SLAUGHTER AND MAY/

28 JANUARY 2026

GLOBAL INVESTIGATIONS BULLETIN

PRESERVING THE INTEGRITY OF DEFERRED PROSECUTION AGREEMENTS: GÜRALP SYSTEMS V SFO //

On 13 January, the Administrative Court delivered a significant judgment that reinforced the integrity and effectiveness of the Deferred Prosecution Agreement (DPA) regime. The Court held that the DPA entered into by Güralp Systems Limited remained enforceable beyond its stated expiry, where the company had failed to meet its payment obligations.

DPAs enable corporate entities to avoid prosecution and conviction by admitting facts, paying a financial penalty, and implementing remedial measures to address alleged wrongdoing. In this case, Güralp sought to rely on a technicality in the terms of its DPA to argue that its obligation to pay the financial penalty ceased to be enforceable once the agreement reached its specified expiry date.

Had Güralp's argument succeeded, the implications would have been significant. It would have permitted a DPA counterparty to evade agreed financial penalties simply by delaying payment, materially undermining the effectiveness of DPAs and eroding confidence in the regime as a mechanism for corporate accountability.

In rejecting Güralp's position, the Court emphasised that DPAs are public-interest instruments, not ordinary commercial contracts. As such, they must be interpreted in a manner that gives effect to their statutory purpose and the wider public interest they are designed to serve.

The dispute

Güralp entered into a DPA with the Serious Fraud Office (SFO) on 22 October 2019 in connection with allegations that it had conspired to make corrupt payments to a South Korean official and had failed to prevent bribery, contrary to section 7 of the Bribery Act 2010. Under the terms of the DPA, Güralp was required, among other things, to disgorge profits of approximately £2.07 million, with payment due by 22 October 2024, five years after the agreement was executed. Güralp did not make the required payment by the deadline — or at all — and accepted that fact.

Thirty days after the payment deadline had passed, in November 2024, the SFO applied to the Crown Court under paragraph 9 of Schedule 17 to the Crime and Courts Act 2013 (the Act), alleging a breach of the DPA. A successful application under paragraph 9 may result either in agreement on proposals to remedy the breach or in termination of the DPA, enabling the prosecution to proceed.

Güralp challenged the application on the basis that a deferred prosecution agreement must include an expiry date, which in this case was specified in clause 4 as 22 October 2024. It argued that the DPA therefore came to an end on that date, regardless of its failure to make the required payment. Güralp contended that an application for breach could only be made while the DPA remained "in force" and that, because the SFO's application was issued around 30 days after 22 October 2024, the SFO was barred from pursuing it.

The central issue for the Court was therefore one of contractual interpretation: whether, on its proper construction, the DPA remained in force at the time the SFO issued its application in November 2024. Applying the established principles of contractual construction set out in *Arnold v Britton*, the Court agreed with the SFO that the DPA continued to operate.

The Court's findings

1. The DPA remained in force

The Court held that the DPA did not expire automatically on 22 October 2024, in circumstances where payment had not been made. Properly construed, and read as a coherent whole, the DPA continued in force, in order to permit the SFO to take enforcement action. In reaching that conclusion, the Court relied on several features of the agreement.

- **Expiry mechanism:** Clause 4 provided that the DPA would terminate on or before 22 October 2024 *"when the financial terms have been fully satisfied"*, indicating that non-payment prevented automatic expiry.
- **Express breach and enforcement provisions:** Non-payment was expressly identified as a breach in clause 14, with contractual mechanisms for enforcement set out in clauses 25 and 26.
- **Timing of breach:** A breach of the payment obligations could only arise after midnight on 22 October 2024; until that point, the obligation had not technically been breached. Read together with the enforcement provisions, this supported the conclusion that the parties contemplated the DPA continuing beyond that date to allow time for an enforcement application to be made.

2. *2. Public-interest context mattered*

In applying the principles of contractual interpretation, the Court placed significant weight on the public-interest context in which the DPA was approved. In particular, it treated the 2019 DPA approval judgment as part of the objective background known to the parties and relevant to the proper construction of the agreement.

The Court emphasised that:

- a DPA is a statutory instrument, approved by the court as being in the interests of justice and on terms that are fair, reasonable and proportionate;
- such court approvals have no parallel in ordinary commercial negotiations and are designed, in part, to protect the integrity of the criminal justice system; and
- a DPA would not ordinarily be approved on the basis that its core financial obligations could simply fall away if they were not met.

Against that background, the Court concluded that *"very clear words would be required"* to demonstrate that the parties intended Güralp to be relieved of its obligation to pay any outstanding amounts after 22 October 2024. There were no such words in the DPA. Indeed, the Court found that it would be *"quite contrary to the interests of justice"* if a company could avoid the financial penalties imposed under a DPA simply by failing to pay by the deadline.

3. Reasonable time for enforcement

The Court therefore concluded that the DPA remained in force after 22 October 2024 in order to allow the SFO a reasonable period in which to take enforcement action. If no application is made within that reasonable period, the DPA will expire. In this case, the SFO's application - made within 30 days of the breach - was held to have *"certainly"* been brought within a reasonable time. The Court did not, however, define the outer limits of what may constitute a reasonable period.

The judgment therefore establishes that a DPA will not expire automatically on its stated expiry date where payment obligations remain outstanding. However, the length of time available to the SFO to bring enforcement action before a DPA expires remains unresolved. In future cases, enforcement applications brought significantly later than the 30 days seen here may be open to challenge.

Practical implications and Next Steps

This decision provides a clear reaffirmation of the enforceability and integrity of the DPA regime. DPAs are statutory instruments, approved by the court and designed to operate in the public interest. They cannot be circumvented through technical or opportunistic arguments. Courts will construe DPAs by reference to their statutory purpose, placing particular weight on safeguarding the integrity of the criminal justice system and advancing the public interest.

Parties to DPAs should therefore proceed on the basis that non-compliance with their terms - even after the stated expiry date - may give rise to enforcement action, including variation of the DPA's terms or its termination and the reinstatement of criminal proceedings.

The SFO's breach application to the Crown Court may now proceed, although the route the Court will ultimately adopt remains uncertain. It may approve measures to remedy the breach, for example by imposing a new payment schedule. Alternatively, the DPA may be terminated, permitting the SFO to pursue a prosecution. The latter course would be more complex: the underlying conduct occurred over a decade ago, the individuals involved were acquitted at jury trials in 2019, and the SFO would still be required to satisfy the Full Code Test, demonstrating both a realistic prospect of conviction and that prosecution would be in the public interest. These factors may present significant challenges, particularly where a corporate defendant cannot face imprisonment and may lack the financial means to discharge the penalty.

However, the DPA provides that, if prosecution becomes necessary, the Statement of Facts agreed by Güralp in 2019 may be relied upon as admissions by the company under section 10 of the Criminal Justice Act 1967. If criminal proceedings are reinstated, this creates the prospect of a novel enforcement scenario in which corporate admissions made under a DPA are deployed to prosecute a company many years after the agreement was entered into.

Whichever route is taken, the case marks new territory for UK enforcement. It is the first occasion on which the SFO has sought to enforce a DPA against a corporate entity for breach. By contrast, enforcement of DPA breaches is more established in the United States: for example, Boeing's breach of its DPA with the US Department of Justice in 2024 led to the reinstatement of criminal proceedings, culminating in a guilty plea and increased financial penalties.

The Güralp decision represents an important stage in the development of the UK DPA regime and sends a clear signal that, where DPA terms are not satisfied, enforcement risk does not end when a DPA reaches its stated expiry date.

RECENT NEWS //

SFO Round-Up: Leadership Departures at the SFO; Dawn Raids Mark New Investigation into Home REIT; Reports of Joint Inquiry with Malaysian Authorities into IJM; Successful SFO Confiscations; Guilty Pleas in Ethical Forestry Fraud Case; Safe Hands Directors Charged with Fraud; SFO Publishes Guidance on Foreign Bribery Indicators

January has been an active month for the Serious Fraud Office (SFO), despite the unexpected announcement that its Director, Nick Ephgrave, will step down at the end of March — around two and a half years before the end of his term. Ephgrave will remain in post until then, after which an interim Director will be appointed pending the completion of a formal recruitment process. His departure comes at a critical time for the SFO. Three other senior officials, including the Head of Bribery Sara Chouraqui, and case controllers Elizabeth Collery and Victoria Jacobson, have also announced that they are leaving the agency. This represents a significant loss of senior experience on complex multinational investigations, at a point when the SFO has a larger caseload than in recent years, including high-profile trials listed for 2026 involving former employees of Patisserie Valerie, and Petrofac.

Just prior to the news of Ephgrave's retirement, on 14 January, the SFO announced the launch of a new investigation into the management of Home Reit, a social housing vehicle that was listed on the London Stock Exchange. The investigation was initiated through dawn raids, during which six individuals were arrested and seven sites were searched. The investigation concerns allegations of fraud and bribery in relation to Home REIT's business model, which involved acquiring properties that were block-let to charities and community interest companies, with investor returns promised from the resulting rental income.

Separately, it has been reported that the Malaysian Anti-Corruption Commission (MACC) is cooperating with the SFO on potential inquiries into construction company IJM, in connection with possible money laundering. Reports indicate that the SFO has submitted a number of information requests to the MACC regarding IJM, although no formal investigation has yet been announced by the SFO.

The SFO has also continued its efforts to recover funds for victims of fraud. Using civil recovery powers under section 281 of the Proceeds of Crime Act (POCA) the SFO recovered more than £400,000 in relation to a 2002 email fraud scheme operated by Abdullah Ali Jammal, a former director of a retailer-depositor bank. The scheme defrauded eighteen victims, many of whom lost tens of thousands of pounds. Mr Jammal fled the UK before he could be charged and was therefore never convicted. The SFO has said that the case's unusual circumstances justified an alternative approach to recovering funds. This follows another successful confiscation order in December 2025, which secured over £928,000 following an investigation linked to convicted former Axiom investment manager David Kennedy. These recovered funds will also be returned to the victims of that fraud.

On 16 January, the SFO announced that three former directors of Ethical Forestry Limited had pleaded guilty to charges of fraud. The investigation, which began in 2017, uncovered that the directors had misled around 3,000 UK investors over a seven-year period by encouraging them to withdraw funds from legitimate pension schemes to invest in tree-planting projects in Costa Rica. While trees were planted, no provisions were made for commercial harvesting, meaning investors' funds could not generate the promised returns.

On 22 January, the SFO charged Richard Wells, a former director of SHP Capital, and Neil Debenham, a former senior executive, with conspiracy to defraud. The investigation into Safe Hands Plans Ltd and its parent, SHP Capital, opened in 2022 and concerned a pre-paid funeral plan scheme that collapsed the same year after failing to secure authorisation from the FCA. Approximately

46,000 plan holders had made payments towards funeral plans before the collapse.

Finally, towards the end of last year, the SFO, together with law enforcement partners from the International Foreign Bribery Taskforce (IFBT), published Guidance setting out an agreed list of potential indicators of foreign bribery. The IFBT comprises prosecuting agencies from the "Five Eyes" alliance — the UK, US, Canada, Australia, and New Zealand. The Guidance is designed to support professionals in high-risk sectors, compliance teams, and the broader business community by drawing on the collective casework and expertise of all IFBT members. It does not introduce new or novel red flags; the listed indicators will already be familiar to organisations with established anti-bribery programmes. Its primary value lies in establishing a minimum international standard of bribery indicators, providing a practical benchmark at a time when enforcement priorities can differ across jurisdictions.

The indicators are grouped under five headings: conduct, government affiliations, country links, ownership, and other associations. Key examples include opaque or overly complex ownership structures, involvement of trusts or shell companies, use of third-party agents or consultants, lack of rationale in awarding contracts, ownership of high-value assets disproportionate to income or company size, disproportionately high commissions, and the involvement of politically exposed persons (PEPs). Individually, these indicators do not automatically signify criminal activity. However, when considered together and in context, they may highlight circumstances that warrant closer scrutiny.

For organisations with existing, effective anti-bribery frameworks, the Guidance is unlikely to require policy overhauls. Rather, it provides a useful international benchmark and can serve as a practical checklist to refresh and assess existing programmes.

CPS Update: Fund Managers Convicted for Fraud Linked to Libyan Investment Fund

Three fund managers have been convicted of orchestrating a fraud that diverted £11.4 million from funds intended for the Libyan people. Frederic Marino and Yoshika Ohmura were found guilty of fraud by abuse of position following a retrial at Southwark Crown Court, while Aurelien Bessot had previously pleaded guilty to the same offence. The CPS established that the individuals had exploited their roles managing investments linked to Libya's sovereign wealth fund. Rather than optimising the investments, they used a London-based hedge fund to generate undisclosed fees and channelled the proceeds through shell companies, causing substantial losses to the Libyan Investment Authority.

FCA Round-up: Investigations Announced into The Claims Protection Agency and WHSmith; Upper Tribunal Upholds Ban and Fine for Dishonest Adviser; Consultant Fined for Insider Dealing; Former Carillion Finance Directors Fined; and Building Society Fined for Financial Crime Control Failings

The High Court has issued the second part of its judgment dismissing a judicial review of the FCA's decision to publicly name a firm under investigation. The first part of the judgment, handed down in October 2025, was covered in earlier editions of this publication. The second part follows the Court of Appeal's refusal to grant permission to appeal and provides additional information that could not previously be made public. The firm was identified as The Claims Protection Agency Ltd (TCPA) and operates in the motor finance claims sector. The FCA's investigation focuses on TCPA's promotion and handling of motor finance claims, including marketing claims that customers could receive higher redress than likely under FCA guidance. The regulator is also examining whether customers were misled about fees or pressured into signing up.

On the 19 December 2025, the FCA also announced an investigation into WH Smith in connection with its compliance with listing and disclosure obligations. The company disclosed the investigation in a market announcement, which the FCA subsequently confirmed later the same day. This represents the fifth publicly named investigation by the FCA since the publication of its Updated Enforcement Guidance in June 2025, which introduced revised transparency measures for the regulator.

The FCA continues to take robust action against individuals whose misconduct undermines consumer trust. The Upper Tribunal has upheld the FCA's decision to ban Mr Reynolds from working in financial services and fine him over £2 million. Reynolds was found to have acted dishonestly in giving pension transfer advice and investment recommendations, disregarding his customers' interests. The FCA found that he had encouraged British Steel Pension Scheme members to transfer out of their defined pension scheme despite knowing the advice was unsuitable, recommended high-risk, inappropriate investments while concealing exit fees, and falsified documents. When confronted, he was dishonest with regulators, allowed key evidence to be destroyed, and transferred his family home into a trust to avoid paying debts. Therese Chambers described Reynold's conduct as among the worst seen by the regulator in all British Steel Pension Scheme cases.

On 7 January, the FCA fined two former finance directors of Carillion for issuing misleading statements prior to the company's collapse eight years ago. The FCA found that Richard Adam and Zafar Khan were aware of serious financial difficulties in Carillion's UK business but failed to reflect these in company announcements or alert the Board and audit committee, resulting in inadequate oversight. As finance directors, they were responsible for the company's financial reporting systems and controls. The FCA concluded that both acted recklessly and were knowingly involved in breaches of the Market Abuse Regulation and Listing Rules, imposing fines of £232,800 and £138,900, respectively.

On 16 January, the FCA fined Russel Gerrity £309,843 for insider dealing in breach of Article 14 of the Market Abuse Regulation, reflecting the regulator's heightened focus on market abuse. Gerrity, a consultant in the petrophysical sector, had access to non-public information about oil and gas discoveries. The FCA found that between October 2018 and January 2022, he profited by purchasing shares in Chariot Oil & Gas Limited and Eco (Atlantic) Oil and Gas Plc ahead of announcements that increased their share prices. On a separate occasion, he avoided a loss by selling shares before an announcement that no resources had been found, which subsequently caused the share price to fall. The FCA noted that some of Gerrity's trading was first flagged through Suspicious Transaction and Order Reports (STORs), highlighting the critical role of industry in detecting market abuse.

In its final fine of 2025, the FCA imposed £44 million on Nationwide Building Society for inadequacies in its financial crime systems and controls. The regulator found that Nationwide's systems were unsuccessful in maintaining up-to-date due diligence and risk assessments for personal current account customers and in monitoring their transactions. Some customers were using personal accounts for business purposes, leading to inadequate processes around managing the associated financial crime risks. As a result, the FCA found that the firm could not identify, monitor, or manage money laundering risks effectively, nor maintain an accurate view of higher-risk customers. This fine underscores the FCA's ongoing focus on ensuring firms maintain robust systems and controls to prevent financial crime.

OFSI Fines Bank of Scotland £160,000

On 26 January, OFSI announced its first fine of 2026, imposing a £160,000 penalty on the Bank of Scotland for making funds available to a designated person without a licence. The bank opened a personal current account for the designated individual and processed 24 payments totalling £77,384 to and from that account. The breach was voluntarily disclosed in March 2023 by the bank's parent, Lloyds Banking Group (LBG). As a result, OFSI applied the full 50% voluntary disclosure discount. Although LBG had implemented sanctions screening measures, its automated systems failed to detect a spelling variation of the designated individual's name. The account had been opened using a UK passport that reflected the alternative spelling, which differed from the name recorded on the sanctions list and was therefore not flagged by the bank's automated screening tools. The case highlights the inherent limitations of automated sanctions screening and underscores the importance of robust contingency procedures to identify and manage screening failures.

High Court Upholds OFSI's Power to Amend Sanctions Licences in Insolvency Context

The High Court has upheld OFSI's decision to amend a General Licence governing VTB Bank's participation in the administration of its UK subsidiary, VTB Capital plc (VTBC) - confirming the breadth of OFSI's licensing powers under the UK sanctions regime.

VTBC entered administration in December 2022 and was operating under a General Licence permitting payments while its affairs were managed by insolvency practitioners. The administrators proposed a creditors' scheme of arrangement under which VTBC's parent, VTB Bank (Russia's second-largest bank) could participate in distributions on a "frozen" basis, with payment deferred until non-sanctioned creditors had been paid.

VTB Bank indicated that it would vote against the proposed creditors scheme. This risked placing it in a better position than non-sanctioned creditors, given that it was also pursuing enforcement action in Russia. In response, OFSI amended the licence so that any distributions to VTB Bank were subject to deductions reflecting the value of assets affected by the Russian enforcement activity. Following the introduction of the deductions mechanism, VTB Bank no longer had sufficient voting power to block the scheme, and it was approved.

VTB Bank subsequently brought judicial review proceedings challenging OFSI's deduction mechanism. The court rejected VTB Bank's argument that OFSI had exercised its sanctions powers for an improper purpose or to rewrite insolvency outcomes. What mattered was the purpose of the decision - supporting the objectives of the sanctions regime and mitigating unintended harm to third parties - rather than the commercial impact on the sanctioned entity.

Several wider points also emerged. First, OFSI can legitimately use licensing to shape how a designated person participates in insolvency proceedings where this supports an orderly process and protects non-sanctioned creditors. Second, challenges to licence amendments face a high bar: orthodox judicial review principles apply, including the demanding threshold for irrationality. Third, Article 6 ECHR was not engaged, as the licence amendment permitted limited dealings with frozen assets rather than determining civil rights. Finally, OFSI's published guidance on advance stakeholder engagement was treated as aspirational rather than binding, with urgency, asset-preservation concerns and policy risk justifying more limited consultation. Overall, the decision reinforces OFSI's wide discretion to amend licences swiftly where sanctions policy is engaged.

ICO Update: DSAR Guidance Published, Joint Cross-Border Investigation, and Enforcement Action

The Information Commissioner's Office (ICO) has published updated guidance on data subject access requests (DSARs), reflecting changes introduced by the Data (Use and Access) Act 2025 (DUA Act) and recent case law. Timed to coincide with the DUA Act's latest set of commencement regulations, the guidance clarifies several practical aspects of DSAR management. Key DUA Act changes reflected in the ICO Guidance include:

- Controllers can 'stop the clock' where clarification is reasonably required.
- Data subjects must be informed of their right to make a complaint to the controller.
- The volume of requests is a relevant factor when determining if a request is unreasonable or disproportionate.

Other changes reflected in the guidance are:

- Repeated demands for information in different formats may be treated as manifestly unfounded or excessive.
- Controllers must disclose specific recipients in supplementary information.
- Exemptions can apply to supplementary information.

Overall, the updated guidance balances operational flexibility with heightened transparency requirements. While the DUA Act clarifications are intended to make the day-to-day management of DSARs more manageable, the case law-driven requirement to disclose specific recipients by default raises the bar for transparency and record-keeping. Organisations may need to map data disclosures accurately and update transparency and exemption frameworks, which should improve predictability and defensibility in the long term.

The ICO is also leading a joint cross-border investigation with data protection authorities in Jersey, Guernsey, and the Isle of Man into a June 2025 cyber incident affecting trade union Prospect Custodian Trustees Ltd. The regulators are reviewing the extent of personal data exposure, the adequacy of Prospect's security controls, and compliance with breach notification obligations. Representing over 160,000 members, Prospect is cooperating fully with the investigation. The case underscores the growing cross-border collaboration in data protection enforcement.

In parallel, the ICO has taken enforcement action in several new cases. LastPass UK Ltd was fined £1.2 million for security failings linked to a 2022 breach affecting up to 1.6 million UK users. The ICO found that inadequate technical safeguards allowed unauthorised access to a backup database, although there is no evidence that customer passwords were decrypted, as these are stored locally on users' devices. Separately, on 20 January, the ICO also fined Allay Claims Ltd £120,000 and ZMLUK Ltd £105,000 for sending millions of unsolicited marketing messages in breach of the Privacy and Electronic Communications Regulations (PECR). Allay sent over 4 million promotional texts about PPI tax refunds without valid consent, while ZMLUK sent more than 67 million marketing emails using third-party data where recipients could not provide informed consent. Both companies failed to offer clear opt-out mechanisms and misused the 'soft opt-in' exemption. The ICO emphasised that businesses must obtain explicit consent before sending marketing communications and will continue to act against unlawful messaging that causes harm.

Bank pays US$312m to Settle French Dividend Tax Probe

France's national financial prosecutor (PNF) has announced a €267.5 million settlement with HSBC to resolve allegations of dividend tax fraud involving its Paris branch and London traders. Approved under a judicial public interest agreement (CJIP) on 8 January, the settlement concludes an investigation into trades between 2014 and 2019. The PNF stated that the fine reflected the bank's size, the nature of the misconduct, and public impact, but was reduced due to HSBC's cooperation, acknowledgment of wrongdoing, and corrective measures.

HORIZON SCANNING //

What to look out for:

- **Major SFO trials in 2026:** Several high-profile SFO prosecutions are scheduled for 2026. The fraud trial of former employees of the collapsed bakery chain *Patisserie Valerie* is listed for three-months commencing on 2 March 2026. Later in the year, the trial of senior executives in the *Petrofac* bribery case is due to begin on 5 October 2026.
- **Independent Review of Disclosure and Fraud Offences (Jonathan Fisher KC):** The final report and the government's recommendations are expected shortly. In an interim update published on 26 January, Fisher KC identified several priority areas likely to feature in the final report, including enhanced data sharing, stronger upstream fraud prevention, wider use of modern technology across the system, and enhanced international cooperation by the UK.

OFSI enforcement reforms: OFSI's response to its 2025 consultation on strengthening its enforcement framework is expected later this year. The consultation proposed a number of significant changes, including:

- publication of a new case assessment matrix, together with expanded guidance on enforcement decision-making;
- the introduction of a settlement scheme for monetary penalty cases;
- a streamlined enforcement process for information, reporting and licensing breaches, supported by standalone guidance; and
- increases to the statutory maximum penalties for financial sanctions breaches.

CONTACTS

JONATHAN COTTON

PARTNER

T: +44 (0)20 7090 4090
E: Jonathan.Cotton@slaughterandmay.com

EWAN BROWN

PARTNER

T: +44 (0)20 7090 4480
E: Ewan.Brown@slaughterandmay.com

ORLA FOX

SENIOR KNOWLEDGE LAWYER

T: +44 (0)20 7090 3814
E: Orla.Fox@slaughterandmay.com

London
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Brussels
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
T +852 2521 0551
F +852 2845 2125

Beijing
T +86 10 5965 0600
F +86 10 5965 0650