SLAUGHTER AND MAY/

GLOBAL INVESTIGATIONS BULLETIN

April 2022

RECENT PUBLICATIONS //

Evolution not revolution: The Economic Crime (Transparency and Enforcement) Act 2022 (22 March), by Jonathan Cotton, Jane Edwarde, Andrew Jolly, Anna Lambourn, Mark Gulliford, and Harriet Redwood.

UK FINANCIAL SANCTIONS ENFORCEMENT //

The Office of Financial Sanctions Implementation (OFSI), established in 2016, is the agency with primary responsibility for investigating and enforcing breaches of financial sanctions in the United Kingdom. In light of Russia's invasion of Ukraine and the resulting sanctions enacted against Russia, and the upcoming change in law to make civil sanctions breaches a strict liability offence, enforcement will undoubtedly be a key governmental priority. This month's Bulletin examines OFSI's past enforcement actions and discusses the road ahead for enforcement. *Last month's Bulletin reviewed the Russian sanctions framework; read it here for background.*

Penalties available

OFSI has the power to enforce breaches of sanctions on a civil basis, and may work with prosecutors (including the Serious Fraud Office, HM Revenue and Customs, and the Crown Prosecution Service) to bring a criminal action. A civil penalty may be imposed if OFSI is satisfied that, on the balance of probabilities, sanctions were breached, and the person / entity did not know or have reasonable cause to suspect that their activity was in breach of such laws. Once Chapter 1 of the Economic Crime (Transparency and Enforcement) Act 2022 comes into force, that knowledge defence is removed and the offence becomes one of strict liability. A prosecution may instead be brought if it passes the evidential and public interest tests within the code for crown prosecutions: that there is sufficient evidence to provide a realistic prospect of conviction, and the prosecution is in the public interest.

The Policing and Crime Act 2017 sets out the available civil penalties that OFSI may impose, which include a fine of up to £1 million, or 50% of the value of the breach, whichever is higher. Criminal penalties are set out in the statutory instruments implementing the various sanctions, but usually include the imposition of an unlimited fine, plus up to seven years' imprisonment for individuals. OFSI has issued guidance on the issuance of monetary penalties (updated in January 2022), which provides information on OFSI's enforcement process, the procedure for issuing penalties, and the right to appeal any decision made.

OFSI's enforcement actions

OFSI has brought six civil enforcement actions with fines ranging from £5,000 to £20.47 million. Five actions were brought against banking or financial services providers, and one was brought against a telecommunications company.

Company	Date of enforcement notice	Self-report?	Penalty
Raphael & Sons plc	21 January 2019	Yes	£5,000
Travelex UK Ltd	8 March 2019	No	£10,000
Telia Carrier UK Ltd	9 September 2019	No	£146,341
Standard Chartered Bank	18 February 2020	Yes	£20.47 million
Clear Junction Ltd	2 February 2021	Yes	£36,393.45
TransferGo Ltd	25 June 2021	No	£50,000

Given the low number of actions it is difficult to discern any trends or themes, but some key points can be drawn out.

The first two actions, brought against Raphael & Sons plc and Travelex UK Ltd, were brought for dealing with the funds of a designated person, and the amounts were low: £200 and £204 at each institution. There was only the single instance of "dealing" at each institution; this did not appear to be a repeat or systemic issue. The fine against Raphael & Sons qualified for a 50% discount on the basis that they had self-reported, whereas Travelex did not self-report and was issued the full penalty of £10,000. In neither notice does OFSI comment on how it arrived at the penalty amount. The cases are notable because they show that OFSI has brought enforcement action in respect of a single breach.

The action brought against Telia, a telecommunications provider, was brought in respect of making economic resources available to a designated person or entity. In this case, Telia indirectly facilitated international calls to SyriaTel, which was designated. OFSI originally calculated the value of economic resources provided as amounting to £234,000. This was the first action brought that resulted in an appeal to a Minister under section 147 of the Policing and Crime Act 2017. The Minister reduced the fine imposed by OFSI on the basis of new evidence introduced during the appeal process. The notice stated that such an introduction would not normally occur during the Ministerial review, but OFSI permitted it on the basis that the new evidence would have a "likely significant impact".

The action taken against Standard Chartered Bank (SCB) was OFSI's first big-ticket matter, with a penalty of £20.47 million issued. This action was taken in respect of a large number of loans made to Denizbank AS, a nearly-wholly owned subsidiary of Sberbank (which was designated under the 2014 Crimea sanctions). When Sberbank was first designated, SCB originally cut ties with Denizbank, but later introduced dispensations that permitted loans to be made where it thought an exemption applied. The dispensations were not adequately applied, resulting in loans being made that should not have been. OFSI classified this as a "most serious" breach of controls given the repeated failings. Thus, even though SCB qualified for a penalty reduction for self-reporting, this only amounted to a 30% reduction rather than a 50% reduction. SCB also exercised its right to Ministerial review and the penalty was further reduced from the original amount proposed (£31.5 million).

In the final two enforcement actions, which resulted from connected transactions, TransferGo and Clear Junction requested a Ministerial review. Unlike in the previous cases, where such a review resulted in a reduction in the penalty, no such reduction was applied here. In addition, both companies had requested anonymity in the enforcement notice, but this was denied. This is unsurprising, given that OFSI's guidance states that it "will normally publish details of all monetary penalties it imposes… [which] helps increase awareness to deter future non-compliance, and promote good practice".

Final thoughts

The challenge facing OFSI now is one of having enough resources to enforce the additional sanctions measures that have been adopted, which, by any estimation, is going to be an enormous burden. In HM Treasury's Outcome Delivery Plan for 2021-2022, it was reported that OFSI had the equivalent of less than 40 full time employees, whose jobs also include issuing licences and publishing guidance and interpretation. A recent House of Commons Treasury Committee report urged the government to consider increasing OFSI's resources — a "surge capacity" — in the form of additional staff with appropriate expertise. Legislation is only as strong as the enforcement capability, and it appears that the need for additional resource is at least acknowledged.

RECENT NEWS //

Economic Crime (Enforcement and Transparency) Act enacted

Following its two-week sprint through parliament, the Economic Crime (Transparency and Enforcement) Act 2022 was passed on 15 March. The Act introduces a new register of overseas entities, amends the Unexplained Wealth Order regime, and updates the sanctions designation and enforcement framework. Most notably for corporates, the Act will permit the enforcement of civil sanctions breaches on a strict liability basis, removing the existing defence of having no knowledge or awareness that their actions would breach sanctions (that defence will remain for criminal prosecution). The Act and its implications are summarised in this briefing, published 22 March.

Sanctions & OFSI update: updated Russian sanctions guidance published; US DOJ reveals first prosecutions for breaches of 2014 Russian sanctions

On 31 March, the Office of Financial Sanctions Implementation (OFSI) published updated Guidance to Russian financial and investment sanctions. Further details on the designation of additional Russian and Belarusian individuals and entities are available on the government website here.

On 3 March, the US Department of Justice (DOJ) revealed an indictment charging 71-year-old US citizen John Hanick with violating Russian sanctions and making false statements. Hanick allegedly helped Russian oligarch Konstantin Malofeyev set up a Russian news television network, in violation of the US's sanctions imposed against Russia in 2014 for its annexation of Crimea. Malofeyev has also been charged for breaches of sanctions, becoming the first Russian oligarch to be criminally charged since the Russian invasion of Ukraine. These are the first two US prosecutions for breaches of the 2014 Russian sanctions legislation. Malofeyev was designated in 2014 for his role in financing a Russia-aligned separatist group in Ukraine. It is expected that the Office of Foreign Assets Control (OFAC) and the Bureau of Industry and Security may use their civil enforcement powers to pursue administrative cases concurrently with DOJ criminal investigations. The charges came one day before the US government announced a new "KleptoCapture" taskforce dedicated to targeting the crimes of Russian officials and elites who violate sanctions and other economic countermeasures the US has imposed on the country. UK authorities arrested Hanick at the request of the US on 3 February in London with a view towards extradition.

SFO update: reported investigation into insurance firms over South America bribery allegations; SFO director evades questions on Unaoil investigation

On 30 March, the US Department of Justice (DOJ) publicised its decision not to prosecute UK-based insurer Jardine Lloyd Thompson Group plc (JLT), and hinted at a future bribery resolution with the Serious Fraud Office (SFO) (the SFO has not yet publically announced such an investigation). The DOJ "reached this conclusion despite the bribery committed by an employee and agents of the Company and its subsidiaries" between 2014 and 2016. According to the DOJ, employees and agents of JLT paid

some “$10,800,000 to a Florida-based third-party intermediary that the employee and agents knew would be used, in part, to pay approximately $3,157,000 in bribes to Ecuadorian government officials”. The aim of the bribery was to “obtain and retain contracts with Seguros Sucre, the Ecuadorian state-owned and -controlled surety company”. Around $1.2 million of these bribe payments were laundered through, and into, bank accounts in the US. Despite its findings, the DOJ declined prosecuting JLT based on: (i) JLT's voluntary self-disclosure of the conduct; (ii) its full and proactive cooperation in the matter, including providing all known relevant facts and continuing cooperation in the DOJ ongoing investigations and any prosecutions that might result; (iii) the nature and seriousness of the offence; (iv) JLT's timely and full remediation, including separation from the executive and third-party intermediary company involved in the misconduct and the efforts to enhance its anti-corruption training and compliance program; and (v) JLT's agreement to disgorge the full amount of its unscrupulous gains. The DOJ told JLT it would credit the funds against the company's separate resolution with the UK SFO as long as it covers the same underlying conduct and any fine is paid within the next 12 months.

Director Lisa Osofsky has declined to answer questions from the Justice Committee about the quashing of a second former oil executive's bribery conviction, saying she does not want to “impinge on” a judge-led review of SFO's disclosure failures. Osofsky said she is “not in a position to answer anything” about the recent decision to overturn the conviction of Paul Bond, who was jailed for conspiracy to give corrupt payments following the SFO's investigation into bribery involving the Unaoil energy consultancy. The Court of Appeal criticised the SFO's failure to disclose information about “wholly inappropriate” contacts between former US Drug Enforcement Administration agent David Tinsley — who was acting on behalf of the family which owned and controlled Unaoil — and senior officials at the SFO, including Osofsky. The quashing of former Unaoil executive Ziad Akle's conviction for bribery in December prompted Attorney General Suella Braverman to announce an independent review led by former High Court judge and former director of public prosecutions Sir David Calvert-Smith.

FCA update: FCA publishes statement on compliance with Russian sanctions; former Redcentric CFO receives sentence; FCA, Bank of England and OFSI publish joint statement on sanctions and cryptoasset sector

The Financial Conduct Authority (FCA) published a statement on the UK’s tranche of sanctions on Russia, noting that it expects firms to have established systems and controls to comply with sanctions obligations. The FCA’s expectations of firms’ systems and controls in relation to compliance with financial sanctions are set out in FCG 7 of the FCA’s Financial Crime Guide, which includes examples of good and poor practice in relation to firms’ governance, risk assessments and approaches to screening in relation to financial sanctions. Where transactions give rise to concerns about sanctions evasion or money laundering, firms should also consider obligations to report to the UK Financial Intelligence Unit (UKFIU) at the National Crime Agency (NCA) under the Proceeds of Crime Act 2002. Firms undertaking trade finance activities should consult the FCA's "Dear CEO" letter of September 2021 for additional guidance on sanctions considerations.

Tim Coleman, former Chief Financial Officer of Redcentric Plc, was sentenced to five and a half years’ imprisonment and disqualified from being a director for 10 years. He was found guilty of two offences of making false and misleading statements to the markets contrary to section 89(1) of the Financial Services Act 2012, and three offences of false accounting contrary to section 17(1)(a) of the Theft Act 1968. Redcentric is an IT service provider and AIM-listed company. Mr Coleman was found to have inflated the company's cash position to the Redcentric Board, and used the same false figures to assure key investors about Redcentric's financial position, persuading them not to sell their investments. Redcentric issued false and misleading unaudited interim results in November 2015 and false and misleading audited final year results in June 2016, which materially overstated Redcentric's cash

position (by £13.1 million and £12.2 million respectively) and misstated its net debt position. Redcentric's share price had been artificially inflated, so when the true position was revealed shareholders suffered immediate share value losses. Mark Steward, the FCA's Executive Director of Enforcement and Market Oversight, said that the sentence "reflects the seriousness of the crimes and should serve as a deterrent to anyone considering committing similar offences". The FCA will now pursue confiscation proceedings against Mr Coleman. Mr Coleman's sentence follows that of Estelle Croft, a former finance director at Redcentric, who was sentenced to three years' imprisonment having pleaded guilty to charges of making false statements and false accounting. Ms Croft was ordered to pay £120,346.70 following confiscation proceedings. Read the FCA press release here.

The FCA, the Bank of England, and OFSI published a joint statement on sanctions and the cryptoasset sector following the Russian invasion of Ukraine. In the statement, the regulators reminded firms that the use of cryptoassets to circumvent economic sanctions is a criminal offence under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692) and regulations made under the Sanctions and Anti-Money Laundering Act 2018. The FCA has already written to all registered cryptoasset firms and those holding temporary registration status to highlight the application of sanctions on various entities and individuals. The FCA reminded all authorised financial institutions to check the FCA register to identify whether any cryptoasset firms they do business with are registered, or to check the equivalent register of the jurisdiction in which the cryptoasset firm is based. The joint statement confirmed that the FCA and the Prudential Regulation Authority will act if they see authorised financial institutions supporting cryptoasset firms operating in the UK illegally. The joint statement also set out suggested steps that firms could take to reduce the risk of sanctions evasion via cryptoassets, including ensuring that customers and their transactions are screened against relevant updated sanctions lists and, where blockchain analytics solutions are deployed, ensuring that compliance teams understand how these capabilities can be best used to identify transactions linked to higher risk wallet addresses.

MLA guidelines for foreign authorities replaced with 2022 version

On 29 March 2022, the Home Office announced it had replaced its guidance on "Requests for MLA in criminal matters: guidelines for foreign authorities" with a 2022 version entitled "Request for Mutual Legal Assistance in criminal matters: guidelines for authorities outside of the United Kingdom". It has also removed Polish and Turkish translations as they are now out of date and new translations are being developed.

Meta fined €17 million by Irish regulator

Ireland's data protection regulator announced that it had fined Meta €17 million for failing to adequately protect users' personal data. The Data Protection Commission issued the penalty after it received 12 data breach notifications between 7 June and 4 December 2018. The Data Protection Commission found that Meta breached the GDPR's accountability rules by being unable to demonstrate which security measures it had in place to protect users. The regulator was the lead enforcer in a GDPR article 60 cross-border investigation, with the Irish commission leading as regulator for Meta's European headquarters in Ireland. Two other member state supervisory authorities objected to the draft decision, but the Irish regulator said that "consensus was achieved through further engagement between the DPC and the supervisory authorities concerned".

INTERPOL launches Financial Crime and Anti-Corruption Centre

The International Criminal Police Organisation (INTERPOL) announced the launch of its financial crime and corruption initiative on 15 March. The Financial Crime and Anti-Corruption Centre aims to

centralise INTERPOL's existing financial crime expertise and analysis, and help law enforcement agencies in its 195 member countries to coordinate cross-border actions and share information more readily. The centre will work closely with established international organisations in this area, including the Financial Action Task Force and the Egmont Group. INTERPOL's announcement follows a call in November from the Organisation for Economic Co-operation and Development, for countries to conduct more joint investigations and share evidence more efficiently in corruption probes. In its statement from 10 March on the "conflict in Ukraine" — in which it stated that "Neutrality is fundamental to INTERPOL's work and existence" — the agency noted that so far in 2022, nearly 60,000 checks had been made by member countries against data supplied in Russia. Practitioners have commented that INTERPOL's efforts could come at an awkward time as North American and European countries have pledged to create a transatlantic taskforce to open investigations into Russia-linked sanctions evasion and money laundering cases following its invasion of Ukraine. INTERPOL has recently come under scrutiny for its November decision to elect as its president Ahmed Nasser Al Raisi, a high-ranking military official from the UAE who has faced (and denied) allegations of complicity in torture from human rights groups.

Dutch prosecutor Daniëlle Goudriaan to succeed Drago Kos as OECD chair

The Organisation for Economic Co-operation and Development (OECD) working group on bribery elected Dutch prosecutor Daniëlle Goudriaan as its new chair as of 1 January 2023. Goudriaan is the Netherlands' representative to the college of prosecutors at the European Public Prosecutor's Office, helping to set strategies and ensure consistency between cases under chief prosecutor Laura Kövesi's leadership. Goudriaan was formerly the national coordinating prosecutor for corruption within a division of the public prosecution service specialising in complex fraud, and previously part of the Dutch delegation in the OECD's working group, a member of its management group, and chair of its regular meetings with global enforcement officials.

Rio Tinto fined in Australia

The Australian Securities and Investment Commission (ASIC) fined Anglo-Australian mining company Rio Tinto A$750,000 for failing to disclose material information about the value of a Mozambique mining project. ASIC said on 7 March that the fine resolves a case against Rio Tinto over the company's failure to record in its 2012 interim accounts that mining assets held by a Mozambique subsidiary were no longer economically viable. The agency added that its case against two former Rio Tinto senior executives, Tom Albanese and Guy Elliott, has been dismissed. ASIC had charged the company, Albanese, and Elliott in 2018 with making allegedly deceptive statements about the value of the Mozambique coal reserves prior to taking a multi-billion write-down on the asset. Rio Tinto purchased the Mozambique coal reserves for US $3.7 billion in April 2011, only to sell it for US $50 million in July 2014. Rio Tinto has also been under investigation by the Serious Fraud Office since July 2017, in relation to the conduct of business in the Republic of Guinea

SEC floats mandatory disclosures on emissions and climate change risks

On 21 March, the US Security and Exchange Commission (SEC) gave its initial approval to a new requirement for public companies to disclose their emissions and the risks that climate change poses for their business. SEC Chairman Gary Gensler said the aim of the proposal was to create a standardised process for companies to report their role in climate change. This would provide more clarity to businesses on their disclosure obligations and greater transparency for the growing number of investors who look at a company's sustainability record when deciding to invest. Shareholder pressure has already led many companies to make their emissions numbers public. The SEC opened up the

proposal to public comment; at the end of the 60-day period, the regulator will consider the feedback and vote on a final ruling within the following months. Read more in the SEC announcement.

Fraud Act 2006 - House of Lords publishes call for evidence

The House of Lords Committee on the Fraud Act 2006 and Digital Fraud (the Committee) published a call for evidence, inviting views on what measures should be taken to tackle the increase in fraud cases. The Committee notes that fraud is the most commonly experienced crime in England and Wales, accounting for approximately 42% of all crime against individuals. The Committee will look at a wide range of issues including: how the provisions in the Fraud Act 2006 (the Act) are used in practice for the detection, prevention and prosecution of fraud; whether the Act is in need of reform; how the Act is being applied to tackle fraud committed online or through digital means; and what more needs to be done across the public and private sector to stop fraud committed through digital services. The deadline for responses is 22 April 2022. The Committee are particularly keen to receive submissions from victims of fraud. Read more on the Fraud Act 2006 Committee webpage.

Cyber Security Breaches Survey 2022 published

The Department for Digital, Culture, Media and Sport (DCMS) published its Cyber Security Breaches Survey 2022. In the last 12 months, 39% of UK businesses identified a cyber attack, remaining consistent with previous years of the survey. However, the report also found that enhanced cyber security led to higher identification of attacks, suggesting that less cyber-mature organisations in this space may be underreporting. Of the 39% of UK businesses who identified an attack, the most common threat vector was phishing attempts (83%), with 21% identifying more sophisticated attack types such as a denial of service, malware, or ransomware attack. Within the group of organisations reporting cyber attacks, 31% of businesses and 26% of charities estimated they were attacked at least once a week. One in five businesses and charities said they experienced a negative outcome as a direct consequence of a cyber attack. In its press release, the DCMS said the report shows that cyber attack are becoming more frequent, with organisations reporting more breaches over the last 12 months, although the number of businesses which experienced an attack or breach remained the same as in 2021. The DCMS urges businesses and charities to strengthen their cyber security practices now, and includes guidance in the press release regarding the steps that should be taken in this regard.