRA Deputy Chair John Lonsdale stated, “Although the investigation has not found evidence of breaches of the Banking Act or the BEAR [the Banking Executive Accountability Regime], APRA remains determined to ensure Westpac rectifies its risk governance weaknesses effectively and sustainably.”

Westpac is subject to a court enforceable undertaking to implement a risk governance remediation plan across its business with ongoing independent review of its progress.

APRA press release

---

UK SFO closes bribery probe into KBR Inc

The UK’s Serious Fraud Office (SFO) announced on 18 March that it has closed its four-year investigation into the British subsidiaries, offices and agents of US engineering firm KBR Inc. The probe concerned allegations of bribery and corruption linked to Monaco-based oil and gas consultancy company Unaoil, which did not meet the standards of evidence for prosecution, according to the agency.

In its April 2016 10-Q form filed with the US Securities and Exchange Commission (SEC), KBR revealed that the US Department of Justice (DOJ) started an investigation into allegations of Unaoil-brokered corrupt practices purportedly involving numerous clients, adding that it was cooperating with the authorities. In the quarterly report published on 28 April 2017, the company revealed that the SFO commenced its own probe into the activities of KBR’s UK subsidiaries, their officers, employees, and agents.

In August 2020, the DOJ probe ceased to involve KBR, while the SFO informed the company that its investigation was no longer focused on allegations involving Unaoil “although some lines of inquiry remain” open, according to a press release from the firm.

Unaoil is part of an ongoing corruption scandal, with some of its top managers being accused in the US and the UK of offering millions of pounds in bribes to government officials around the globe to secure public contracts for their clients.

SFO press release

SFO press release (6 August 2020)

KBR press release (28 April 2017)
EU adopts cybersecurity strategy conclusions

The Council of the EU adopted on 22 March conclusions on the bloc’s cybersecurity strategy for the next decade, which looks to establish a framework to protect consumers and businesses from cyber-attacks as well as promote secure information systems within and outside the bloc. The conclusions include forthcoming action points such as creating an EU-wide network of security operations centres and potentially creating a cyber intelligence working group.

The cybersecurity strategy, presented in December 2020 by the European Commission and High Representative for Foreign Affairs Josep Borrell, centres on a core principle of both strategic autonomy and preservation of an open economy. Other areas of action highlighted by the Council include defining a joint cyber unit to give focus to the cyber crisis management framework and a commitment to the quick implementation of the EU 5G toolbox to guarantee network security.

The conclusions also discuss the importance of quickening the pace of critical internet security standards implementation, supporting effective encryption while balancing the needs of law enforcement investigators, and improving cooperation with multinational groups and partner states to better understand emerging cybersecurity risks.

Other external actions include improving the efficiency and effectiveness of the bloc’s cyber diplomacy toolbox, particularly in terms of addressing threats to supply chains, crucial infrastructure, and other forms of economic security. Lastly, the conclusions highlight the proposed EU external cyber capacity building agenda, which aims to improve cybersecurity capabilities globally.

US FinCEN Director discusses new AML Act

Blanco referenced the 9 March FinCEN notice on antiquities and art trading as one of the latest examples of AML Act application. FinCEN is also due to publish an advance notice of proposed rulemaking (ANPRM) which will address CTA requirements on beneficial ownership reporting.

Additionally, Blanco stated that the agency is engaged in efforts to make the beneficial ownership information that it collects accessible via an IT database by stakeholders, adding that FinCEN’s project team is currently developing use and confidentiality protocols for that database.

Lastly, Blanco urged the banking community to submit feedback in response to the upcoming ANPRM and other consultations which FinCEN intends to publish at frequent intervals.
OECD issues FAQs on bribery and corruption risks in mineral supply chains

During its Global Anti-Corruption and Integrity Forum held on 23 March, the Organisation for Economic Cooperation and Development (OECD) issued a frequently asked questions (FAQs) document on the bribery and corruption risks in mineral supply chains, with a view to assist companies in identifying, preventing and mitigating risks stemming from mineral sourcing.

The document encourages companies to cooperate with law enforcement agencies when suspicions of bribery risks arise and should solicit suppliers to undertake audits, disclose beneficial ownership information and allegations of foreign bribery, and ensure disciplinary and legal liability against responsible employees and business associates. According to the FAQs, companies that contribute to “adverse impacts” on people and the environment should ensure remediation by identifying and compensating victims of corruption.

The FAQs provide more clarity on the recommendations in the OECD’s due diligence guidance for responsible supply chains of minerals from conflict-affected and high-risk areas, which explains on how entities should combat bribery and corruption associated with minerals production and trade.

City of London Police data sees reports of online shopping fraud at an all-time high

The City of London Police announced on 24 March that new data released by the national policing lead for fraud shows an increase in online shopping and romance fraud committed in the last 11 months, with related cybercrime and online fraud causing losses of approximately £34.5 million since March 2020.

A total of 6,073 Covid-19 related fraud and cybercrime reports have been received by Action Fraud since 1 March 2020 and the UK’s dedicated national fraud units have arrested 156 criminals alleged to have committed fraud during the lockdown imposed as a result of the pandemic.

According to the new data, over 416,000 reports of fraud and cybercrime were received with online shopping fraud increasing by 42 percent to an all-time high, while romance fraud has risen by 20 percent over the past 11 months when compared to 2019. Meanwhile, computer software service fraud has dropped by 15.5 percent.

The City of London Police’s National Fraud Intelligence Bureau (NFIB) has shut down 1,030 websites, 425 phone numbers and 597 email addresses linked to criminal activity. In addition, the Intellectual Property Crime Unit (PIPCU) has taken down several websites believed to be selling counterfeit coronavirus related products such as testing kits and face masks.

The UK’s Dedicated Card and Payment Crime Unit (DCPCU) has also executed 99 warrants and made 56 arrests, of which 27 percent were related to coronavirus “smishing” incidents.
UN experts call on businesses to scrutinise Xinjiang-sourced supply chains

The UN Working Group on Business and Human Rights issued on 29 March a statement urging global companies to thoroughly scrutinise their supply chains following serious concerns linking alleged abusive practices against Muslim Uyghurs, including detention and forced labour, to more than 150 Chinese and foreign domiciled businesses and factories.

According to sources cited by the 16 UN experts, hundreds of thousands of members of the Uyghur minority have been subjected to exploitative working in businesses and factories in the Xinjiang Uyghur Autonomous Region (XUAR), and abusive living conditions in "re-education" facilities. Dante Pesce, Chairperson of the Working Group, called on the Chinese government to cease any forced employment in low-skilled, labour-intensive industries, as well as other measures that are not compliant with international human rights standards.

The experts also underlined that the organisations involved in human rights abuses, such as forced labour and enslavement, are reportedly operating as part of supply chains of multiple well-known global brands. Reiterating the obligations under the UN Guiding Principles on Business and Human Rights, the experts contacted the government of China and 13 other countries, as well as private businesses, located inside and outside of China, to ensure that such businesses respect human rights throughout their operations. Vice Chairperson of the Working Group, Surya Deva, stressed that businesses "Must conduct meaningful human rights due diligence [...] to identify, prevent, mitigate and account for human rights abuses caused, contributed to or directly linked to their operations".

According to a BBC report from 25 March, the statement comes after a social media post by China's Communist Youth League, alleging that global companies are spreading rumours about boycotting Xinjiang cotton, caused a backlash by Chinese state media, e-commerce platforms and consumers. The post refers to statements by Swedish retailer H&M and US sportswear company Nike, expressing concerns about reports of cotton production involving forced labour in Xinjiang, and announcing they will refrain from sourcing cotton from XUAR. The statements, made in 2020, resurfaced this month following the imposition of Xinjiang-related sanctions on Chinese individuals and entities by the European Union.

On 31 March, H&M issued a conciliatory statement, in which it underlines both the importance of the Chinese market and consumers, and the company's responsibilities as a "major buyer", expressing dedication to "regaining the trust and confidence of our customers, colleagues, and business partners in China".

Aperio Analysis by Vivien Li

Extensive evidence of forced labour programmes targeting the Uyghur and other ethnic minorities in China mean that companies with supply chain links to XUAR face significant legal, reputational and economic risks with regard to their suppliers. At the same time, companies that are either part of a value chain that stretches to XUAR or engage with local authorities in the fields of surveillance, biometrics, or tracking technology, are also at risk of facilitating human rights violations. When it comes to human rights due diligence, companies should trace their supply chains to origin and, to the extent possible, identify any associations between their sub-suppliers and forced labour in XUAR. While conducting due diligence in XUAR is challenging due to limits on access, a lack of freedom of speech for workers, and the extent and severity of human rights violations occurring there, companies need to go well beyond the due diligence they ordinarily undertake. Companies should also have human rights policies and practices in place to ensure their operations do not directly or indirectly contribute to violations.
UK NCA’s latest SARs In Action magazine

The UK’s National Crime Agency (NCA) published on 30 March the latest issue of its Suspicious Activity Reports (SARs) In Action magazine, which includes recent developments involving the utilisation of SARs, from digital engagement conducted by the UK Financial Intelligence Unit (UKFIU) with law enforcement agencies, to specific updates from officers of the Bribery and Corruption Unit (BCU), Modern Slavery and Human Trafficking Unit (MSHTU), and the Association of Chartered Certified Accountants.

The magazine sums up recent steps taken by the UKFIU to enhance its digital engagement with law enforcement agencies, such as interactive workshops and webinars on anti-money laundering (AML), underground banking, and cryptocurrency and announces that a joint webinar for the accountancy sector in collaboration with the Institute of Chartered Accountants in England and Wales will take place on 27 April.

Summing up the effective ways of utilising SARs in identifying new cases of bribery and corruption and further assisting existing ones, an anonymous officer from the BCU emphasised that the Unit advises reporters to indicate the source of any additional information comprised in the SAR – open-source research, copies of contracts or paperwork provided by the client.

With regards to intelligence sharing within the accountancy sector, Wesley Walsh, AML Supervision Manager at the Association of Chartered Certified Accountants, underlined that a sub-group of the Accountancy Sector Intelligence Sharing Expert Working Group (ISEWG) was created to review all alerts issued by the Joint Money Laundering Intelligence Taskforce (JMLIT). The sub-group will assess the alerts’ suitability for the accountancy sector and reformat them specifically for the sector, in order to ultimately make them available to money laundering reporting officers, and enable them to be issued by accountancy professional body supervisors (PBSs) to their members.

Laura Simpson, Senior Officer at the Modern Slavery and Human Trafficking Unit (MSHTU), summarised key accomplishments achieved by the NCA MSHTU Project AIDANT, which is focused on multi-agency activities targeting sexual exploitation, labour exploitation and child trafficking, and by the UKFIU MSHTU November 2020 conference on SAR interrogation and collaboration with financial institutions. Simpson announced that further phases of Project AIDANT and conferences on modern slavery and trafficking generated illicit finance will be launched throughout 2021.

UK FCA launches whistleblower campaign

The UK’s Financial Conduct Authority (FCA) announced on 24 March the launch of a new whistleblower campaign to encourage individuals working in the financial services sector to report any potential wrongdoing to the regulator.

As part of the new campaign, the FCA introduces a mandatory e-learning module for its staff on how to ensure that the intelligence received by the regulator is managed correctly, with the protection of the whistleblowers’ identity. In addition, the FCA has produced a digital toolkit for whistleblowing and consumer groups, as well as for industry bodies, which describes potential cases of wrongdoing and how the FCA deals with the shared information.

The FCA has updated its website to include information for potential whistleblowers and remains committed to expanding the ways in which individuals can report misconduct.
UK Pensions Regulator calls on industry to step up reporting of scams

The UK’s Pensions Regulator (TPR) warned on 25 March that the recent decrease in pension scams reporting may not reflect actual criminal trends, calling on the pensions industry to be alert to suspicious activity and to support its ongoing anti-scam campaign. According to the regulator, pension scam reports fell by almost 80 percent from 2014 to 2020, with a slight increase this year.

The TPR’s Executive Director Nicola Parish states that multiple levels of stakeholders from trustees to providers and administrators are not sending in suspected scam reports, while the Covid-19 pandemic can make investors increasingly vulnerable. Parish is encouraging the entire pensions industry to report suspected scams via the Action Fraud service or by calling 101 in Scotland.

The TPR’s anti-scam campaign targets pension providers, trustees, and administrators and was launched in November 2020. With more than 200 organisations having signed up to the campaign so far, it aims to encourage those requesting cash drawdown to ask for guidance from The Pensions Advisory Service. Additionally, the campaign aims to encourage the industry to take appropriate due diligence measures and document pensions transfer procedures.

Volkswagen seeks damages from ex-CEOs over emissions scandal

Volkswagen AG announced on 26 March that its supervisory board has decided to seek damages from former CEO Martin Winterkorn and former Audi CEO Rupert Stadler over alleged breaches of the “duty of care” under the German Stock Corporation Act, following a six-year investigation into the diesel emissions fraud scandal at the company.

According to the company’s press release, the investigation concluded that Winterkorn failed to clarify the situation behind the use of illegal software concerning 2.0 TDI diesel engines sold in North America between 2009 and 2015, while Stadler failed to ensure that investigations regarding the software were carried out with respect to 3.0 and 4.2 V-TDI diesel engines developed by Audi AG and installed in Volkswagen, Audi and Porsche vehicles in the EU. Volkswagen AG stated that no violations were identified in relation to other members of the company’s supervisory board.

The decision to claim damages from the two executives concludes an investigation launched in October 2015 following issuance of a notice of violation by the US Environmental Protection Agency (EPA) against Volkswagen, alleging that the company violated the Clean Air Act when installing illegal software in vehicles in order to pass emissions tests. The company pleaded guilty in March 2017 to conspiracy to commit fraud, obstruction of justice and false statements, and settled the charges for $4.3 billion in criminal and civil penalties.
J5 countries host event on FinTech companies

The US Internal Revenue Service (IRS) announced on 25 March that the Joint Chiefs of Global Tax Enforcement (J5) hosted a virtual event which brought together cryptocurrency experts, data scientists and investigators to take part in a "challenge" to open J5 tax crime investigations involving FinTech companies.

During the event, legal experts from the five countries used analytical tools and real datasets to generate leads and identify criminal suspects, which can lead to subsequent investigation and enforcement action by the J5. The countries stressed that the FinTech industry is vulnerable to tax avoidance and money laundering, particularly when cryptocurrencies are involved and considering the virtual nature of FinTech products and services.

The event was first organised in 2018 and focuses on identifying facilitators and enablers of international tax crime.

US blocks Venezuela’s request for World Trade Organisation sanctions review

The US objected to the adoption of the World Trade Organisation (WTO) Dispute Settlement Body’s (DSB) meeting agenda on 26 March which included a request by Venezuela to assess whether sanctions imposed by the US between 2018 and 2019 violated the global trading rules, according to a statement made by the US Mission in Geneva.

The US stated during the DSB meeting that Venezuela's request for a sanctions review panel was submitted by an illegitimate government which it does not recognise. The US Trade Representative spokesperson Adam Hodge highlighted that the US "will reject any effort by Maduro to misuse the WTO to attack US sanctions aimed at restoring human rights and democracy to Venezuela". Venezuelan Foreign Minister Jorge Arreza responded that the US sanctions are "unilateral coercive measures".

During a 2019 WTO meeting, Venezuela requested consultations with the US government on the US trade sanctions, pursuant to a series of regulations and executive orders issued in 2018. Following the US administration’s refusal, Venezuela asked that a panel be established to review the US sanctions, in accordance with the WTO rules of procedure for the settlement of disputes.

The US objection to the adoption of the agenda during the DSB meeting blocks Venezuela from seeking a WTO review of US sanctions and suspends all agenda items. The EU has requested that WTO representatives ensure that the meeting goes forward and "the DSB discharge the important duties with which it is entrusted".

IRS press release
J5 press release
US statement at WTO DSB meeting
WTO DSB meeting agenda
Request for establishment of a panel by Venez...
EU issues declaration on the conflict in Syria

The High Representative of the European Union published on 14 March a declaration on behalf of the EU on the ten years since peaceful protests started throughout Syria, which has resulted in internationalised armed conflict following the regime’s repression of the Syrian people and its failure to address the causes of the uprising. The declaration states that targeted EU sanctions on prominent members and entities of the Syrian regime will be renewed at the end of May if there is no credible progress.

In the declaration, the EU states that the human rights violations and severe violations of international humanitarian law by all parties, especially by the Syrian regime, over the past ten years has caused “enormous human suffering”. The EU highlights the importance of accountability for all violations of international humanitarian and human rights law as a legal requirement and a central measure in achieving sustainable peace and reconciliation in Syria. The EU also notes that all actors in Syria must focus on the fight against terrorist organisation Da’esh to prevent its resurgence.

Targeted EU sanctions on prominent members and entities of the regime will be renewed at the end of May if there is no credible progress

The EU has not changed its policy as outlined in its latest conclusions and remains committed to the unity, sovereignty, and territorial integrity of the Syrian state. It continues to demand an end to repression, the release of detainees, and for the Syrian regime and its allies to engage meaningfully in the complete implementation of UN Security Council resolution 2254. Targeted EU sanctions on prominent members and entities of the regime will be renewed at the end of May if there is no credible progress and as long as the repression continues, states the declaration.

EU Council press release

Aperio Analysis by Larissa Normanton

Almost half a million have been killed since the outbreak of the civil war and uprising against the Al-Assad regime in 2011, and 11 million - half the pre-war population - have been displaced. Supported by Russia and Iran-backed militias, since 2015 the regime has regained control over the majority of the country, with the exception of an opposition enclave in Idlib in the north-west of the country - an ungovernable pocket dominated by Salafist-jihadist rivalry amongst ever-splintering groups as well as Turkey-backed opposition - and Kurdish-controlled territory in the north-east. According to the UN, more than 80 percent of the population lives below the poverty line. Whilst Assad has tried, and will continue to try, to use sanctions as a scapegoat for the state of Syria’s economy, the reality is that back in 2011, the economic situation played a key role in fuelling the civil uprising that started in the southern province of Dara’a and transformed into the ongoing civil war. In some ways Syria is back where it started before the start of the civil war ten years ago. The underlying socio-economic grievances that fuelled the uprising are even more pronounced today and despite continuing unrest and increasing sanctions, it is very unlikely that Assad will step down – and even more unlikely that Russia would allow this given the costs Moscow has incurred in protecting his position.
UK sanctions Myanmar conglomerates

The UK’s Foreign, Commonwealth and Development Office (FCDO) announced on 25 March that it has imposed sanctions on military-owned conglomerate Myanmar Economic Holdings Ltd (MEHL) over its alleged connections with serious human rights violations against the Rohingya population and its association with senior military figures involved in the 1 February coup.

According to Foreign Secretary Dominic Raab, the action targets the financial interests of the Myanmar military in order to "help drain the sources of finance of their campaigns of repression against civilians". MEHL is allegedly owned by parts of the armed forces and military officers and has contributed funds to support the military in perpetrating human rights violations against the Rohingya population in 2017.

The measures have been taken in conjunction with the US Department of the Treasury’s Office of Foreign Assets Control (OFAC) which, according to the US State Secretary Antony Blinken, has designated MEHL and a second entity, Myanmar Economic Corporation Limited (MEC), over being part of the economic interests of the military, as the "two largest military holding companies" in Myanmar.

On 1 April, Raab announced further sanctions targeting Myanmar, adding MEC to its sanctions list, for being a major conglomerate that is allegedly “in practice owned and governed by, and for the benefit of, the Myanmar Ministry of Defence”. MEC has interests in a wide range of sectors, including banking, mining, real estate, metals, and transportation.

US designates Ukrainian oligarch and former governor for corruption

US Secretary of State Antony Blinken announced on 5 March the designation of Ukraine’s former Dnipropetrovsk Oblast governor Ihor Kolomoyskyy for corruption during 2014 and 2015 that purportedly resulted in personal gain as well as undermining the law and public faith in government institutions. Secretary Blinken also expressed "concern about Kolomoyskyy’s current and ongoing efforts to undermine Ukraine’s democratic processes and institutions, which pose a serious threat to its future".

The former Ukrainian governor, who is described by the US as an oligarch, has been designated pursuant to the Department of State, Foreign Operations, and Relations Programs Appropriations Act 2020, Section 7031(c). The designation also includes the former official’s wife, Iryna Kolomoyskyy and children, Angelika Kolomoska and Israel Zvi Kolomoyskyy. All four are barred from obtaining US visas.

In a press statement announcing the designations, the Secretary of State added that the latest action reaffirms US support for the "political, economic, and justice sector reforms that are key to Ukraine’s Euro-Atlantic path".
EU designates 11 Myanmar high-ranking military officials and amends designation criteria

The EU Council designated on 22 March 11 high-ranking officials in response to the 1 February military coup and subsequent repression of peaceful demonstrators. The designations are being made pursuant to Council Implementing Regulation (EU) 2021/480 and Council Decision (CFSP) 2021/483.

According to the EU Council, the designations include ten senior military officials, including the Commander-in-Chief of the Myanmar Armed Forces (Tatmadaw), Min Aung Hlaing, and Deputy Commander-in-Chief of Tatmadaw, Soe Win, who have been directly involved in restricting the rights of freedom of expression and access to information, arbitrarily arresting opposition leaders and killing civilian and unarmed protesters. Among the designated persons is also the new Chairperson of the Union Election Commission, Thein Soe, who was involved in cancelling the results of the 2020 elections in Myanmar without providing any proven evidence of fraud.

The measures include an asset freeze and a travel ban, and will coexist with the remaining arms embargo, export ban on dual-use goods, and restrictions on certain equipment for military and communications monitoring, and the previous designation of 14 individuals involved in atrocities against the Rohingya population.

Others designated include: Tatmadaw’s Vice-President Myint Swe, former Minister of Defence Swin Win, current Minister of Defence Mya Tun Oo, Secretary of the State Administration Council (SAC) Dwe Aung Lin, Joint Secretary of the SAC Ye Win Oo, Deputy Minister of Home Affairs and Chief of Police Than Hlaing, and members of the Tatmadaw and SAC Maung Maung Kyaw and Moe Myint Tun.

Seven of the EU designated persons are also currently listed by the UK: Dwe Aung Lin, Min Aung Hlaing, Mya Tun Oo, Maung Maung Kyaw, Moe Myint Tun, Ye Win Oo, Than Hlaing.

On the same day, the EU Council amended the designation criteria, pursuant to Council Regulation (EU) 2021/479 and Council Decision (CFSP) 2021/482, allowing for the imposition of sanctions against persons, entities and bodies whose activities are intended to undermine democracy and the rule of law in Myanmar, as well as legal persons, entities and bodies owned or controlled by and providing revenue and support to the Tatmadaw.

The EU has also decided to withhold financial assistance to the government; freeze all assistance to government bodies deemed to be supporting the military; and will continue to review all policy options, including further measures against Myanmar entities.

EU renews Bosnia and Herzegovina sanctions

The Council of the European Union renewed on 26 March the sanctions framework with respect to the situation in Bosnia and Herzegovina for one year, until 31 March 2022.

The restrictive measures were adopted on 21 March 2011 and include an asset freeze and travel ban, but no individuals or entities have been listed under the regime yet.

The EU adopted Council Decision (CFSP) 2021/543, which enables the EU to impose targeted restrictive measures against individuals and entities seeking to undermine the sovereignty, territorial integrity, constitutional order and international personality of Bosnia and Herzegovina, seriously threaten the security situation or undermine the 1995 Dayton/Paris General Framework Agreement for Peace.
OFAC sanctions Myanmar holding companies

The US Department of the Treasury’s Office of Foreign Assets Control (OFAC) announced on 25 March the imposition of sanctions on Myanmar (Burma), by adding the two largest military holding companies in Myanmar to its list of specially designated nationals and blocked persons (SDN). The designations have been made pursuant to Executive Order (EO) 14014, which authorises property blocking with respect to Myanmar.

The two entities, which dominate important sectors of the country’s economy are Myanmar Economic Holdings Public Company Limited (MEHL), which has interests in banking, trade, construction, mining, tourism, and agriculture, and Myanmar Economic Corporation Limited (MEC), which operates in the mining, manufacturing, and telecommunications sectors.

OFAC also issued Burma General License (GL) 1, 2, and 3, which authorise activities involving the official business of the US government, activities involving international organisations and entities, and transactions in support of non-governmental organisations. In addition, under GL 4, companies are permitted to wind-down any transactions and activities with MEHL and MEC or any other entities of which they own 50 percent or more until 22 June 2021, starting from when such transactions are prohibited.

Furthermore, OFAC published two frequently asked questions. FAQ 882 provides an organisational chart of the organisations included within UN programmes, funds, and other entities and bodies, and its specialised agencies and related organisations which are covered by GL 2.

FAQ 883 clarifies that for the duration of GL 4 – until 22 June 2021 – OFAC authorises all transactions and activities prohibited by EO 14014 that are ordinarily incident and necessary to the winding-down of transactions involving MEHL and MEC, or entities in which they own a 50 percent or greater interest.

According to US State Secretary Antony Blinken, the sanctions are imposed in response to the military’s “refusal to disavow the coup and continuing violence against peaceful protestors”, and target the two companies for being “managed by current or former Burmese [Myanmar] military officers, regiments, and units, and organisations led by former service members”.

The measures have been taken in conjunction with the UK, which designated MEHL for being owned by parts of the Myanmar armed forces and for having contributed funds to support the military’s human rights violations against the Rohingya population.

US renews sanctions with respect to significant malicious cyber-enabled threats

The White House published a notice on 29 March continuing the national emergency for another year concerning significant malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the US.

The notice states that significant malicious cyber-enabled activities continue to pose an unusual and extraordinary threat to US national security, foreign policy, and economy. The sanctions regime was first declared in April 2015 by Executive Order 13694 pursuant to the International Emergency Economic Powers Act.
US designates two senior Myanmar military officials and two entities

The US Treasury Department’s Office of Foreign Assets Control (OFAC) announced on 22 March the designation of the Chief of the Myanmar Police Force and Deputy Home Affairs Minister Than Hlaing, Myanmar’s Bureau of Special Operations Commander Aung Soe, and two entities over the ongoing repression of pro-democracy protests since the 1 February military coup. The listings are made pursuant to Executive Order (EO) 14014 on blocking property with respect to the situation in Burma.

The two entities, which are added to the OFAC specially designated nationals and blocked persons list (SDN), pursuant to Executive Order (EO) 14014, are 33rd Light Infantry Division of the Burmese Army (33 LID) and the 77th Light Infantry Division of the Burmese Army (77 LID) over alleged instances of excessive force, including killings by security forces. 33 LID was also designated by OFAC on 17 August 2018, pursuant to EO 13818 for its involvement in human rights violations against the Rohingya population.

According to OFAC, under Hlaing’s and Soe’s leadership, the Police Force and the regional commands of the Bureau of Special Operations have engaged in systemic attacks which led to the killing of tens of peaceful protestors.

In addition, OFAC’s press release describes that the deployment of 33 LID and 77 LID, as part of the country’s security forces’ systemic use of lethal force, has implied excessive force, including killing and injuring several peaceful protestors in the cities of Mandalay and Rangoon.

State Secretary Antony Blinken reiterated on the same day the US’ commitment to continue acting against coup leaders and perpetrators of violence in Myanmar, calling on the military regime to release unjustly detained persons and cease all attacks on civil society members.

Concurrently, the European Union also imposed an asset freeze and a travel ban against Hlaing, Myanmar Armed Forces (Tatmadaw) Commander-in-Chief, Min Aung Hlaing, as well as eight other senior military officers and the Chairperson of the Union Election Commission, Thein Soe.

OFAC press release
Identifying information
Department of State press...

US renews South Sudan sanctions

US President Joseph Biden announced on 29 March the renewal for one year of the national emergency with respect to South Sudan until 3 April 2022.

The South Sudan sanctions were declared on 3 April 2014, under Executive Order (EO) 13664, pursuant to the International Emergency Economic Powers Act (IEEPA), concerning 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” continues to pose “an unusual and extraordinary threat” to the US.

White House notice
US President letter
OFAC designates Myanmar commander’s children and six of their companies

The US Treasury Department’s Office of Foreign Assets Control (OFAC) designated on 10 March Myanmar Commander in Chief Min Aung Hlaing’s two adult children and six of their companies in response to the Myanmar military’s 1 February coup and ongoing killing of civilian protesters.

Aung Pyae Sone and Khin Thiri Thet Mon are now designated and subject to asset and property freezes pursuant to Executive Order (EO) 14014 on the situation in Myanmar. Hlaing was designated on 11 February. The designated entities, that are said to have benefited from Hlaing’s position and influence are: A&M Mahar Company Limited, Sky One Construction Company Limited, the Yangon Restaurant, the Yangon Gallery, Everfit Company Limited, and the Seventh Sense Company Limited. According to a Treasury Department press release, Aung Pyae Sone secured a competition-free land lease permit for the Yangon Restaurant and Gallery for 30 years. He also reportedly paid 1 percent of the rental rates of comparable properties in the capital.

In a separate release, Secretary of State Antony Blinken stated that both children “have long used their connections to the CINC for personal enrichment”, asserting that coup leaders and family members “should not be able to continue to derive benefits from the regime as it resorts to violence and tightens its stranglehold on democracy”.

OFAC Director Andrea Gacki said that the “indiscriminate violence by Burma’s security forces against peaceful protestors is unacceptable”, adding that the US will continue to work multilaterally to end the violence and “restore democracy and the rule of law in Burma”.

European Council extends Ukraine territorial integrity sanctions for six months

The Council of the EU decided on 12 March to extend until 15 September 2021 the sanctions regime targeting individuals and entities responsible for undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, pursuant to the Council Implementing Regulation (EU) 2021/446.

The EU restrictive measures currently target 177 individuals and 48 entities and include travel restrictions, asset freezes and a ban on making funds or other economic resources available to the listed persons and entities.

The EU sanctions over Ukraine’s territorial integrity were first introduced on 17 March 2014, pursuant to Council Regulation (EU) 269/2014. Other measures adopted by the EU in relation to Ukraine include economic sanctions targeting specific sectors of the Russian economy, which are in force until 31 July, as well as restrictive measures imposed as a result of the illegal annexation of Crimea and Sevastopol, which expire on 23 June.
US BIS imposes further export controls on Myanmar, adds four to the Entity List

The US Commerce Department issued two final rules on 4 March imposing further restrictions on exports, re-exports, and in-country transfers of sensitive items subject to the Export Administration Regulations (EAR) to Myanmar in response to the 1 February military coup. In addition, two Myanmar military and security services entities and two other companies have been added to the Commerce Department’s Bureau of Industry and Security (BIS) Entity List.

According to an 8 March notice, Myanmar is now subject to a more restrictive review of licence applications for exports and re-exports involving items subject to the EAR by moving it from EAR Country Group B to Country Group D:1 and rendering Myanmar’s end users ineligible for or subject to further restriction regarding the use of certain licence exceptions for exports, re-exports, and transfers. The licence exceptions relate to shipments of limited value (LVS), shipments to Group B countries (GBS), technology and software under restriction (TSR), servicing and replacement parts and equipment (RPL), aircraft, vessels, and spacecraft (AVS), and encryption commodities, technology, and software.

Additionally, Myanmar is moved from Computer Tier 1 to Computer Tier 3 under licence exception computers (APP), while being added to the list of countries subject to the military end-use and end user controls (MEU) and associated licencing policies. Applications to export or re-export items to Myanmar for military end-use or military end users will be reviewed under a presumption of denial.

The additions to the Entity List are Myanmar’s Ministries of Defence and Home Affairs, the Myanmar Economic Corporation, and Myanmar Economic Holding Ltd. The first two were designated for their roles in the February military coup and for “posing risks of being or becoming involved in, activities contrary to US national security and foreign policy interests”, while the two companies were found to be owned and operated by the Ministry of Defence and providing the Ministry with revenue. Under the BIS notice, a licence requirement for all items subject to the EAR and a licence review policy of presumption of denial are imposed for all four entities, while no licence exceptions are available for exports, re-exports, or transfers associated with them.

The new restrictions came into force on 8 March.

EU lifts sanctions on former Libyan PM

The Council of the European Union announced on 26 March its decision to delist Khalifa Ghwell, the former prime minister and defence minister of the General National Congress of Libya, when the EU’s sanctions regime on Libya is renewed on 2 April 2021.

The sanctions, which were first imposed on Ghwell in 2021, include a travel ban and asset freeze. The EU Council’s press release states that sanctions intend to “bring about a change in policy or activity by entities and individuals responsible for malign behaviour” and that “delisting is appropriate whenever the criteria for listing are no longer met”.

EU Council press release
The UK’s Foreign and Commonwealth Office (FCO) announced on 22 March that it has designated four Chinese government officials and a Xinjiang security agency, under the UK’s global human rights sanctions regime, over systemic repression perpetrated with respect to Uyghurs and other minorities in the Xinjiang Uyghur Autonomous Region (XUAR). The measures are taken in coordination with the United States and Canada, which listed the same individuals and entity, pursuant to Executive Order 13818 and through the Special Economic Measures (People’s Republic of China) Regulations, respectively.

The sanctions target former Secretary of the Political and Legal Affairs Committee of the XUAR, Zhu Hailun, Deputy Secretary of the Party Committee of XUAR, Wang Junzheng, Secretary of the Political and Legal Affairs Committee of the XUAR, Wang Mingshan, Director of the XUAR Public Security Bureau, Chen Mingguo, and the Public Security Bureau of the Xinjiang Production and Construction Corps (XPCC). The measures are based on allegations of systemic repressive practices against Uyghur Muslims and members of other ethnic and religious minorities in Xinjiang, which the designated individuals and entities have allegedly been supporting and perpetrating.

In a joint statement, the UK, US, and Canada call on China to cease all human rights violations and halt its “extensive programme of repression”, which includes “severe restrictions on religious freedoms, the use of forced labour, mass detention in internment camps, forced sterilization, and the concerted destruction of Uyghur heritage”. The governments also urge China to grant unhindered access to Xinjiang to the international community, including UN independent investigators and foreign diplomats.

On 12 January, UK Foreign Secretary Dominic Raab announced a package of measures to ensure that UK organisations, governments and the private sector are not complicit in the human rights violations in Xinjiang. The measures include a review of Xinjiang export controls to determine which specific products should be subject to export controls in the future, the imposition of financial penalties targeting businesses failing to publish annual modern slavery statements under the Modern Slavery Act, and detailed guidance for UK organisations on the specific risks and challenges of effective due diligence in Xinjiang.

Highlighting the active response of the international community to the situation in Xinjiang, with 39 countries signing a joint statement at the UN aimed at holding China accountable for human rights violations, Raab reiterated the UK’s commitment to react to any egregious violations of human rights. With respect to the latest designations, Raab stated that they will be imposed immediately and imply travel bans and asset freezes against individuals and an asset freeze against the entity.

In response to the sanctions, the Chinese Ministry of Foreign Affairs announced on 26 March reciprocal sanctions against four entities and nine individuals in the UK, which include a travel ban and an asset freeze with respect to property and business in China. Designations include former Conservative party leader Iain Duncan Smith and the Conservative party’s Human Rights Commission, MPs Tom Tugendhat, Neil O’Brien, Nus Ghani and Tim Loughton, two members of the House of Lords, David Alton and Helena Kennedy QC, Barrister Geoffrey Nice and Uighur expert at Newcastle University, Joanne Nicola Smith Finley. Listed entities include the China Research Group, independent research group Uyghur Tribunal and London law firm, Essex Court Chambers.

On 27 March, China imposed similar sanctions on the Chair and Vice Chair of the United States Commission on International Religious Freedom (USCIRF), Gayle Manchin and Tony Perkins, Member of the Canadian Parliament Michael Chong, and the Subcommittee on International Human Rights of the Standing Committee on Foreign Affairs and International Development of the House of Commons of Canada.

In response to the reciprocal sanctions on the USCIRF commissioners, the US State Secretary Antony Blinken released a statement condemning the decision and reiterating US solidarity with international partners calling on China to cease any human rights violations and abuses against Uyghurs and other ethnic minority groups.

UK government press release
UK OFSI notice
UK Foreign Secretary statement
EU designates individuals and entities in China and other countries over human rights

The Council of the European Union announced on 22 March the second imposition of designations under the global human rights sanctions regime targeting 11 individuals and four entities in China, Russia, North Korea (DPRK), Libya, South Sudan, and Eritrea. The designations are made pursuant to Council Implementing Regulation (EU) 2021/478 and Council Decision (CFSP) 2021/481.

The designations, consisting of asset freezing measures and travel bans, target four Chinese officials and one state-controlled security agency for overseeing the large-scale detention, surveillance and indoctrination programme targeting Uyghur Muslims and people from other minorities in the Xinjiang Uyghur Autonomous Region (XUAR). The measures are taken in coordination with Canada and the UK, which concurrently announced sanctions against the same individuals and entity, as well as the US, which announced the listing of two of the officials under Executive Order (EO) 13818.

In response to the sanctions, China imposed reciprocal designations on five members of the European Parliament, three members of the Belgian, Lithuanian, and Dutch parliaments, two German and Swedish academics, the Political and Security Committee of the Council of the European Union, the Subcommittee on Human Rights of the European Parliament, and two NGOs – the Mercator Institute for China Studies in Germany, and the Alliance of Democracies Foundation in Denmark.

On 23 March, four leading MEPs condemned China’s decision to impose reciprocal sanctions, expressing solidarity with parliamentarians, European universities, NGOs and academics who have been targeted by the sanctions, and reiterating the EU’s commitment to “actively denounce human rights violations and breaches of international law”. The four MEPs are the Chair of the European Parliament’s Foreign Affairs Committee, David McAllister, Chair of the European Parliament’s Subcommittee on Human Rights, Maria Arena, Chair of the Special Committee on Foreign Interference, Raphaël Glucksmann, and Chair of the European Parliament’s delegation for relations with the People’s Republic of China, Reinhard Butikofer.

In addition to the Chinese officials, the EU is designating: (1) two DPRK ministers for implementing “repressive security policies” which pose a serious threat to the political system and the people of North Korea, as well as the country’s public prosecutor’s office, for enabling “legitimacy to serious human rights violations committed by DPRK security apparatus”; (2) two senior officials in the Chechen Republic, Russia over systematic torture and repression against people of the LGBTI community and political opponents; (3) the Libyan Kaniyat Militia, its commander and another senior member, over “extrajudicial killings and enforced disappearances of persons between 2015 and 2020 in Tarhuna”; and (4) a senior military official of South Sudan and the national security agency of Eritrea for “torture and extrajudicial killings” in the two countries.

The specific EU designations include:

- Former Secretary of the Political and Legal Affairs Committee of the XUAR, Zhu Hailun; Secretary of the Political and Legal Affairs Committee of the XUAR, Wang Mingshan; Head of Xinjiang Production and Construction Corps, Wang Junzheng; Director of the XUAR Public Security Bureau, Chen Mingguo, and the Public Security Bureau of the Xinjiang Production and Construction Corps

- State Security Minister of DPRK, Jong Kyong-thaek; Social Security Minister of DPRK, Ri Yong Gil; and the Office of the Prosecutor of the DPRK

- Libya’s Kaniyat Militia, its leader, Mohammed Khalifa Al-Kani and another senior member, Abderrahim Al-Kani

- Head of the Department of the Russian Ministry of Internal Affairs, Aiub Vakhaevich Kataev; Commander of the Russian Special Rapid-Response Unit (SOBR) Team “Terek”, Abuzaid Dzhandarovich Vismuradov

- Major General of the South Sudan People’s Defence Forces (SSPDF), Gabriel Moses Lokujo

- The government of Eritrea’s National Security Office

EU Council press release
Council Implementing Regulation (EU) 2021/478
Council Decision (CFSP) 2021/481
US OFAC designates Chinese officials over human rights violations in Xinjiang

The US Treasury Department’s Office of Foreign Assets Control (OFAC) announced on 22 March the designation of Wang Junzheng, the Secretary of the Chinese Party Committee of the Xinjiang Production and Construction Corps (XPCC), and Chen Mingguo, Director of the Xinjiang Public Security Bureau (XPSB), pursuant to Executive Order (EO) 13818 implementing the Global Magnitsky Human Rights Accountability Act.

According to OFAC, Wang is being designated for “having acted or purported to act for or on behalf of, directly or indirectly, the XPCC”, while Chen is being sanctioned for “being a foreign person who is a leader or an official of the XPSB”, which has engaged in serious human rights abuse related to Chen’s tenure. XPCC is a paramilitary organisation which was designated on 31 July 2020, while the XPSB is a government entity, which was designated on 9 July 2020, over being directly or indirectly connected to serious human rights abuse with respect to Uyghurs and members of other ethnic minorities in the Xinjiang Uyghur Autonomous Region.

Of a separate statement on the same day, US State Secretary Antony Blinken reiterated the US’ call for cessation of any repression or violation of the rights of Uyghurs in China, including by “releasing all those arbitrarily held in internment camps and detention facilities”.

The designations are being made in coordination with similar actions taken by the UK, the EU, and Canada, which also listed the two officials and several others, along with four entities, involved in serious human rights abuses in China, North Korea, Russia, South Sudan, and Eritrea.

Aperio Analysis by Vivien Li

For most businesses, it is unlikely that they will have direct dealings with the abovementioned sanctioned Chinese officials. However, it remains incumbent on businesses to demonstrate that they have adopted the necessary human rights policies and practices and should undertake "careful and robust" due diligence to ensure their operations do not directly or indirectly contribute to human rights violations. Business should also continuously monitor and improve their business processes aimed at mitigating human rights risks.

UN extends North Korea Panel of Experts

The UN Security Council (UNSC) passed resolution (UNSCR) 2569 on 26 March extending the mandate of the UN Panel of Experts assisting the sanctions committee on the Democratic People's Republic of Korea (DPRK) until 30 April 2022. The mandate also covers measures imposed by relevant 2016 and 2017 resolutions.

UNSC members request that the panel provides the sanctions committee with a work programme within 30 days of reappointment pursuant to UNSCR 1718 (2006), which established the sanctions committee. The panel is also instructed to submit a midterm report by 7 August and a final report by 28 January 2022.
US BIS issues final rule expanding Russia chemical weapons sanctions

The US Department of Commerce issued a final rule on 17 March to expand export controls on Russia imposed under the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991. This follows a conclusion reached on 2 March by the US Secretary of State that the Russian government has violated international law by using chemical or biological weapons against its own nationals, including the alleged use of the Novichok nerve agent against Sergei Skripal and Alexei Navalny.

The Department of Commerce states that the Russian government has acted in “flagrant violation” of commitments made under the Chemical Weapons Convention. The Bureau of Industry and Security (BIS) within the Department of Commerce confirmed that it will re-examine licence applications under a presumption of denial for exports and re-exports of national security items bound for Russia.

Licence applications will be re-examined under a presumption of denial for exports and re-exports of national security items bound for Russia.

BIS further states that it will suspend licence exceptions authorising the export and re-export of operation and sales technology and software and the replacement of parts and components. This reconsideration and suspension of licence applications is aimed at preventing Russia from accessing US technologies that might aid its use of chemical or biological weapons.

Aperio Analysis by George Voloshin

The latest US chemical weapons sanctions against Russia have little new in terms of content. Russia was already sanctioned by the Trump administration in August 2018 and, again, in August 2019 in connection with the 2018 poisoning of former spy Sergei Skripal and his daughter in Salisbury. The real question now is what the Biden administration’s response will be during the second round of chemical weapons sanctions implementation, beginning in June when it must report to Congress on whether Russia has altered its behaviour. The toughest this can get is the imposition of new broader sanctions against Russian sovereign debt. The 2019 sanctions were only imposed on non-ruble denominated primary debt issuances, meaning that US banks (interpreted broadly) could still take part in secondary market operations as well as in primary market bids for OFZ (Russian Treasuries denominated in rubles). In case of drastic restrictions on debt, for instance for all currencies and both the primary and secondary markets and/or with an unlikely but still possible extension to non-US persons, any such move could have tremendous consequences for Russia’s financial stability and the wellbeing of western investors with heavy exposure to Russian debt markets. Something to watch closely.
EU renews sanctions on former Ukrainian president and his inner circle

The Council of the European Union announced on 4 March that it will extend the existing asset freeze imposed on former Ukrainian president Viktor Yanukovych, his son Oleksandr Yanukovych and their close associates, for misappropriating state funds or abuse of office causing the loss of public assets, until 6 March 2022.

According to the amended regulations, former education minister Dmytro Tabachnyk and former first deputy prime minister Serhiy Arbuzov have been removed from the sanctions list. Sanctions against former health minister Raisa Vasylivna Bohatyriova have been extended until 6 September. The restrictive measures were first imposed on 18 individuals in March 2014 and subsequently extended on an annual basis.

In April 2017, more than three years after Yanukovych lost power after the Euromaidan protests, the new Ukrainian administration started a process of returning over £1 billion in assets that were allegedly misappropriated by the former president and government officials close to him.

EU revokes Egypt misappropriation sanctions framework, delists nine people

The Council of the European Union announced on 12 March that it has revoked the EU framework for sanctions against individuals responsible for misappropriating Egyptian state funds, ten years after the measures were first imposed. As a result, the EU Council has lifted restrictive measures against nine individuals, including members of the late president Hosni Mubarak’s family.

The decision was taken after the Court of Justice of the European Union (CJEU/ECJ) annulled on 3 December 2020 the EU asset freezes imposed on Mubarak and members of his family between 2016 and 2018. The ECJ found that the 2011 Council measures were taken without sufficient verification of the circumstances in which the former president was imprisoned in Egypt following the 2011 Arab Spring protests. The Court added that “the Council cannot conclude that a listing decision is taken on a sufficiently solid factual basis before having itself verified that the rights of the defence and the right to effective judicial protection were observed at the time of the adoption of the decision by the third state in question.”

The EU Council imposed sanctions against 19 Egyptian officials and their associates in March 2011 following mass civilian protests, with more than half having been delisted following the EU’s annual reviews.
UK government issues new list of high-risk third countries for AML purposes

The UK’s HM Treasury published on 24 March a new UK list of high-risk third countries for the purposes of enhanced customer due diligence requirements, under the Sanctions and Anti-Money Laundering Act 2018.

The Money Laundering and Terrorist Financing (Amendment) (High-Risk Countries) Regulations 2021 make amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 to review the definition of high-risk third country, as defined in the European Commission Delegated Regulation (EU) 2016/1675 for identifying states with strategic anti-money laundering and countering the financing of terrorism deficiencies.

The statutory instrument amends the definition of a high-risk third country to those identified in Schedule 3ZA to the MLRs 2017. According to the UK government’s money laundering advisory notice, the UK list replicates the 21 jurisdictions identified by the Financial Action Task Force as high-risk or under increased monitoring.

The statutory instrument was laid before parliament on 25 March and entered into force the following day.

Central Bank of Ireland announces AML/CFT registration obligations for VASPs

The Central Bank of Ireland announced on 16 March that the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2020, which transposes into national law the EU’s Fifth Money Laundering Directive (5MLD), will require virtual asset service providers (VASPs) to register for the purposes of anti-money laundering and countering the financing of terrorism (AML/CFT).

The Central Bank of Ireland will assess whether companies have effective AML/CFT procedures in place and whether their beneficial owners and senior executives meet the standards for fitness and probity in the financial system. VASPs will be required to apply for AML/CFT registration with the Central Bank, which will include providing evidence of its ML/TF risk assessment mechanisms, AML/CFT policies, training plans and reporting lines, as well as details regarding indirect ownership and management.

In addition, VASPs will be expected to conduct customer due diligence checks and to monitor transactions, and report any suspicious activity to Ireland’s Financial Intelligence Unit. AML/CFT breaches may result in enforcement action under the Irish Central Bank’s Administrative Sanctions Procedure.
UK government designates six individuals under Syria sanctions regime

The UK government's Foreign, Commonwealth and Development Office announced on 15 March the designation of six Syrian officials under the UK's autonomous sanctions regime, pursuant to the Syria (Sanctions) (EU Exit) Regulations 2019. The six individuals have been sanctioned for their role in the Bashar Al-Assad regime and the deteriorating human rights situation in Syria, according to Foreign Secretary Dominic Raab, who said they are being held "to account for their wholesale assault on the very citizens they should be protecting". The UK government's announcement coincides with the 10th anniversary of the Syrian uprising.

Those designated will be subject to asset freezes and travel bans.

The sanctioned individuals are:

- Foreign Affairs Minister Faisal Miqdad
- Media Adviser to the President Luna Al-Shibl
- Yassar Ibrahim, identified as an influential financier of President Al-Assad and front person for his personal economic interests
- Muhammad Bara' Al-Qatirji, whom the UK government accuses of benefiting the regime through oil and wheat trade deals
- Republic Guard Commander Major General Malik Aliaa, identified as being responsible for violence against civilians by his troops in 2019 to 2020 in northwestern Syria
- Army 5th Corps Commander Major General Zaid Salah, held responsible for violence against civilians during the Idlib offensive from April 2019

Canada and Australia sanction those involved in the construction of the Kerch Strait bridge

Canada’s Minister of Foreign Affairs Marc Garneau announced on 29 March sanctions on two individuals and four entities, in action coordinated with Australia’s Minister for Foreign Affairs Marise Payne who announced on 30 March that Australia has imposed sanctions against one individual and four entities. The Russian individuals and entities are being listed for their alleged involvement in the construction and operation of the Kerch Strait Railway Bridge, which links Russia to Crimea and Sevastopol.

The individuals and entities sanctioned by the Canadian and Australian governments are Aleksandr Nikolaevich Ganov, the Director General of JSC TC Grand Service Express; JSC Lenpromtransproyekt; JSC “The Berkakit-Tommot-Yakutsk Railway Line’s Construction Directorate”; Federal State Unitary Enterprise “Crimea Railway” (also known as Federal United Enterprise “Crimea Railways”); and First Crimean Insurance Company. The Canadian government has also designated one other individual, Leonid Kronidovich Ryzhenkin, the Deputy General Director for infrastructure projects at Stroigazmontazh.

All six were listed by the EU and the UK in October 2020.
Switzerland amends Anti-Money Laundering Act

The Swiss parliament adopted on 19 March amendments to the Anti-Money Laundering Act (AMLA), which includes requirements for financial intermediaries to conduct customer due diligence (CDD) checks and clarify the background and scope of transactions.

Under the new rules, financial intermediaries are expected to file suspicious activity reports with the Money Laundering Reporting Office when having a “well-founded suspicion” of the illegal origin of funds. In addition, associations which collect and distribute funds abroad for charitable, religious, cultural, educational or social purposes are required to be registered with the commercial registry, due to their increased risk of terrorist financing and money laundering.

Switzerland has been subject to the follow-up process by the Financial Action Task Force (FATF) since the publication of its mutual evaluation report in 2016. In February 2020, a FATF follow-up report found that the country is still only “partially compliant” with five recommendations and asked Switzerland to continue to report back on the progress made in implementing its anti-money laundering and counter terrorist financing standards.

The legislative improvements to AMLA were made to take forward FATF’s recommendations on undertaking CDD measures. However, lawyers, notaries, fiduciaries and other advisors remain excluded from the scope of the AMLA. In addition, the bill does not lower the current threshold of CHF 100,000 (£76,800) for cash payments in the trade in precious metals and stones, as required by FATF.

Aperio Analysis by Alex Kottke

Ostensibly the Swiss government’s revision to its anti-money laundering law is a step in the right direction for a country which has long been fabled for the primacy of financial secrecy. And yet, the term “half-measure” readily springs to mind. Granted, tightened requirements surrounding customer due diligence at financial institutions will be of general assistance in the fight against financial crime committed in or through Switzerland. But what about the potential gatekeepers of such activity, namely lawyers and financial advisors? Their exclusion from the scope of the amendment to the legislation underlines the enduring commitment to protect even those professionals who may be engaging in disreputable business. The financial lobby ultimately has won out in this respect during this round and the appeasing effect on international regulators – notably FATF – is therefore mitigated. Switzerland clearly still has some way to go to shake off its international image of complicity in financial malpractice.

UN renews its mission in South Sudan

The UN Security Council (UNSC) voted on 12 March to extend the UN Mission in South Sudan (UNMISS) for another year until 15 March 2022 following the adoption of UNSC resolution 2567 (2021). The resolution continues the four-pillar programme of protecting civilians, allowing for humanitarian aid, supporting the peace process, and investigating human rights violations.

The resolution also sets out a three-year plan for preventing a return to civil war in the nation and calls on all parties in the country to immediately halt the current violence.

It further expresses the UNSC’s intent to consider appropriate actions against those who undermine peace and security in the region, reminding member states of their obligations to halt the sale or transfer of weapons to South Sudan.
Russia passes draft law that would allow MPs to avoid responsibility for anti-corruption breaches in certain circumstances

The Russian State Duma passed on 10 March a draft law during its first reading that would allow Russian MPs and state officials to avoid responsibility for contravening anti-corruption laws in certain "uncontrollable" circumstances.

The draft law would apply to judges, prosecutors, election committee members, employees of state-owned companies, military personnel and government officials. The draft bill includes the following examples of circumstances beyond an individuals’ control: natural disasters, epidemics, labour strikes, terrorist acts, restrictive measures adopted by foreign governments, such as sanctions, and military campaigns.

Instances of violations would have to be rectified within one month from the end of the circumstances in question and the removal of responsibility applicable to the individual would be determined by a special compliance commission.

The draft law states that violations of anti-corruption laws include non-compliance with unspecified restrictions and prohibitions, violations of conflict of interest rules and non-fulfilment of obligations, such as the failure to file income or property declarations. The law would not protect individuals from liability for criminal acts such as bribery.

Aperio Analysis by Claire Burchett

Although the draft bill is likely to be put into the context of the recent investigations by Russian opposition leader Alexei Navalny into the alleged secret palace of Russian President Vladimir Putin, as a way to legalise corruption, it has actually been in discussion since early 2019 and was registered in late 2020. Proponents of the proposed law have argued that the role of the special commission under the new law would mean that specialised anti-corruption agencies would be free to focus on more complex and serious corruption cases. However, while the examples of non-compliance with anti-corruption laws given in the draft does not include criminal acts, the examples of violations are vague, and the rationale to be used by the commission for removing responsibility is unclear, possibly leaving the law open to exploitation.

US renews national emergency on Iran

US President Joe Biden announced on 5 March the continuation for another year of the national emergency with respect to Iran, which was declared by Executive Order (EO) 12957 of 15 March 1995, pursuant to the International Emergency Economic Powers Act.

According to the White House notice, the actions of Iran’s government, including its proliferation of missiles and other asymmetric and conventional weapons, its assistance to terrorist groups and the Islamic Revolutionary Guard Corps’ hostile activities “continue to pose an unusual and extraordinary threat to the national security, foreign policy and economy of the US”.

The national emergency declared by EO 12957 is distinct from that declared on 14 November 1979 by EO 12170 in connection with Iran’s hostage crisis, which was renewed separately on 12 November 2020.
US State Department designates ISIS-DRC and ISIS-Mozambique and their leaders

The US State Department designated on 10 March two affiliate branches of the Islamic State of Iraq and Syria (ISIS) in the Democratic Republic of the Congo (DRC) and Mozambique as well as the leaders of each organisation.

ISIS-DRC and ISIS-Mozambique have been designated as foreign terrorist organisations pursuant to Section 219 of the Immigration and Nationality Act as well as specifically designated global terrorists (SDGTs) pursuant to Executive Order (EO) 13224. Seka Musa Baluku, the leader of ISIS-DRC, and Abu Yasar Hassan of ISIS-Mozambique are likewise designated as SDGTs. Both groups and their leaders are subject to asset and property freezes, travel bans, and restrictions on engaging in any transactions with US individuals or entities, with foreign financial institutions subject to sanctions if they facilitate funds on their behalf.

The two groups were reportedly founded after the April 2019 launch of the Islamic State Central Africa Province and operate as distinct groups, contrary to ISIS-affiliated media portrayals, according to the State Department. ISIS-Mozambique also goes by the name Ansar al-Sunna or al-Shabaab and is believed to be responsible for over 1,300 deaths and displacement of 670,000 civilians since 2017 under Hassan’s leadership.

ISIS-DRC is accused of killing nearly 850 civilians in the DRC last year, as well as launching attacks against military units in the area. The group is also known as the Allied Democratic Forces (ADF), and under that name was sanctioned in 2014 by the UN Security Council and the US Treasury Department. Baluku and five of his associates in the ADF were also designated in 2019 under the Global Magnitsky sanctions regime for human rights violations, and all six were sanctioned by the UN in 2020. The 2019 ADF and Baluku designations were updated on 10 March.

OFAC revokes Dan Gertler licence granted in the final days of the Trump administration

A US State Department spokesperson announced on 8 March that the Treasury Department’s Office of Foreign Assets Control (OFAC), in consultation with the State Department, has revoked the 15 January 2021 licence granted to mining tycoon Dan Gertler in the final days of the Donald Trump administration.

The spokesperson noted that that the year-long licence, which was issued pursuant to the Global Magnitsky Sanctions Regulations and authorised all transactions and activities necessary for Gertler and related entities, “is inconsistent with America’s strong foreign policy interests in combatting corruption around the world”, with reference to US anti-corruption and stability efforts in the Democratic Republic of the Congo (DRC).

The US Treasury’s 2017 designation of Gertler as a specially designated national identified the Israeli national as a “billionaire who has amassed his fortune through hundreds of millions of dollars’ worth of opaque and corrupt mining and oil deals in the DRC”.

Bloomberg reported on 19 March that the lobbying efforts to secure Gertler’s January reprieve came after multiple requests by Israel’s Ambassador to the US Ron Dermer and Israeli Intelligence Chief Yossi Cohen, who reportedly told US officials that Gertler is a national security asset.
EU resolution proposes law on corporate due diligence and accountability for supply chains

The European Parliament (EP) adopted on 10 March resolution 2020/2129 (INL), setting out principles for proposed new legislation on corporate due diligence (DD) and accountability for human rights, environmental and governance implications within businesses’ supply chains. The resolution calls for the urgent adoption of a directive by the European Commission that requires mandatory DD procedures and ensures companies are held accountable when involved in violations.

The document provides recommendations aimed at influencing the Commission’s future proposal for a directive on sustainable corporate governance, including mandatory human rights and environmental DD with regards to impacts across supply chains, which the Commission has committed to publish in the second quarter of 2021. The resolution also provides expansive definitions on the scope of the proposed requirement and calls for the publication of general non-binding guidelines for undertakings on how to comply with DD obligations.

The adoption of the resolution follows a 11 October 2020 report by Lara Wolters MEP, who stated during an 8 March EP debate on corporate DD and accountability that “businesses fully understand that mandatory standards are the only path to a level playing field and to business certainty” and that “due diligence should be exercised by all companies with risks in their supply chains”. Didier Reynders, the EU’s Commissioner for Justice, stressed that “we want to incentivise outside of the EU good practice that protects the environment in line with our international commitments and our efforts on climate change and environmental protection”, adding that the EU Commission’s proposal will take a “holistic approach, where due diligence is part of sustainable corporate governance”.

The Parliament also calls on the Commission to propose a negotiating mandate for the EU to constructively engage in the negotiation concerning a legally binding UN instrument to regulate the activities of transnational corporations and other businesses on international human rights law.

On 31 March, organisations representing indigenous peoples, Afro-descendant peoples and other peoples and communities with collective rights and traditions, as well as human rights, land, and environmental defenders, sent an open letter to the President of the EU Commission Ursula von der Leyen, and the Commission’s Directors General for Environment and Justice, recommending a set of elements to be considered in upcoming legislative measures. The recommendations include mandating that all EU companies and investors undertake transparent combined and integrated human rights and environmental DD and requiring human rights and environmental impact assessments to be carried out as part of the process.

EP recommendations include

- The proposed DD obligations should require taking all commensurate measures to prevent, cease, mitigate, and address adverse impacts on human rights, the environment and good governance from occurring in their value chains. In addition, undertakings should be required to communicate their DD strategy to workers’ representatives, affected stakeholders, and national competent authorities
- Member state governments should be responsible for implementing and enforcing measures imposed pursuant to the proposed law, designating one or more national competent authority to carry out risk-based or factual investigations
- Undertakings should be required to provide a grievance mechanism, allowing any stakeholder to express reasonable concern regarding the existence of a potential or actual adverse impact on human rights, the environment or good governance
- To ensure a level playing field for EU businesses, the resolution recommends that proposals should extend not only to defined categories of EU businesses but also to equivalent categories of non-EU businesses operating in the European single market through the supply of goods or services. Furthermore, the rules should also apply to publicly listed SMEs and high-risk SMEs, which should receive technical assistance on complying with the requirements
UK Treasury issues proposals for Emissions Trading Scheme regulatory framework

On 8 March, the FCA published a consultation on regulating emissions bidding under the UK ETS

In addition, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 will be amended to ensure that the UK ETS is governed by the anti-money laundering and countering the financing of terrorism (AML/CFT) regime, including for the trading of carbon emissions allowances. The proposed amendments would reference the appropriate AML/CFT provisions to reflect the UK’s departure from the EU and will incorporate the relevant prohibitions against financial crime in the trading of UK allowances.

If approved, the SI will be governed by the Greenhouse Gas Emissions Trading Scheme Auctioning Regulations 2021, which are yet to be adopted. The UK ETS is expected to take effect later in the year, according to the explanatory memorandum.

On 8 March, the FCA published Consultation Paper (CP) 21/6 on regulating emissions bidding under the UK ETS, which accompanies government efforts in relation to the UK emissions auction platform and trading allowances in the secondary market. The proposed amendments are made to reinstate provisions that enable the supervision of UK businesses intending to bid on the auction platform, which became ineffective at the end of the EU transition period. The proposed measures cover the FCA’s options when dealing with AML/CFT failures by regulated entities and changes to the technical standards under the UK Market Abuse Regulation. The consultation ran until 6 April.

The UK Department for Business, Energy and Industrial Strategy (BEIS) published on 10 March updated guidance on the UK ETS, which replaces the UK’s participation in the EU ETS.

The UK’s HM Treasury laid the Recognised Auction Platforms (Amendment and Miscellaneous Provisions) Regulations 2021 before parliament on 8 March. The draft statutory instrument (SI) amends the UK’s financial services legislation to enable the auctioning of carbon emissions allowances, as part of the wider effort to establish a UK Emissions Trading Scheme (ETS) after the UK’s exit from the EU.

The draft SI includes emissions allowances in the scope of financial instruments, by amending the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO). To help detect and fight market abuse, the act of bidding in a UK emissions allowance auction would become a regulated activity requiring authorisation from the Financial Conduct Authority (FCA).
US-renews-national-emergencies-concerning-Ukraine-Venezuela-and-Zimbabwe


EU-imposes-first-sanctions-under-human-rights-regime-against-four-Russians-over-Navalny


US designates Russian officials and entities over Navalny and restricts exports

The US Treasury Department's Office of Foreign Assets Control (OFAC) designated on 2 March seven individuals pursuant to Executive Order (EO) 13661 for their involvement in the poisoning or imprisonment of Russian opposition figure Alexei Navalny. The State Department concurrently announced several Russian designations pursuant to the Countering America's Adversaries Through Sanctions Act (CAATSA) and EO 13382 on weapons of mass destruction proliferation.

OFAC's designations include the Kremlin's Domestic Policy Directorate Chief Andrei Yarin, First Deputy Chief of Staff of the Presidential Executive Office Sergei Kiriyenko, and Deputy Ministers of Defence Aleksei Krivoruchko and Pavel Popov. Additionally, the list includes Federal Security Service (FSB) Director Alexander Bortnikov, Federal Penitentiary Service (FSIN) Director Alexander Kalashnikov, and Prosecutor General Igor Krasnov. Bortnikov has also been designated pursuant to EO 13382 for "acting or purporting to act for or on behalf of, directly or indirectly" the FSB.

The US State Department announced on the same day the designation of the 27th Scientific Centre, 33rd Scientific Research and Testing Institute, 48 Central Scientific Research Institute Sergeiv Posad, 48 Central Scientific Research Institute Kirov, 48 Central Scientific Research Institute Yekaterinburg, and State Scientific Research Institute of Organic Chemistry and Technology (GoSNIIOKhT), pursuant to CAATSA for operating for or on behalf of, the Russian defence or intelligence sectors.

The FSB, GoSNIIOKhT, 33rd Scientific Research and Testing Institute, 27th Scientific Center, the Main Russian Intelligence Directorate (GRU), and GRU officers Anatoliy Vladimirovich Chepiga and Alexander Yevgeniyevich Mishkin have also been designated by the State Department pursuant to EO 13382 for their involvement in activities or transactions "that have materially contributed to, or pose a risk of materially contributing to, the proliferation of weapons of mass destruction or their means of delivery".

In addition, the State Department’s Directorate of Defense Trade Controls announced that it would amend the International Traffic in Arms Regulations 126.1 to include Russia on the "list of countries subject to a policy of denial for exports of defence articles and defence services, with certain exceptions for exports to Russia in support of government space cooperation". After a 15-day Congressional notification period, all US foreign assistance to Russia, arms sales, arms sales financing, and financial assistance will be terminated, and exports of national security sensitive goods and technology will be prohibited for a minimum of 12 months starting from the date of publication in the Federal Register. Several waivers will be available.

Concurrently, the US Department of Commerce announced the addition of 14 entities to the Bureau of Industry and Security’s Entity List for "their proliferation activities in support of Russia's weapons of mass destruction programs and chemical weapons activities".

On the same day, the EU Council announced the first set of designations under the recently established Global Human Rights Sanctions Regime against Russians deemed to be involved in Navalny’s imprisonment, which includes the Head of the Investigative Committee of the Russian Federation, Alexander Bastrykin, along with Krasnov, Kalashnikov, and the Head of the National Guard, Viktor Zolotov.

| OFAC notice |
| Identifying information |
| Department of State press statement |
US BIS adds 14 to the Entity List for supporting Russian WMD and chemical weapons activities

The US Commerce Department's Bureau of Industry and Security (BIS) announced on 2 March the addition of 14 organisations to its Entity List, all of which are in Russia, Germany, or Switzerland and allegedly support Russian weapons of mass destruction (WMD) proliferation and activities involving the use of chemical weapons.

This latest action supplements the August 2020 addition of five Russian government sites to the Entity List for acting in support of chemical and biological weapons programmes.

The Entity List restricts the export, re-export, and in-country transfer of items subject to the Export Administration Regulations (EAR) to those reasonably believed to be involved, or to pose a significant risk of becoming involved, in activities contrary to the national security or foreign policy interests of the US.

The Entity List now includes:
- Chimmed Group in Germany
- Chimconnect BmbH
- Chimconnect AG in Switzerland
- Pharmkontract GmbH in Germany
- Femteco
- Interlab
- LabInvest
- OOO Analit Products
- OOO Intertech Instruments
- Pharmkontract GC
- Rau Farm
- Regionsnab
- Riol-Chemie in Germany
- 27th Scientific Center of the Russian Ministry of Defence

OFAC designates two Houthi military leaders

The US Treasury Department's Office of Foreign Assets Control (OFAC) announced on 2 March its decision to designate two leaders of the Yemeni rebel group Ansar Allah, also known as the Houthi movement, pursuant to Executive Order (EO) 13611.

Houthi Naval Forces Chief of Staff Mansur Al-Sa'adi is said to have planned “lethal attacks against international shipping in the Red Sea” and to have helped smuggle Iranian-made weapons into the country. Ahmad 'Ali Ahsan al-Hamzi, a Commander in the Yemeni Air Force and Air Defence Forces, is supposed to have directed targeted drone strikes and to have acquired weapons from Iran for use in the Yemeni civil war. Both have received training in Iran, according to the OFAC press release.

The decision comes after Ansar Allah was briefly named as a specially designated global terrorist (SDGT) and foreign terrorist organisation (FTO), pursuant to EO 13224 on 19 January. Three of its leaders were designated amid widespread concern that sanctions might disrupt humanitarian aid efforts. US State Secretary Antony J. Blinken announced on 12 February the Department's decision to remove the SDGT and FTO designations, while keeping in place measures applicable to all those placed on the specially designated nationals (SDN) list.

The sanctions involve asset freezes, a prohibition on transactions involving the blocked persons and an interdiction to provide them with funds or other forms of support.
OFAC designates Mexican cartel collaborator over drug trafficking and money laundering

The US Treasury Department’s Office of Foreign Assets Control (OFAC) announced on 3 March the designation of fugitive Mexican citizen Juan Manuel Abouzaid El Bayeh as a specially designated narcotics trafficker pursuant to the Foreign Narcotics Kingpin Designation Act, for allegedly facilitating money laundering (ML) and narcotics shipments to the US for the Mexican drug trafficking organisation Cartel de Jalisco Nueva Generacion (CJNG).

According to OFAC, Abouzaid has been designated for providing financial and technological support, as well as goods and services to CJNG, in order to assist the criminal network with international drug trafficking. As a result of OFAC’s action, Abouzaid El Bayeh’s property and interests in property in the US or in the possession or control of US persons must be blocked.

In June 2020, Abouzaid was among the 1,770 individuals whose bank accounts were frozen by the Mexican authorities for links to the CJNG. In addition, in October 2018, the US Department of Justice (DOJ) unsealed an indictment charging Abouzaid with conspiracy to distribute cocaine and methamphetamine with the intention that it would be imported into the US.

OFAC issues cyber-related GL and FAQs

The US Treasury Department’s Office of Foreign Assets Control (OFAC) issued on 2 March cyber-related General License (GL) 1B authorising certain transactions with the previously designated Russian Federal Security Service (FSB), which are otherwise prohibited pursuant to Executive Order (EO) 13757, the Cyber-Related Sanctions Regulations, the Weapons of Mass Destruction Proliferators Sanctions Regulations, and the Countering America’s Adversaries Through Sanctions Act (CAATSA).

GL 1B authorises certain transactions and activities with the FSB which are necessary and ordinarily incident to FSB acting in its administrative, investigatory and law enforcement capacities or which are needed for complying with its rules. Additionally, it authorises certain other transactions and activities that are necessary and incident to the requesting, receiving, utilising, paying for, or dealing in licences, permits, certifications, or notifications issued or registered by the FSB and are related to the importation, distribution, or use of IT products in the Russian Federation, provided certain criteria are met.

At the same time, OFAC clarifies that these exemptions are applicable provided that the concerned exportation, re-exportation, or provision of any goods or technology that are subject to the Export Administration Regulations (EAR) are licenced by the US Department of Commerce.

OFAC underlines that GL 1B does not authorise the exportation, re-exportation, or provision of any goods, technology, or services to the Crimea region of Ukraine, nor the transfer of any property or debiting of any account blocked pursuant to other regulations, or any other blocked transactions or activities or involving blocked persons.

Additionally, OFAC amended three related frequently asked questions (FAQs), 501, 502, and 503. GL 1B, which is applicable from 2 March, replaces and supersedes in its entirety GL 1A.
CONSULTATIONS

UK consultation on restoring trust in audit, includes proposal on fraud prevention

The UK Department for Business, Energy and Industry Strategy published a white paper for consultation on 18 March setting out the government’s proposals to strengthen the UK’s auditing framework and restore public trust by establishing a new regulator to enforce corporate reporting regulations. The policy proposals include new obligations on both auditors and directors relating to the detection and prevention of material fraud and granting powers to the new regulator to enact civil sanctions, including fines and action orders, on entities and senior company leaders who breach the requirements.

Chapter 6 (starting on page 93) of the white paper focuses on the purpose and scope of audit, which includes proposals on establishing a new corporate auditing profession, new principles for auditors to reinforce good audit practice, a new duty on auditors to take a wider range of information into account in reaching audit judgments, and new obligations on auditors and directors relating to the detection and prevention of material fraud.

More specifically, the Brydon Review identified fraud and auditors’ related responsibilities as the most complex and misunderstood of all the topics it covered. As such, the government agrees that a holistic approach is needed in relation to fraud and proposes to legislate to require directors of Public Interest Entities to report on the steps they have taken to prevent and detect material fraud. The white paper asks respondents whether they agree with the government’s proposed response to the package of reforms relating to fraud.

The policies offered in the white paper also purportedly aim to ensure responsible governance of the most significant UK corporate entities, maintain best practices at a global level, and provide access to reliable company performance information for investors, creditors, employees, and other stakeholders.

The white paper’s executive summary states that the government agrees with the findings of all three reviews and that problems with corporate reporting and audit are by no means exclusive to the UK, as the recent discovery of the “major fraud” at German payment processor Wirecard illustrates.

In response to the CMA study, the white paper proposes putting in place a mandatory managed shared audit requirement for FTSE 350 companies that are registered in the UK. Under the proposals, regulators will have enforcement and sanctioning powers against companies that violate the new regulation, including proportionate financial penalties levied for audit information delays or failures to provide necessary information.

Comments on the policy proposals will be accepted until 8 July.

UK government press release
UK government documents
Consultation paper
US agencies request information on the use of AI by financial institutions

Five US federal financial regulatory agencies, namely the Federal Reserve Board, the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA) and the Office of the Comptroller of the Currency (OCC), issued a request for feedback on 29 March on the use of artificial intelligence (AI) by financial institutions.

The request for information (RFI) seeks insight from financial institutions, trade associations, consumer groups, and other relevant stakeholders on the increasing application of AI by financial institutions, including for fraud prevention, personalisation of customer services, and credit underwriting. The RFI aims to enable US regulators to better understand the use of AI applications by financial institutions, such as machine learning; the risk, control and governance of AI; as well as the challenges faced in building and implementing AI applications.

According to the RFI, financial institutions are using AI to help flag potential suspicious transactions and fraud detection; analyse data; and to improve cybersecurity such as detecting compromising activities.

The RFI was published in the Federal Register on 31 March and is open for comments until 1 June 2021.

FATF consults on updated guidance on risk-based approach to virtual assets and VASPs

The Financial Action Task Force (FATF) issued a consultation on 19 March on proposed updates to its guidance on the risk-based approach to virtual assets (VAs) and virtual asset service providers (VASPs).

The guidance is being updated to include anti-money laundering and countering the financing of terrorism (AML/CFT) requirements for VAs and VASPs following FATF’s 12-month stablecoin review and the G20 report on stablecoins.

The updated guidance includes revised VA and VASP definitions, stablecoin guidance, peer-to-peer transaction risk guidance, VASP registration guidance, travel rule implementation guidance for the public and private sector, and principles of information sharing and cooperation among VASP supervisors.

The FATF is seeking comment on how peer-to-peer transactions are currently being used for ML/TF, how such activities can be identified, and the options available to mitigate peer-to-peer ML/TF risks.

The FATF also seeks feedback from the private sector on whether a second 12-month review is needed to address issues raised that fall outside the current proposal’s scope, which will be considered in June.

The consultation is open until 20 April.
FATF consults on new non-binding guidance on proliferation financing

The Financial Action Task Force (FATF) launched on 1 March a public consultation on developing new non-binding guidance on proliferation financing, which seeks to assist public and private sector entities in identifying and mitigating proliferation financing risk as defined in newly revised Recommendation 1.

FATF Recommendation 1 was updated in October 2020 to require countries, financial institutions and designated non-financial businesses and professions (DNFBPs) to assess their exposure to proliferation financing risk, which “refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7”, applicable to the Democratic People’s Republic of Korea and Iran country-specific regimes.

The FATF is seeking comments on whether the draft guidance provides enough clarity on risk mitigation methods that companies are expected to adopt, the risk-based approach in the context of proliferation financing and the new obligations introduced in October 2020. In addition, financial institutions are encouraged to suggest other risk indicators, alongside those related to the customer profile, account and transaction activity, maritime sector and trade finance.

The draft guidance notes that risk assessment measures should be implemented proportionately, in relation to the context the entity operates in, its risk profile and the particularities of the sector. According to FATF, the new guidance will not supersede its 2018 guidance on counter proliferation financing, which remains relevant.

Interested entities can submit their responses and drafting proposals to FATF by 9 April. According to the consultation feedback, the revised text of the guidance will be analysed during FATF’s June plenary meeting.

FATF launches study on mitigating unintended consequences of FATF standards

The Financial Action Task Force (FATF) announced on 17 March that it has launched a new project in February to study and mitigate the unintended consequences resulting from the incorrect implementation of FATF standards.

The project will be conducted in two phases: Phase One will focus on research and engagement, which includes gaining insight into the experience of relevant stakeholders about the unintended consequences from the misuse of anti-money laundering and counter financing of terrorism (AML/CFT) standards implementation. Phase Two aims to develop options for preventing and mitigating the unintended consequences identified.

According to the FATF, the four key areas of focus for the project are de-risking, financial exclusion, suppression of non-profit organisations (NPOs) or the NPO sector, and threats to human rights. The latter could involve due process rights violations or opportunities for a fair trial being rescinded because of abuse of AML/CFT regulations. Likewise, NPO suppression is listed as a possible result of a failure to implement the risk-based approaches advised by the FATF. In addition to NPOs, money value transfer service providers and corresponding banking relationships are also mentioned as potential victims of de-risking as a result of improper FATF standards implementation.

Comments are welcome throughout the project, but particularly during Phase One, if submitted on or before 20 April.
US SEC consults on amendments to the Holding Foreign Companies Accountable Act

The US Securities and Exchange Commission (SEC) announced on 24 March that it has launched a public consultation on its interim final amendments to implement the disclosure and submission requirements of the Holding Foreign Companies Accountable Act (HFCA Act), which will oblige firms to report whether they are controlled by a foreign government, have Chinese Communist Party officials on their board and whether government entities own shares in the company.

The interim final amendments will apply to issuers that file “an annual report with an audit report issued by a registered public accounting firm that is located in a foreign jurisdiction”, as well as to registrants for which the Public Company Accounting Oversight Board (PCAOB) was unable to conduct complete inspections due to restrictions imposed by authorities in a foreign jurisdiction.

The HFCA Act was signed into law on 18 December 2020 and requires auditors of foreign companies to allow the PCAOB to oversee their audits and to prohibit them from trading on the US market when they fail to comply with US auditing rules for three consecutive years. Companies identified by SEC as foreign issuers of securities must disclose for each non-inspection year information such as the percentage of shares owned by government entities where the firm is incorporated and whether these entities have a controlling interest, as well as information regarding affiliations with the Chinese Communist Party.

EU Commission consults on amending the Directive on Administrative Cooperation

The European Commission (EC) launched on 10 March a public consultation on its proposed revisions to the Directive on Administrative Cooperation (DAC8), focused on strengthening the fight against tax fraud and evasion, and introducing amendments on cryptoassets and e-money.

The consultation invites responses from stakeholders in private companies, government bodies, research institutions, and non-governmental organisations. The EC aim is to gather views on the use of cryptoassets and e-money as well as on what information is available about customers and transactions, with an additional focus on possible reporting and compliance mechanisms.

The EC has previously issued a call for feedback in relation to the proposed roadmap and the inception impact assessment. The latter, published in November 2020, explains that the DAC8 proposal aims to increase cooperation between tax authorities and keep compliance costs low while tackling tax evasion and other related risks associated with cryptoassets. The current directives do not require crypto brokers to report to tax administrations, resulting in a lack of information and sanctions disparities, the document explains. The Commission received and published nine responses, including from audit firm KPMG and digital currency exchange platform Coinbase.

The proposal forms part of the EUs wider legislative package on regulating cryptoassets and e-money, aimed at fortifying the bloc’s digital finance strategy and other measures. The consultation is open until 2 June with the proposal for a directive planned for the third quarter of the year.
The European Banking Authority (EBA) launched a consultation on 17 March on proposed changes to its guidelines on risk-based supervision of financial and credit institutions’ anti-money laundering and counter financing of terrorism (AML/CFT) obligations.

The proposed changes are intended to address obstacles to effective AML/CFT supervision, including the effective use of different supervisory tools, that were identified in a review of the 2016 guidelines.

The revised guidelines emphasise the need for a comprehensive risk assessment at sectoral and sub-sector levels as well as the importance of robust follow-up processes and having available clear options to consider in determining follow-up actions.

Changes include step-by-step guidelines in areas of supervision that responding entities report difficulties with and additional guidance on putting into place robust supervisory strategies and plans which “ensure that competent authorities allocate their supervisory resources according to the risk exposure of subjects of assessment”.

Training guidance is also featured in the revised guidelines in terms of clarifying what types of training competent authorities ought to provide their staff.

The revised guidelines proscribe greater cooperation between competent authorities, stakeholders, financial intelligence units, tax authorities, AML/CFT authorities in third countries, and law enforcement. Furthermore, they stress the need for supervisory cooperation over domestic groups and individuals as well as cross-border groups or activities.

Responses to the consultation will be accepted until 17 June.

The UK’s HM Revenue & Customs (HMRC) announced on 23 March that it is seeking comments on ways to utilise data to help taxpayers better understand offshore tax rules and obligations and on raising standards in the tax advice market, by defining tax advice and introducing a requirement for all tax advice providers to hold professional indemnity insurance (PII). HMRC is also consulting on proposed measures to tackle the promotion of tax avoidance schemes.

The first consultation document discusses how HMRC could use data to assist taxpayers in understanding and complying with offshore tax obligations and seeks views on the causes of non-compliance and how to improve compliance.

The second consultation seeks views on the UK government’s proposal to introduce a requirement for tax advisers to hold PII, including minimum levels of cover, and ways of enforcing and effectively implementing the policy. To determine who should be mandated to hold PII, HMRC also seeks to define what constitutes tax advice.

A third consultation seeks views on a set of new measures, including additional powers for HMRC to publish details of promoters and suspected schemes, and strengthened sanctions, aimed at tackling promoters and enablers of tax avoidance.

The consultations on supporting taxpayers with offshore tax matters and mandating PII for tax advisers are open until 15 June 2021, and for the consultation on tackling promoters of tax avoidance comments are being accepted until 1 June 2021.
Greensill Capital UK facing US fraud complaint

US coal mining company Bluestone Resources Inc filed on 16 March a civil complaint in the US District Court for the Southern District of New York against Greensill Capital (UK) Ltd, claiming that the supply chain finance firm sought to defraud it in relation to a $850 million financing arrangement. The UK Labour party has called for an inquiry into the relationship between the group’s founder, Alexander David Greensill, known as Lex Greensill, and former prime minister David Cameron, who became an adviser to the company in 2018.

Greensill’s business model was reportedly based on prospective receivables. In the absence of Bluestone registering receivables, debt was rolled over and sold as bonds to Credit Suisse Asset Management (CSAM). According to a 16 March press release, Credit Suisse has suspended and liquidated $10 billion in supply chain finance funds, most of which originated and was structured by Greensill Capital.

The relationship between Greensill and the Swiss bank was unknown to Bluestone, according to the complaint, with the plaintiffs arguing that Credit Suisse’s decision to wind-down funds made the finance firm pressure Bluestone for repayments to cover the liquidity gap. The complaint alleges that this formed part of “a pattern of material misrepresentations”, in which Greensill committed fraud, unjust enrichment, civil conspiracy, as well as breaches of contract, its duty of care and fiduciary duty.

Germany’s Federal Financial Supervisory Authority (BaFin) issued on 3 March a moratorium on the supply chain finance firm’s subsidiary, Greensill Bank AG, citing worries that the financial institution might become over-indebted. At the regulator’s request, insolvency proceedings were opened against the bank on 16 March. BaFin appointed a special representative at Greensill Bank in January after it ordered a forensic report on the company. The regulator filed a criminal complaint after the financial institution allegedly could not provide proof of certain collateral. An internal report reviewed by the Wall Street Journal claims that the regulator received tips about potential fraud in 2020, with whistleblowers alleging that some of the bank’s assets were backed by false invoices.

In response to a parliamentary question, the UK HM Treasury Minister of State Theodore Agnew underlined that the two companies operating in the UK, Greensill Capital UK and Greensill Capital Securities Ltd, are not authorised by the UK financial authorities. Greensill Capital UK is subject to the Financial Conduct Authority’s supervision under anti-money laundering regulations only, while Greensill Capital Securities was an Appointed Representative of a regulated firm, Mirabella Advisers. Lord Agnew added that UK regulators are working to assess the impact of these developments on the British financial sector. Lord Agnew further stated that no member of the Greensill group was authorised or supervised by the Bank of England, while Greensill Capital was approved as a lender in the Coronavirus Large Business Interruption Loan Scheme (CLBILS) by the state-owned British Business Bank.

Several UK MPs are calling on the Cabinet Office to investigate the connections between the Cameron administration and Greensill, after a business card from 2012 showed that Lex Greensill served as senior advisor. According to an official statement cited in a 31 March letter to Cabinet Secretary Simon Case, Lex Greensill worked as a supply chain finance advisor to Cameron between 2012 and 2015 and acted as a Crown Representative from 2013 to 2016. Documents leaked to the Sunday Times claim that Greensill’s appointment was not formally announced.

The Financial Times reported on 16 March that the former PM allegedly approached current cabinet members to secure financial help for Greensill through the Bank of England’s Covid Corporate Financing Facility. Cameron’s efforts reportedly include multiple text messages sent to Chancellor of the Exchequer Rishi Sunak in April last year, according to a 20 March article by the Sunday Times.
US court grants Xiaomi temporary injunction and OFAC publishes two related FAQs

A US District Court judge for the District of Columbia granted an injunction on 12 March to Chinese technology giant Xiaomi Corporation, which temporarily prevents the US Department of Defence from enforcing its designation of the company as a “Communist Chinese Military Company” (CCMC) under the National Defence Authorisation Act. The ruling entered effect on 15 March.

Judge Rudolph Contreras held that the plaintiffs, the company and three shareholders, demonstrated a high likelihood of success in their Administrative Procedure Act (APA) challenge of the Defence Department’s assertion that Xiaomi is a CCMC, following the Department’s listing of the company on 14 January pursuant to Executive Order (EO) 13959. The court notes that the Defence Department did not offer an explanation for the designation at the time, and that the two factual grounds as basis for evidence subsequently submitted to the court are “shaky” and “inadequate” and do not pass the court’s APA review. Judge Contreras further agreed with Xiaomi’s claim that the CMCC designation was unlawful, violating the Department’s statutory authority.

The US Treasury Department’s Office of Foreign Assets Control (OFAC) published on 14 March two new frequently asked questions (FAQs), the first informing all relevant stakeholders that the stipulations laid forth in EO 1395 no longer apply to Xiaomi pending further court proceedings. The second, FAQ 881, notes that the previous Secretary of Defence on 14 January erroneously listed Luokung Technology Corporation (LKCO) pursuant to Section 4(a)(ii) of EO 13959 as “Luokong”. Secretary of Defence Lloyd Austin removed the erroneous name on 14 March and re-listed LKCO. Therefore, the prohibition on LKCO will apply beginning 60 days after 9 March. Meanwhile, the prohibition listed in EO 13959 Section 1(c) will enter into effect on 9 March 2022.

Luokung Technology Corp files motion in US District Court to block CMCC restrictions

Luokung Technology Corporation announced on 5 March that it has filed a motion in the US Federal District Court for the District of Columbia to grant a temporary restraining order blocking the enforcement of Executive Order 13959 in light of Luokung’s 14 January designation by the Department of Defence as a “Communist Chinese Military Company” (CCMC). The complaint alleges that the company’s designation as a CMCC and the associated restrictions imposed by the US government are unlawful. The company seeks to qualify for the 27 May extension of a ban on transactions and activities pursuant to EO 13959 granted by OFAC General License 1A to certain CMCCs “whose name closely matches, but does not exactly match” the exact CCMC. Luokung claims that its designation does not match the company name exactly and should therefore receive the extension. Luokung CEO Xuesong Song stated in a press release that the company “is not a CMCC and is not a state-owned enterprise”.

On 14 March, OFAC released a FAQ acknowledging the 14 January listing’s incorrect spelling of “Luokong” and announced that Secretary of Defense Lloyd Austin removed the erroneous name and re-listed the company the same day. Therefore, the prohibition on the company will apply beginning 60 days after 9 March. Meanwhile, the prohibition listed in EO 13959 Section 1(c) will enter into effect on 9 March 2022.
Italian court acquits Shell and Eni in Nigeria OPL 245 corruption case

Multinational energy companies Royal Dutch Shell plc and Eni S.p.A were acquitted of international corruption charges on 17 March by a Milan Tribunal in Italy, in relation to securing offshore oil prospecting licence (OPL) 245 in Nigeria in 2011.

The charges against a total of 15 defendants were dismissed, including two former Shell executives, Malcolm Brinded and Peter Robinson, and two ex-members of staff. Eni’s current CEO, Claudio Descalzi, his predecessor, Paolo Scaroni, as well as three other current and former company executives were also cleared of wrongdoing.

Shell and Eni acquired Nigeria’s OPL 245 in 2011 for a total sum of $1.3 billion, of which around $200 million constituted a signature bonus paid directly to the government in Abuja. The rest of the money went to Malabu Oil and Gas, a company ultimately controlled by former Nigerian energy minister Dauzia ‘Dan’ Etete.

Prosecutors alleged that Etete fraudulently awarded the rights over OPL 245 to Malabu in 1998 and that he played a crucial role in the bribery scheme. He was charged along with former Russian diplomat Ednan Agaev and two Italian nationals said to have acted as intermediaries. According to a 13 January memorandum, Etete purportedly disbursed kickbacks to the companies’ executives and paid bribes to former public representatives, including Goodluck Jonathan, the country’s president at the time.

In 2018, two middlemen, Emeka Obi and Gianluca Di Nardo, were convicted and sentenced to four years in prison on corruption charges in Italy in relation to the same alleged conspiracy, after a fast-tracked trial. Their role is detailed in the Milan Tribunal’s memorandum against Shell and Eni.

Environmental advocacy group Global Witness stated that the acquittal “brings shame” to Italy and joined other anti-corruption and social justice organisations in calling on the prosecutors to appeal the decision. A spokesperson for the Nigerian government said that the administration was disappointed with the trial’s outcome, according to a Reuters article published on the same day. The court is due to publish its reasoning within 90 days.

Shell press release
Eni press release
Milan court ruling (Italian version...
Hungary and Poland file ECJ complaint over the EU rule of law mechanism

Hungary and Poland have filed a complaint before the Court of Justice of the European Union (CJEU/ECJ) on 11 March over the EU mechanism which ties the disbursement of EU funds to breaches of the principle of rule of law and covers both the 2021-2027 spending plan and the coronavirus stimulus fund.

The two countries allege that the newly established mechanism, which was introduced in December through EU Regulation 2020/2092, violates the principle of legal certainty and the principle of equal treatment of the EU member states. In addition, they claim that the EU lacks competence for defining the rule of law conditions.

The Polish government spokesperson Piotr Müller announced that compliance with the rule of law cannot represent a criterion for the payment of EU funds, which could only be subject to “the fulfillment of objective and specific conditions that arise clearly from legal provisions”. In addition, the Hungarian Minister of Justice Judit Varga stated that the EU Regulation “seriously infringes legal certainty”.

During the European Parliament’s (EP) 11 March plenary session, parliamentarians urged the European Commission (EC) to activate the rule of law mechanism without delay, alleging that the regulation which entered into force on 1 January is legally binding. In a resolution adopted on 25 March, the EP asked the EU executive to adopt guidelines on the application of the new rules by 1 June.

Brazil court annuls ex-president convictions

The Brazilian Supreme Federal Court decided on 8 March to overturn former president Luiz Inácio Lula da Silva's criminal convictions as part of the Operation Car Wash (Lava Jato) corruption probe, due to the Federal Court of Curitiba lacking jurisdiction in four actions, two of which are ongoing.

Supreme Court judge Edson Fachin ruled that the offences did not take place in the state of Paraná and the case must be retried in the capital city Brasilia. Fachin’s decision annuls the convictions on procedural grounds and orders the competent court to look again at the merits of the cases.

Lula was sentenced in 2017 to nine years and six months in prison for bribery and money laundering after an investigation found that he received approximately BRL 3.7 million (£459,000) worth of bribes from construction company OAS SA in the form of an apartment. In exchange, the former president allegedly helped OAS secure contracts with state-owned company Petróleo Brasileiro S.A. (Petrobras). After the sentence was increased by an appeals court to 12 years and one month, Lula was released in 2019 following a Supreme Court decision which stated that a person can be imprisoned only after the exhaustion of all remedies.

In 2019, Lula was sentenced in a separate lawsuit to nearly 13 years in prison after he was found guilty of receiving bribes from construction companies OAS SA and Odebrecht, in return for the awarding of lucrative public contracts with Petrobras.

On 23 October 2020, a case was filed against Lula before the 13th Federal Court of Curitiba by the Brazilian Federal Public Ministry (MPF) over money laundering allegations involving the same two companies. According to the MPF, Lula accepted nearly BRL 4 million (£498,000) worth of bribes through four donations to the benefit of the Lula Institute.
PRESS AND MEDIA

Former French president Nicolas Sarkozy sentenced to prison for corruption

Former French president Nicolas Sarkozy was sentenced on 1 March to three years in prison with a two-year suspended sentence for attempting to bribe former judge Gilbert Azibert to obtain inside information on an inquiry into the financing of his 2007 presidential campaign, according to a France24 article published on the same day. Sarkozy’s attorney Thierry Herzog and Azibert, who were also on trial, received the same sentence.

According to the Paris Correctional Tribunal’s findings, Sarkozy offered a senior position in Monaco’s State Council to Azibert, with Herzog acting as an intermediary, in exchange for confidential information on an inquiry targeting illicit payments made by L’Oreal heiress Liliane Bettencourt to Sarkozy’s close associates in the French government. In March 2013, Sarkozy was indicted for allegedly taking advantage of Bettencourt’s mental state to obtain the funds, but was cleared of the charges.

Sarkozy’s lawyer, Jacqueline Laffont, reportedly described the sentence as “extremely severe” and “totally unfounded and unjustified”, announcing that she would file an appeal. During a 3 March interview with TF1, Sarkozy alleged that there were multiple irregularities with the investigation by the office of the National Financial Prosecution and its seniority.

In January, the Guardian reported that the former president was involved in a preliminary investigation over influence peddling allegations related to a €3 million contract with a Russian insurance company, the Reso-Garantia Group. In February 2020, Thierry Gaubert, a former aide to Sarkozy, was charged over allegedly receiving €440,000 in a secret offshore bank account from Muammar Gaddafi’s government in 2006 to fund Sarkozy’s presidential campaign.

Sarkozy was scheduled to appear in court on 17 March in another case, the so-called Bygmalion affair, related to bypassing the legal threshold for financing his 2012 election campaign by using a system of false invoices.

French government. In March 2013, Sarkozy was indicted for allegedly taking advantage of Bettencourt's mental state to obtain the funds, but was cleared of the charges.

Sarkozy’s lawyer, Jacqueline Laffont, reportedly described the sentence as “extremely severe” and “totally unfounded and unjustified”, announcing that she would file an appeal. During a 3 March interview with TF1, Sarkozy alleged that there were multiple irregularities with the investigation by the office of the National Financial Prosecution and its seniority.

In January, the Guardian reported that the former president was involved in a preliminary investigation over influence peddling allegations related to a €3 million contract with a Russian insurance company, the Reso-Garantia Group. In February 2020, Thierry Gaubert, a former aide to Sarkozy, was charged over allegedly receiving €440,000 in a secret offshore bank account from Muammar Gaddafi’s government in 2006 to fund Sarkozy’s presidential campaign.

Sarkozy was scheduled to appear in court on 17 March in another case, the so-called Bygmalion affair, related to bypassing the legal threshold for financing his 2012 election campaign by using a system of false invoices.

Former French president Nicolas Sarkozy was sentenced on 1 March to three years in prison with a two-year suspended sentence for attempting to bribe former judge Gilbert Azibert to obtain inside information on an inquiry into the financing of his 2007 presidential campaign, according to a France24 article published on the same day. Sarkozy’s attorney Thierry Herzog and Azibert, who were also on trial, received the same sentence.

According to the Paris Correctional Tribunal’s findings, Sarkozy offered a senior position in Monaco’s State Council to Azibert, with Herzog acting as an intermediary, in exchange for confidential information on an inquiry targeting illicit payments made by L’Oreal heiress Liliane Bettencourt to Sarkozy’s close associates in the French government. In March 2013, Sarkozy was indicted for allegedly taking advantage of Bettencourt’s mental state to obtain the funds, but was cleared of the charges.

Sarkozy’s lawyer, Jacqueline Laffont, reportedly described the sentence as “extremely severe” and “totally unfounded and unjustified”, announcing that she would file an appeal. During a 3 March interview with TF1, Sarkozy alleged that there were multiple irregularities with the investigation by the office of the National Financial Prosecution and its seniority.

In January, the Guardian reported that the former president was involved in a preliminary investigation over influence peddling allegations related to a €3 million contract with a Russian insurance company, the Reso-Garantia Group. In February 2020, Thierry Gaubert, a former aide to Sarkozy, was charged over allegedly receiving €440,000 in a secret offshore bank account from Muammar Gaddafi’s government in 2006 to fund Sarkozy’s presidential campaign.

Sarkozy was scheduled to appear in court on 17 March in another case, the so-called Bygmalion affair, related to bypassing the legal threshold for financing his 2012 election campaign by using a system of false invoices.

German prosecutors indict three former Steinhoff executives over balance sheet fraud

Reuters reported on 4 March that German prosecutors have indicted three former executives of Frankfurt-listed South African retailer Steinhoff NV for balance sheet fraud following criminal investigations into accounting irregularities between 2009 and 2017.

According to local media, criminal investigations were initiated by the Oldenburg Public Prosecutor’s Office after PricewaterhouseCoopers (PwC) uncovered financial irregularities in the company’s accounts in 2019, involving more than €6.5 billion in fictitious or irregular transactions between its 2009 and 2017 financial years.

Charges have now been filed against three unnamed Steinhoff former executives for balance sheet manipulation, accusing them of inflating company accounts with more than €1.5 billion in fictitious transactions as well as real estate over valuation of €820 million.

German prosecutors indicted three former Steinhoff executives for balance sheet fraud as part of a criminal investigation into accounting irregularities between 2009 and 2017. The investigation, initiated by the Oldenburg Public Prosecutor’s Office after PricewaterhouseCoopers (PwC) uncovered financial irregularities in the company’s accounts in 2019, involved more than €6.5 billion in fictitious or irregular transactions between its 2009 and 2017 financial years.

Charges have now been filed against three unnamed Steinhoff former executives for balance sheet manipulation, accusing them of inflating company accounts with more than €1.5 billion in fictitious transactions as well as real estate overvaluation of €820 million.

German prosecutors indicted three former Steinhoff executives for balance sheet fraud as part of a criminal investigation into accounting irregularities between 2009 and 2017. The investigation, initiated by the Oldenburg Public Prosecutor’s Office after PricewaterhouseCoopers (PwC) uncovered financial irregularities in the company’s accounts in 2019, involved more than €6.5 billion in fictitious or irregular transactions between its 2009 and 2017 financial years.

Charges have now been filed against three unnamed Steinhoff former executives for balance sheet manipulation, accusing them of inflating company accounts with more than €1.5 billion in fictitious transactions as well as real estate overvaluation of €820 million.

German prosecutors indicted three former Steinhoff executives for balance sheet fraud as part of a criminal investigation into accounting irregularities between 2009 and 2017. The investigation, initiated by the Oldenburg Public Prosecutor’s Office after PricewaterhouseCoopers (PwC) uncovered financial irregularities in the company’s accounts in 2019, involved more than €6.5 billion in fictitious or irregular transactions between its 2009 and 2017 financial years.

Charges have now been filed against three unnamed Steinhoff former executives for balance sheet manipulation, accusing them of inflating company accounts with more than €1.5 billion in fictitious transactions as well as real estate overvaluation of €820 million.

German prosecutors indicted three former Steinhoff executives for balance sheet fraud as part of a criminal investigation into accounting irregularities between 2009 and 2017. The investigation, initiated by the Oldenburg Public Prosecutor’s Office after PricewaterhouseCoopers (PwC) uncovered financial irregularities in the company’s accounts in 2019, involved more than €6.5 billion in fictitious or irregular transactions between its 2009 and 2017 financial years.

Charges have now been filed against three unnamed Steinhoff former executives for balance sheet manipulation, accusing them of inflating company accounts with more than €1.5 billion in fictitious transactions as well as real estate overvaluation of €820 million.
Scottish companies reportedly probed over role in Libya fraud and money laundering scheme

**Dozens of Scottish companies and more than 90 bank accounts are reportedly being investigated by Police Scotland as part of an ongoing investigation into a £5 billion Libyan fraud and money laundering scandal, linked to former Libyan official Ali Ibrahim Dabaiba, also a member of Muammar Gaddafi’s inner circle, according to a 14 March article published by the Sunday Times.**

Details of the Police Scotland’s Operation Adelanter were reportedly shared with Libyan prosecutors in October 2018. According to the investigation, Dabaiba headed Libya’s Organisation for Development of Administrative Centres (ODAC) until 2011, a body tasked with developing the country’s infrastructure. In this capacity, he reportedly awarded a £150 million contract for renovating cultural heritage sites to Edinburgh-registered company Marco Polo Storica Limited, which was dissolved in 2015.

In 2013, the post-Gaddafi administration alleged that Dabaiba was responsible for misappropriating between $6 and $7 billion from the ODAC’s budget through fraudulent public tenders and subsequently laundered the proceeds of embezzlement through shell companies around the world, with the leaked documents claiming that at least £50 million of the illicit funds is believed to have passed through Marco Polo Storica.

The Scottish Crown Office agreed in 2014 to help the Libyan authorities investigate the allegations of money laundering. In addition, the investigation reportedly uncovered in 2017 that Dabaiba owned numerous properties in the UK, according to a 2016 article published by the Guardian.

---

**NCA amber alert reportedly warns London galleries of money laundering risks**

**The UK’s National Crime Agency (NCA) has issued an amber alert to London’s art galleries, underlining that they must respond to the increased risk of money laundering (ML) within the sector, according to a 19 March article by the Evening Standard.**

The alert was reportedly issued following a request by the NCA that art galleries file more suspicious activity reports (SARs). The Director General of the NCA’s National Economic Crime Centre (NECC), Graeme Biggar, told the media outlet that the response from art dealers so far was “inadequate” and did not generate a significant increase in the number of SARs filed.

The UK’s £9 billion art market is one in which parties often operate with anonymity, use nominees, or do not reveal the source of funds, Biggar underlined. These circumstances can allow money launderers to move large amounts of wealth without raising suspicion, the NECC Director said.

The alert reportedly cites the example of London art dealer Matthew Green, indicted by the US DOJ in February 2018, on charges of money laundering. Green extended an offer to an undercover agent to launder the proceeds of a securities fraud through the sale of a Picasso painting for £6.7 million, according to prosecutors. The case is ongoing.

---

*Times article*

*Times article (18 October...)*

*OCCRP article (25 July 20...)*

*Evening Standard article*

*DOJ press release (2 Marc...)*

*Superseding indictment in...*
Former chief of staff to ex-Maltese PM Muscat charged with corruption

The Guardian reported on 20 March that Keith Schembri, former chief of staff to ex-Maltese prime minister Joseph Muscat has been charged with corruption, fraud and money laundering together with 10 other individuals, in relation to dealings with former managing director of Allied Group Adrian Hillman.

According to Malta Today, Schembri allegedly paid bribes worth €650,000 to Hillman between 2011 and 2015 through foreign bank accounts, with the aim of securing contracts for his company Kasco Trading Ltd to supply Allied Newspapers Ltd with machinery for a new printing press. Schembri’s company allegedly won the contract for the construction of Allied’s €30 million printing press. The media outlet reported that a second inquiry concerns suspected kickbacks from the sale of Maltese passports, involving Schembri and his financial advisors Nexia BT Advisory Services Ltd.

Schembri was initially accused of corruption and money laundering in 2016 by journalist Daphne Caruana Galizia. The Daphne Caruana Galizia Foundation, an NGO which was established in 2019 following the journalist’s assassination, wrote on 20 March that “Schembri’s arraignment on these charges is overdue”.

On 25 March, the Times of Malta reported the launch of court proceedings with regard to allegations of forgery, fake accounting and tax evasion involving Nexia BT Advisory Services Ltd and financial services company Zenith Finance Ltd, previously known as MFSP Financial Management Ltd. Investigators allegedly stated in court that €650,000 was paid by Schembri to Hillman through MFSP, after funds were passed into the company through accounts at Credit Suisse Group AG and Jyske Bank (Gibraltar) Ltd.

Zenith Financial Services executives Matthew Pace and Lorraine Falzon are also charged with money laundering and corruption in the case. Malta’s Financial Services Authority announced on 26 March that it has suspended the company’s operations and has ordered it “to refrain from onboarding of new clients and refrain from providing existing clients with any new or additional services”.

Whistleblower claims Credit Suisse continued to aid tax evasion after plea agreement

A former employee of Swiss bank Credit Suisse claims that the bank continued to assist wealthy Americans evade taxes, despite its plea agreement with the US authorities in May 2014 in which the bank admitted to helping US taxpayers hide offshore accounts, according to reporting by the New York Times on 13 March.

Credit Suisse’s settlement with the US Justice Department in May 2014 included a $2.6 billion payment and the bank’s commitment to shut down all the accounts of recalcitrant account holders as well as assist in criminal investigations being carried out by the US authorities.

According to documents sent to the US Justice Department and the Internal Revenue Service seen by the New York Times, the former senior Credit Suisse employee claims that the bank continued to hide assets for US clients following its plea agreement and despite its commitments to close US client accounts.
Mexico scrutinising deals with Vitol after US DPA with the DOJ over bribery allegations

Reuters reported on 22 March that Mexico is re-examining and attempting to renegotiate state contracts with Vitol SA following the company’s December 2020 acknowledgement that it paid bribes to officials at Mexican state-owned Petróleos Mexicanos (Pemex) to secure business dealings. The US Department of Justice (DOJ) reached a settlement agreement with Vitol Inc, the Houston-based US subsidiary of the Dutch Vitol Holding BV, on 3 December 2020, over alleged violations of the Foreign Corrupt Practices Act (FCPA), the bulk of which involved Brazil in addition to Mexico and Ecuador, in which Vitol agreed to pay $164 million to the US and Brazil.

Mexico has reportedly launched its own criminal proceedings into Vitol’s alleged bribery involving Pemex, according to a 3 March announcement by President Manual Lopez Obrador. Furthermore, Pemex CEO Octavio Romero Oropeza reportedly told Reuters on 18 March that the state energy company is examining all its contracts with Vitol to identify possible signs of corruption or other irregularities and is seeking to eliminate any unfavourable provisions. Total Pemex and Vitol contracts are worth approximately $1 billion, according to an anonymous source cited by the news outlet. One contract for ethane gas worth $230 million was reportedly signed by a former Vitol trader who is named in the DOJ’s deferred prosecution agreement as a primary agent in allegedly making bribe payments to officials in Ecuador.

The December 2020 DOJ complaint alleges that Vitol conspired to pay over $2 million in bribes to Mexican officials to improperly secure oil contracts between 2015 and 2020. Furthermore, the DOJ alleges that Vitol and co-conspirators set up shell companies and fake invoices and email accounts with pseudonyms to transfer the corrupt payments into shell companies offshore, using several US bank accounts in the process.

Following the deferred prosecution agreement, Vitol SA released a 3 December statement in which CEO Russell Hardy asserted that the company is enhancing its controls and procedures in line with best practices.

UBS Group AG allegedly facing at least €3 billion in penalties in French tax fraud case

Bloomberg reported on 23 March that UBS Group AG is allegedly facing at least €3 billion in penalties once the Paris Court of Appeal has reached a verdict in the company’s appeal of a 2019 ruling requiring it to pay a €3.7 billion fine and €800 million in civil damages in a money laundering and tax fraud case.

According to the media outlet, during closing arguments in the case on 22 March, French prosecutors requested the Paris Court of Appeal impose a €2 billion fine on UBS, while the French state, which is a plaintiff in the case, is claiming €1 billion in damages from the Swiss bank, in addition to any penalties that the court will impose.

UBS Group AG and UBS (France) SA were found guilty in 2019 by the High Court of Paris of illegally helping French clients conceal billions of euros from the French tax authorities and laundering the proceeds of tax evasion between 2004 and 2012, following a seven-year investigation. The bank appealed the decision, alleging that the case is based on unfounded allegations by former employees, with no specific evidence of wrongdoing.

A verdict on the case brought before the Paris Court of Appeals is expected in several months.
Forced labour in the supply chain

On 17 March 2021, the UK's Department for Business, Energy and Industrial Strategy (BEIS) published a report that concluded that companies are failing to undertake necessary due diligence to establish whether their supply chains are implicated in forced labour or the abuse of minorities in China and the country's Xinjiang Uyghur Autonomous Region (XUAR).

Extensive evidence of forced labour programmes targeting the Uyghur and other ethnic minorities in China mean that companies in the textile, technology and renewables industries face significant legal, reputational and economic risks with regard to their suppliers. Businesses that are either part of a value chain that stretches to XUAR or engage with local authorities in the fields of surveillance, biometrics, or tracking technology, are also at risk of unintentionally facilitating human rights violations.

The need for supply chain due diligence

Since July 2020, the international community has taken a number of steps in response to human rights violations against the Uyghur minority in XUAR that will require companies to fully understand the risks of working with entities in the region.

Sanctions

- On 22 March 2021, the UK imposed sanctions on four Chinese officials and the Public Security Bureau of Xinjiang Production and Construction Corps (XPCC), a Chinese paramilitary and economic organisation in XUAR, for human rights abuses. The UK will impose asset freezes and travel bans against the four officials and the XPCC's Public Security Bureau.

- In a coordinated move, the EU, US and Canada also announced sanctions against the above subjects.

- On 31 July 2020, the US Treasury's Office of Foreign Assets Control (OFAC) imposed economic sanctions on the XPCC.

Withhold Release Orders (WRO) in the US

- In September 2020, US Customs and Border Protection issued five WROs on items originating from XUAR, including hair, clothing and technology products.
The US issued a further WRO in November 2020 against all cotton products made by XPCC and in January 2021 against cotton products and tomato products produced in XUAR. Under the WROs, US Customs and Border Protection is instructed to detain shipments of the relevant items and, to obtain their release, an importer must present proof that no forced labour was used for manufacture throughout the supply chain of the finished goods.

Supply chain legislation

- On 18 February 2021, the US House of Representatives re-introduced an updated bipartisan bill known as the Uyghur Forced Labor Prevention Act. The original bill was passed by the House and referred to the Senate Foreign Relations Committee in 2020. The bill, which is likely to be signed into law, would prohibit all imports to the US of goods made in XUAR unless it can be demonstrated with “clear and convincing” evidence that the goods were produced without the use of forced labour.
- On 10 March 2021, the European Parliament voted to adopt binding EU laws that will require companies to identify, address and remedy their impact on human rights throughout their supply chains.

How companies can protect themselves against human rights risks in Xinjiang

Conducting effective human rights due diligence in XUAR is inhibited by a number of factors, including poor access, a lack of freedom of speech for workers, and the extent and severity of human rights violations on the ground. However, it remains incumbent on businesses to demonstrate that they have performed adequate due diligence and have the necessary human rights policies and practices to ensure their operations do not directly or indirectly contribute to human rights violations. Unfortunately, cutting direct ties with factories or suppliers based in XUAR is insufficient since these entities themselves frequently source products or workers from within XUAR. Companies should trace their supply chains to origin and, to the extent possible, identify any associations between their sub-suppliers and forced labour in XUAR.

Aperio Intelligence’s established due diligence team can support businesses to:

- Identify a Chinese counterparty’s ownership structure and links to the XPCC which may expose it to forced labour practices.
- Establish whether a Chinese counterparty receives government incentives or subsidies that may be connected to internment camps, referred to by the Chinese authorities as vocational training centres, in XUAR.
- Investigate whether a counterparty has any known links – either directly or through its own suppliers – to the mass detention of Uyghurs in XUAR.
- Identify where an entity of interest constitutes a shell company which is used to hide the provenance of certain goods or particular financial transactions.

From a broader risk management perspective, Aperio can assist businesses to implement effective ESG programmes:

- Strong leadership to develop effective governance and oversight of supply chain and human rights issues.
- Practical implementation and monitoring of corporate policies and procedures that support decision-making practices and help prevent human rights abuses.
- Stakeholder engagement and greater visibility of actors along the value chain.
- Continuous monitoring and improvement of business processes aimed at mitigating human rights risks.

If you would like more information on how Aperio Intelligence can assist you to conduct human rights due diligence please get in touch with Vivien Li - Head of APAC vivien.li@aperio-intelligence.com or Simon Jennings - Head of ESG simon.jennings@aperio-intelligence.com