

RANKINGS AND AWARDS //

We were pleased to retain our top tier rankings in the recent round of legal directory publications. We remain in Band 1 for Financial Crime with Chambers & Partners UK, and in Tier 1 for Regulatory Investigations and Corporate Crime with Legal 500 UK. We have also retained our tier 1 rankings for Commercial Litigation, Banking Litigation, Competition Litigation and Tax Litigation and Investigations.

We have additionally been shortlisted for two awards at GIR Awards 2023, including partner Gayathri Kamalanathan being nominated for Investigations Professional of the Year.

RECENT PUBLICATIONS //

[Two steps forward, no steps back - corporate criminal liability reform](#) - client publication by Jonathan Cotton, Ella Williams and Orla Fox, on new corporate offences in the Economic Crime and Corporate Transparency Act.

THE ECONOMIC CRIME AND CORPORATE TRANSPARENCY ACT - RECEIVES ROYAL ASSENT //

The Government's flagship [Economic Crime and Corporate Transparency Act](#) received Royal Assent on 26 October 2023 and is now law. The Act is the second instalment, following last year's Economic Crime Act 2022, in the Government's efforts to fight economic crime and improve corporate transparency. The Act introduces wide-ranging reforms and in this article we highlight some of the key provisions.

Corporate Criminal Liability Reforms

Some of the most significant changes the Act delivers are reforms to the corporate criminal liability regime, namely a new offence of failure to prevent fraud (set out in s199-206) and expansion of the 'identification principle' (s196-198) - the test whereby criminal liability is attributed to corporates for crimes with a mental element. These provisions will make it much easier to fix corporates with criminal liability for economic crime.

The failure to prevent fraud offence is similar in design to the failure to prevent bribery offence set out in section 7 of the Bribery Act 2010. The new offence will make an organisation liable where a

fraud offence is committed by an associated person (including an employee, agent or subsidiary) with the intention of benefiting the organisation, or those to whom it provides services (eg. its customers or clients). The offence will only apply to large organisations, which meet at least two of the following three criteria: (i) more than £36 million turnover; (ii) more than £18 million in total assets; and (iii) more than 250 employees. Importantly, an organisation will have a defence if it can prove that it had in place reasonable prevention procedures. The offence is likely to come into effect in mid-to-late 2024 after the Government issues guidance on the reasonable procedures defence.

Under the expanded identification principle an organisation will itself commit an economic crime where the offence is committed with the involvement of a "senior manager". This will significantly broaden the number and type of employees who can trigger criminal liability for the business. The list of economic crimes to which this applies is comprehensive and includes, amongst others, bribery, money laundering, sanctions breaches, fraud and false accounting and certain offences under FSMA. This change comes into force on 26 December 2023.

These reforms create a powerful package that will make it easier for corporates to be prosecuted in the UK for economic crimes. We examine these new offences, and what they mean for in-scope organisations in the client briefing linked above.

Expanded search powers for the SFO

The Act also expands the scope of the Serious Fraud Office's (SFO) investigative powers. Currently, the SFO has powers (provided by section 2 of the Criminal Justice Act 1987) to search property and compel persons to answer questions and produce documents - without requiring a warrant. Section 2A of the Criminal Justice Act permits the SFO to use these 'section 2' powers at a pre-investigation stage but only in cases of international bribery and corruption.

The Act expands the SFO's Section 2A power to all SFO cases (s211). This means the SFO will be able to compel individuals and companies to provide information at the pre-investigation stage for suspected cases of fraud or domestic bribery and corruption. This is likely to result in an uptick in the number of companies receiving pre-investigation compulsory notices from the SFO.

Whilst the new Section 2A powers could allow the SFO to operate more efficiently by identifying the most egregious cases at an earlier stage, there is also the risk that it leads to excessive amounts of information and backlogs. As ever, a key factor in how effective these new powers will be is whether the SFO has the resources to use them and whether it does so effectively. The SFO's expanded Section 2A powers are not yet in force and will require secondary legislation.

Companies House Reforms

A large portion of the Act deals with reforms to Companies House, taking it from a passive recipient and repository of information to a more assertive regulator. The Act introduces, amongst other things, new identity verification requirements for directors, 'persons with significant control' (PSCs) and members of a limited liability partnership. It also introduces restrictions on who can file documents at Companies House on behalf of companies, the use of corporate directors and changes to company record keeping requirements. The Act also gives new powers to Companies House to take action against companies that persistently refuse to provide information, and powers to remove or decline to include inaccurate information on the companies register. Many of the Companies House Reforms will require secondary legislation and development of procedures and guidance by Companies House to implement the changes. It is expected that it may be a year before most of these provisions are enforceable.

New powers to seize cryptoassets

The Act will also give law enforcement agencies new powers to freeze and seize cryptoassets which are the proceeds of crime or associated with illicit activity, such as money laundering or fraud (Part 4 of

the Act). The Act achieves this by introducing amendments to the Proceeds of Crime Act 2002 (POCA), which are designed to bring cryptoassets within the scope of civil forfeiture powers under Part 5 of POCA and the criminal confiscation regimes under Parts 2, 3 and 4 of the POCA.

The Act also gives enforcement agencies the ability to confiscate cryptoassets before a suspect has been arrested, plus the authorisation in certain circumstances to destroy cryptoassets and enable the courts to order their sale. Some of these new powers on cryptoassets will only become enforceable after secondary legislation has been issued.

Customer information sharing

At present, businesses in the anti-money laundering (AML) regulated sector can only disclose information to each other if certain conditions are met, including that they must have: (1) notified the National Crime Agency (NCA); and (2) received a request from the NCA or another firm. This prevents firms from voluntarily and quickly sharing information with each other when they have concerns about economic crime.

The Act changes this by enabling firms to share customer information with each other for the purposes of preventing, investigating and detecting economic crime, without the involvement of law enforcement or a request from another firm. The Act allows: (1) direct sharing between two businesses in the AML regulated sector (s188); and (2) indirect sharing through a third-party intermediary (s189). These changes should encourage information-sharing and facilitate the detection of economic crime across the industry. These new provisions are not yet in force and will require secondary legislation.

Comments

The Act introduces sweeping reforms. The changes to the corporate criminal liability regime coupled with the new investigative powers for the SFO are particularly significant. Nick Ephgrave (the new Director of the SFO) has said that “this is *the most significant boost to the SFO’s ability to investigate and prosecute serious economic crime in over 10 years*” and “*big businesses can no longer turn a blind eye to fraud*”. Ephgrave’s background as a police officer and the new tools and offences at his disposal may well result in a more proactive investigative approach from the agency. However, it remains to be seen whether this is enough to turn the tide on the SFO’s recent difficult history and make it a more formidable prosecutor of corporate crime.

RECENT NEWS //

SFO Update: Investigation launched into suspected fraud at Axiom Ince; Ex-Balli Steel executive to be extradited to the Czech Republic; Investigation opened into funeral plan provider; Four individuals charged in relation to Patisserie Valerie collapse; ENRC loses application to obtain unredacted report

The SFO [announced](#) on 14 November that it has launched a criminal investigation into collapsed law firm Axion Ince in relation to £66 million of missing client money. Together with the Metropolitan Police, the SFO arrested seven individuals and carried out dawn raids across nine sites. The law firm, which operated 14 branches in England and Wales and employed over 1400 staff, stopped trading and was shut down by the Solicitors Regulation Authority in October, when client money was found to be missing from its accounts. The SFO will investigate how funds were passed from Axiom’s client accounts with Barclays to the State Bank of India to fund the alleged £66 million in spending. London’s Metropolitan Police confirmed that it had originally handled the case after a report from the SRA, but

referred it to the SFO “due to the complexity of the fraud”. Both authorities have said they will continue to work together during the investigation.

On 12 October, District Judge Michael Snow [ruled](#) that a former senior manager of Balli Steel’s Czech subsidiary, British national Andrew Small, should be extradited to the Czech Republic. The Czech authorities charged Small in 2021, accusing him of participating in a scheme to fraudulently obtain loans from local Czech lenders. Small challenged the extradition on the basis that most of his work for the company took place in the UK and that too much time has lapsed since the alleged crimes occurred. The judge was not persuaded, finding that “the gravity of the accusations clearly outweighed the factors against extradition”. The judge also added that there is “a strong public interest in the UK honouring its international extradition obligations”. This decision follows the convictions earlier this year of three other Balli Steel executives for fraud offences.

On 11 October, the SFO [announced](#) that it has opened a criminal investigation into suspected fraud at Safe Hands Plans Limited and its parent company SHP Capital Holdings Limited. The companies operated a pre-paid funeral plan scheme that collapsed in 2022, after failing to secure authorisation from the FCA. Approximately 46,000 plan holders had paid towards funeral plans before the company collapsed. The SFO is in the early stages of the investigation and has said it is “pursuing various lines of enquiry”.

The SFO has [announced](#) that it has brought fraud charges against four individuals, including a former director, who oversaw the financial collapse of Patisserie Valerie’s chain of nearly 200 high street bakeries. The individuals are charged with conspiracy to defraud for allegedly inflating Patisserie Valerie’s balance sheets and annual reports between 2015 and 2018. The SFO opened its investigation into suspected fraudulent conduct at the bakery chain in October 2018, shortly after the company abruptly stopped trading and entered administration. The SFO said the collapse of the company led to the loss of over 900 jobs across the UK.

On 9 October the High Court [found](#) that redactions made by the SFO in an internal report (the Byrne Report) should not be disclosed. The decision relates to the criminal investigation by the SFO into ENRC which was dropped in August and ENRC’s claim that a former SFO case controller and investigator leaked details of the investigation to the media. The Byrne Report set out the conclusions of the SFO’s internal misconduct investigation. The SFO argued that the redactions should remain on the grounds of privilege and confidentiality, as well as public interest immunity. The judge found that for each public interest immunity redaction “*the balance lies in favour of non-disclosure and the redactions on the basis of [public interest immunity] are upheld.*”

Co-founder of crypto exchange FTX convicted of fraud in New York federal court

On 27 October Sam Bankman-Fried, co-founder of cryptocurrency exchange FTX, was convicted in New York federal court on charges including securities fraud, wire fraud and money laundering. The jury found that Bankman-Fried spent FTX customer deposits to fulfil the lending obligations of his cryptocurrency trading hedge fund as well as on real estate in The Bahamas and on political donations. In a statement about the case Damian Williams, U.S. attorney for the Southern District of New York said “Bankman-Fried perpetrated one of the biggest financial frauds in American history – a multibillion-dollar scheme designed to make him the King of Crypto – but while the cryptocurrency industry might be new and the players like Bankman-Fried might be new, this kind of corruption is as old as time.” Bankman-Fried also faces a second trial next year on charges of conspiracy to violate the U.S. Foreign Corrupt Practices Act over an alleged bribe to a Chinese official.

FCA Update: Censure for London Capital & Finance plc; Decision Notice issued to ex-Barclays CEO; ADM Investor Services International Ltd fined for AML failings;

Equifax fined over cybersecurity breach; FCA secured confiscation order against convicted CFO of Redcentric

On 11 October the FCA published a [Final Notice](#) to London Capital and Finance plc for unfair and misleading minibond financial promotions. The Final Notice is part of a wider series of actions being taken in relation to matters connected to London Capital. The FCA found that, between June 2016 and December 2018, London Capital used financial promotions to market minibonds to retail investors, many of whom were vulnerable, and that these promotions presented a misleading picture. Investors were not told about, among other things, the presence of hidden charges and the high-risk and unsustainable nature of the lending being carried out by London Capital. The FCA also found that it used bondholders' money to fund seemingly independent comparison websites to showcase its minibonds next to safer investments, which had a lower rate of return, to entice retail investors to invest in its high-risk products. London Capital also advertised the minibonds as ISA compatible when this was not the case. Since London Capital is insolvent and in administration, the FCA decided to censure the firm instead of imposing a fine. The FCA is not requiring London Capital to pay restitution.

The FCA published a [Final Notice](#) on 12 October, addressed to James ('Jes') Staley (ex-CEO of Barclays) for recklessly approving a letter to the FCA containing two misleading statements about the nature of his relationship with Jeffrey Epstein. Mr Staley has been fined £1.8 million and has been banned from holding a senior management or significant influence function in financial services. Mr Staley has referred the Decision Notice to the Upper Tribunal. Any findings in the Decision Notice are therefore provisional (and will not take effect pending the determination of the case by the Tribunal).

On 2 October, the FCA [fined](#) ADM Investor Services International Ltd over £6.4 million for breaches of Principle 3 (Management and control) of its Principles for Businesses, for inadequate AML systems and controls. ADM's business nature and client base meant it was susceptible to potentially high levels of money laundering risk. The FCA raised concerns with ADM in 2014 regarding the broker's absence of a formal process to classify customers by risk. Following this, during a 2016 firm visit, the FCA identified further systemic failings. As a result of these findings, ADM was asked by the FCA to enter into a voluntary requirement, which would limit higher risk aspects of its business until its systems and controls were deemed adequate. ADM complied with the voluntary requirement, which was later lifted in January 2018. The FCA concluded that ADM had breached Principle 3 on the basis it had failed to comply with regulatory and legal AML requirements and failed to conduct adequate remediation of the weaknesses identified during the 2014 assessment. As such, the FCA imposed a financial penalty of over £6.4 million. ADM did not dispute the FCA's findings and qualified for a 30% settlement discount. Without this discount the FCA would have imposed a financial penalty of just over £9.2 million.

On 13 October, the FCA published a [Final Notice](#) and fined Equifax Limited almost £11.2 million over a cybersecurity breach. The FCA said Equifax had failed to manage and monitor the security of UK consumer data it had outsourced to its US-based parent company in breach of Principles 3, 6 and 7 of the FCA's Principles for Business. The breach allowed hackers to access the personal data of millions of people and exposed UK consumers to the risk of financial crime. In calculating the fine, the FCA noted that Equifax reached an agreement with the authority on the amount of the penalty as well as other terms bringing the total down by 30 percent. The FCA also took into account the company's cooperation during the investigation and the remedial steps it has taken since the breach as mitigating factors. This decision serves as a stark reminder to regulated firms that the risk of enforcement action for cybersecurity breaches is not confined to the ICO. For more on this decision see our client briefing on [The Lens](#).

On 2 November, [Southwark Crown Court imposed a confiscation order](#) of £355,369 against Timothy Coleman, former CFO of Redcentric plc, an IT service provider. Coleman was convicted in February 2022 in an FCA-led prosecution, on charges of false accounting and making misleading statements to

the market. The statements overstated Redcentric's cash position and downplayed its debt. Shareholders suffered losses when the true position was uncovered. The confiscation order of £355,569 represents the value of Coleman's financial benefit from the offences. He was also ordered to pay the prosecutions costs of £119,630.

ICO Update: Enforcement action over generative AI chatbot; Reprimand issued to GAP; Consultation on draft fining guidance

On 6 October the ICO issued a [preliminary enforcement notice](#) against Snap Inc and Snap Group Limited, which operate the popular Snapchat messaging platform, over potential failures to properly assess the privacy risks posed by its generative AI chatbot 'My AI'. The My AI chatbot, powered by OpenAI's GPT technology, was the first example of generative AI embedded into a major messaging platform in the UK. The ICO's investigation provisionally found the risk assessment Snap conducted before it launched 'My AI' did not adequately assess the data protection risks posed by the generative AI technology, particularly to children. For more on this see our client publication on [The Lens](#).

The ICO has issued a [reprimand](#) to Gap Personnel Holdings Limited in respect of infringements of Article 32 (1), Article 32 (1) (b) and Article 32 (1) (d) of the UK GDPR. The organisation did not have appropriate security measures in place, which resulted in an unauthorised threat actor being able to access individuals' personal data twice within a 12-month period.

The ICO published a [consultation](#) on 2 October, regarding how it decides to issue penalty notices and calculate fines under the UK GDPR and DPA 2018 (it does not cover PECR). The guidance covers the ICO's legal powers to impose fines, the circumstances in which the Information Commissioner would consider it appropriate to issue a penalty notice and how the amount of the fine is calculated, including on the concept of an undertaking and aggravating or mitigating factors. The guidance will replace parts of the ICO's Regulatory Action Policy on its approach to fines. The consultation closes on 27 November 2023. For more on this see our client briefing on [The Lens](#).

OFSI Update: OFSI uses disclosure power for first time; Sabre Corp self-reports to OFSI

OFSI used its new disclosure enforcement power for the first time earlier this year against Wise Payments Limited - a regulated fintech company. This power allows OFSI to issue a report detailing financial sanctions breaches in cases where it doesn't also impose a monetary penalty. OFSI acquired this power via the Economic Crime (Transparency and Enforcement) Act 2022. The [report](#) says Wise violated sanctions by making funds available to a company owned or controlled by a designated person. The breach related to a cash withdrawal of £250. Wise froze the business account the day the person was designated, but it took Wise a further five days to block the account's facility to withdraw cash via a debit card. The delay was due to Wise's policy that suspended accounts need to be reviewed by its sanctions specialist. OFSI's decision to publish Wise's breach shows its willingness to pursue even low value violations.

In a [market filing on 2 November](#), Sabre Corporation, a specialist booking software company, confirmed that it told OFSI about a potential sanctions breach in the second half of 2022. Sabre say it received amounts from a Russian airline which were "not material in amount" but may have violated UK sanctions. It remains to be seen what action OFSI will take. If the monetary value of the breach is low (as Sabre contend) we may see OFSI exercising its disclosure power again in the near future.

Sanctions Litigation Update: High Court dismisses first SAMLA licensing challenge; Court of Appeal decision on effect of Russian sanctions on pending litigation

On 26 October the High Court [handed down its decision](#) in *R (Fridman) v Treasury [2023] EWHC 2657*, upholding OFSI's decision to refuse Fridman certain licences. Fridman has been sanctioned under the Russian Sanctions Regulation since March 2022. In August 2022 he applied to OFSI for licences to make several payments based on the derogations in Schedule 5 of the Regulations for basic needs, prior obligations and routine maintenance of assets. In December 2022 OFSI permitted several payments, but refused three payments in respect of his £44 million London home. Fridman challenged OFSI's decision before the High Court. The Court agreed with OFSI's interpretation of the derogations, meaning Fridman did not obtain the additional licences. The judgment provides guidance on a number of issues arising out of the Russian Sanctions Regulations and the Sanctions and Money Laundering Act 2018 (SAMLA), including that OFSI retains a residual discretion under Regulation 64 to refuse to grant a licence payment - even if the conditions for a derogation are met.

On 6 October the Court of Appeal [handed down judgment](#) in *Boris Mints & Ors v PJSC National Bank Trust & Anor [2023] EWCA Civ 1132*. The case involves claims by two Russian banks alleging a conspiracy to enter into uncommercial transactions. The first bank was designated under the Russia Regulations and the defendants argued that the second bank (NTB) was owned or controlled by designated persons (within the meaning of Regulation 7), namely Vladimir Putin. The defendants brought an application to stay the proceedings. The Court of Appeal dismissed the application finding that that entry of a money judgment was not prohibited by the sanctions regime and that various litigation steps (eg. payment of cost orders) could be authorised by OFSI on licensing grounds. However, the Court of Appeal also addressed the question of whether NTB was under the control of a designated person (Vladimir Putin), on an obiter basis. The Court found that the "control test" should be interpreted broadly and that entities could be controlled by a designated person's political influence. As a result, the Court of Appeal found that the Claimants were correct in their interpretation that NTB was controlled by a designated person. This was a radical departure from the lower court's narrower interpretation of 'control' and could have wide-ranging ramifications. At its highest, it could mean that every company in Russia could be considered to fall with the sanctions regime as Vladimir Putin can exert political control through his position. However, in a [statement following the judgment the Foreign Commonwealth and Development Office](#) said that the UK government will not presume that a business operating in a country where a public official is sanctioned would be enough to demonstrate that that person 'controls' the entity.

FRC impose record fine on KPMG over Carillion audit failings

On 12 October, the Financial Reporting Council (FRC) issued [two Final Settlement Decision Notices](#) under its audit enforcement procedure and imposed sanctions against KPMG LLP, KPMG Audit Plc and two former audit partners, following the conclusion of its investigations into the audits of Carillion plc. Carillion plc was an outsourcing giant, handling large numbers of government contracts. Its business collapsed in January 2018 costing thousands of jobs and endangering critical activities such as school meals and hospital cleaning across the UK. A few months before its collapse KPMG had given an unqualified audit opinion. Executive Counsel of the FRC said "the number, range and seriousness of the deficiencies in the audits of Carillion during the period leading up to its failure was exceptional and undermined the credibility and public trust in audit." The fine imposed was £30 million, reduced by 30% to around £21 million after cooperation and admissions were taken into account.

SRA issues guidance for solicitors on interviews

On 26 September, the [SRA published guidance](#), on a solicitor's responsibilities and obligations when involved in interviews in an external investigation. The guidance focuses on the different issues a

solicitor needs to consider when acting for: (a) the company (b) the employee (c) more than one employee or (d) both the employee and the company. In particular, the Guidance mentions avoiding any uncertainty about who the solicitor is acting for, the existence of possible conflicts of interest and the risk of unfair advantage being taken of an interviewee. The guidance provides a helpful reminder on a solicitor's responsibilities under the SRA's Standards, Regulations and Codes in this context.

Financial Action Task Force (FATF): New Consultation on Beneficial Ownership and Transparency of Legal Arrangements; Changes to FATF Recommendations following Plenary Meeting

The FATF has published a [consultation](#) on draft risk-based guidance on beneficial ownership and transparency of legal arrangements relating to recommendation 25. Recommendation 25 specifies that countries should ensure that there is adequate, accurate and up-to-date information on express trusts and other similar legal arrangements, including information on the settlor(s), trustee(s) and beneficiary(ies), that can be obtained or accessed efficiently and in a timely manner by competent authorities. The deadline for responses to the consultation is 8 December 2023.

The FATF has also published the [outcomes of its plenary meeting](#), which took place on 25-27 October 2023 and included discussion of key money laundering, terrorism financing and proliferation financing issues. Described as "a major milestone", delegates agreed on a significant set of amendments to the FATF Recommendations that will provide countries with a much stronger toolbox of measures to deprive criminals of the proceeds of crime. Following amendments to beneficial ownership and transparency standards (see item above), delegates also agreed to release for public consultation the updated FATF Risk-Based Guidance on Recommendation 25. The next plenary meeting will be held in February 2024

CMA settles investigations into Meta and Amazon

The [CMA announced](#) that it has formally ended two separate abuse of dominance investigations into Meta and Amazon. The investigations have been settled without with the CMA reaching a decision on whether the tech companies breached UK competition law, in exchange for commitments by the companies. The commitments require Meta to limit its use of advertising data in its product development and Amazon to guarantee all products are treated equally when featured in its 'Buy Box'. CMA chief executive said there will likely be more of this type of "constructive resolution" under the incoming Digital Markets, Competition and Consumers Bill.

Ofcom publishes its approach to implementing the Online Safety Act

On 26 October, Ofcom published a [document](#) setting out its approach to implementing the Online Safety Act 2023 and what it expects from tech firms. The document sets out the key actions companies should take, how Ofcom will achieve compliance and the outcomes it expects the new rules to deliver. Ofcom will publish guidance and codes of practice for in-scope companies on compliance with the Act in three stages - first duties around illegal harms, second duties regarding child safety and the protection of women and girls, and third transparency, user empowerment and duties on categorised services.

Horizon Scanning

Look out for:

- Secondary Legislation implementing many of the substantive provisions in the Economic Crime and Corporate Transparency Act

