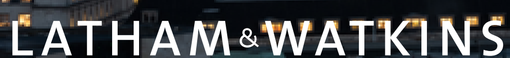
London Litigation Year in Review and 2024 Outlook



Contents

Foreword 3

Data Privacy, Cybersecurity, and AI 5

Competition 11

Shareholder 17

Crypto 24

ESG 30

Banking 38

White Collar Defence and Investigations 44

Latham’s London Litigation & Trial Practice 50

Contributors 51

Martin Davies
Global Vice Chair, Litigation & Trial Department

Welcome to our London Litigation Year in Review and 2024 Outlook. In this report, we examine the litigation trends that shaped the commercial landscape in 2023 and look at how these developments are likely to play out in the year ahead.

In 2023, we noted a general rise in litigation and regulatory risk for businesses. UK regulators, including the Competition and Markets Authority and the Serious Fraud Office, took a more expansive and assertive posture on a range of matters, including competition, white collar, and ESG. Company boards grappled with a steady uptick in shareholder and investor claims. Data privacy and cybersecurity risks, as well as the sudden emergence of powerful AI tools, also loomed large, constituting a C-suite priority for most major companies across industry sectors. Meanwhile, the growing volume and value of crypto disputes in English courts and international arbitral institutions will require businesses active in the crypto space to pay close attention to this evolving area of the law.

None of these trends looks likely to wane in the year ahead, and they overlap significantly, reflecting the multifaceted issues that businesses face. We predict that these trends will combine within cases rather than manifest in a series of separate cases. Indeed, the major cases in the coming years will be defined by the issues that connect and bind these trends, and as multiple trends converge, businesses must approach them holistically rather than individually to tackle future issues strategically and successfully.

In this report, we help companies and boards prepare for the likely future impact of these developments by providing clear context and practical steps to navigate carefully the 2024 litigation landscape.

Data Privacy, Cybersecurity, and AI

LATHAM & WATKINS

By Ian Felstead, James Lloyd, and Sami Qureshi

Data privacy and cybersecurity risks continue to loom large and constitute a C-suite priority for most major companies.

Businesses in all industry sectors are vulnerable and the consequences of a breach cannot be ignored. Meanwhile, the rapid emergence of powerful artificial intelligence technology, while opening up substantial opportunity for growth, brings significant risk of weaponisation by malicious actors.

In this article, we share a few thoughts about how these trends have developed and will continue to play out over the coming year. Further, we explain what boards should do to ensure they discharge their fiduciary duties.

Data Privacy

International data transfers

Data crossing borders dominated the data protection landscape in 2023. In May 2023, the Irish Data Protection Commission (IDPC) ordered Meta Platforms Ireland Ltd. to suspend the transfers of EU/EEA Facebook user data to its processor, Meta Platforms Inc. in the US, and to bring its processing operations into compliance with Chapter V GDPR. The IDPC also issued a €1.2 billion fine,[1] the largest ever under the GDPR.

Just two months later, the European Commission issued an adequacy decision regarding the EU-US Data Privacy Framework (DPF), providing another mechanism for data to flow across the Atlantic. Whether the DPF will survive longer than its predecessor remains to be seen. Indeed, privacy activist Maximilian Schrems has announced that he will challenge the DPF in the EU courts, and French politician Philippe Latombe has already launched another challenge (although the EU General Court has rejected his application for a stay of the adequacy decision).

Children's data

We have also seen continued regulatory focus on the rights of children, as exemplified by the UK Information Commissioner's Office (ICO) "Age Appropriate Design Code".[2] The code sets out standards that online service providers must follow when dealing with the personal data of young people. In September 2023, the IDPC levied a €345 million fine[3] against TikTok Technology Ltd. upon finding that the platform had processed the data of children unlawfully. In particular, the IDPC criticised TikTok for implementing public-by-default settings that allowed anyone, including those not on the platform, to access the content of child users, as well as for failing to comply with transparency obligations in relation to its processing activities in respect of young people's data.

The UK recently enacted the Online Safety Act,[4] which creates new and onerous obligations on companies to protect children from harmful material on their platforms. Enforced by Ofcom, the new act carries the potential for penalties in excess of UK GDPR (with fines potentially reaching as high as 10% of global turnover or £18 million, whichever is greater) and criminal liability for executives complicit in serious failures to comply.

Cybersecurity

Growth in cyberattacks

Early predictions about post-pandemic high risk levels were borne out in the cybersecurity space. According to the UK government's Cyber Security Breaches Survey 2023,[5] approximately 70% of large businesses reportedly experienced a cybersecurity breach or attack in the preceding 12 months. Ransomware attacks have surged over the last year as new threat actor groups emerge, infiltrate, and attack organisations for financial reward, or instead lease or sell their own ransomware variants in a "Ransomware-as-a-Service" (RaaS) model to other criminal enterprises.

Further, the growing risk of supply chain attacks was highlighted by a recent incident in which a "zero-day" vulnerability in file transfer software allowed the ransomware group "Cl0p" to exfiltrate vast amounts of data and extort thousands of organisations around the world.

Growth in regulation

Increasing cyber risk has been met with increasing regulation. In the US, we have seen regulators like the Securities and Exchange Commission clamp down on public companies and require information disclosure within four days of discovering a "material" cybersecurity incident. The US Federal Trade Commission has also imposed executive-level accountability by bringing federal charges against C-suite officers in cases in which the officers were found to have concealed information or obstructed an investigation. It is likely that UK and EU enforcement will take their lead from the US, particularly given the continued success of ransomware groups and the increasing threat that presents to organisations and governments globally.

It is likely that UK and EU enforcement will take their lead from the US, particularly given the continued success of ransomware groups and the increasing threat that presents to organisations and governments globally.

AI: Regulation and Cybersecurity Implications

AI regulation

Lawmakers are rushing to catch up with the rapid emergence and uptake of AI technology, fuelled by the release of OpenAI's ChatGPT. Proposed AI regulation is emerging to address risks that this new technology presents, particularly in the US, the UK, and the EU. In the interim, we have seen the use of existing privacy laws as a blunt instrument for regulating AI. For example, the Italian Data Protection Authority and the ICO have taken action against OpenAI and Snap, respectively. In each case,[6] the regulator focused on allegedly unfair processing and insufficient transparency about how personal data is used in the context of training or deployment of generative AI technologies. Despite the limitations of privacy regulation for the purpose of regulating AI, we expect to see further use of data protection enforcement powers in the coming year, while we await the new legal frameworks that will ultimately govern the creation and use of these emerging technologies.

AI's impact on cybersecurity

Along with technological developments, AI has supercharged the cyber risk landscape, leading to what we expect will be an "AI-powered arms race" with both malicious attackers and company victims looking to the newest technologies for advantage. Large language models and other generative AI technologies enable threat actors to better exploit human vulnerabilities, conducting incredibly

AI has supercharged the cyber risk landscape, leading to what we expect will be an 'AI-powered arms race'.

sophisticated social engineering campaigns by using AI to create more convincing and personalised phishing attempts. In response, top-shelf security firms are leveraging AI to power their detection and response products. These trends are already evident in the US, and a spillover into other jurisdictions is inevitable.

3 Strategies for Boards

Looking ahead to 2024, boards must stay ahead of the curve in cybersecurity and data privacy. Here are some simple measures that boards can take to prepare for the impacts of continued technological change and protect against the risk of attack:

1. Track global regulatory trends

Emerging and novel technologies will continue to draw regulatory focus. As these laws develop and are enforced, businesses will need to be adaptable and may need to reorient themselves according to the unfolding legal landscape. In particular, many businesses that have sourced generative AI products or started to build their own solutions in this space will need to anticipate potential regulatory red lines that could emerge and impact their operational plans.

2. Understand the risks

What are the core risks and threats to the company and how have these evolved? Primarily, this depends on what industry the company is in, the technology it uses, and the data it holds. For example, the average total cost of a data breach to a company in healthcare, financial services, or technology is generally higher than for retail or hospitality companies.

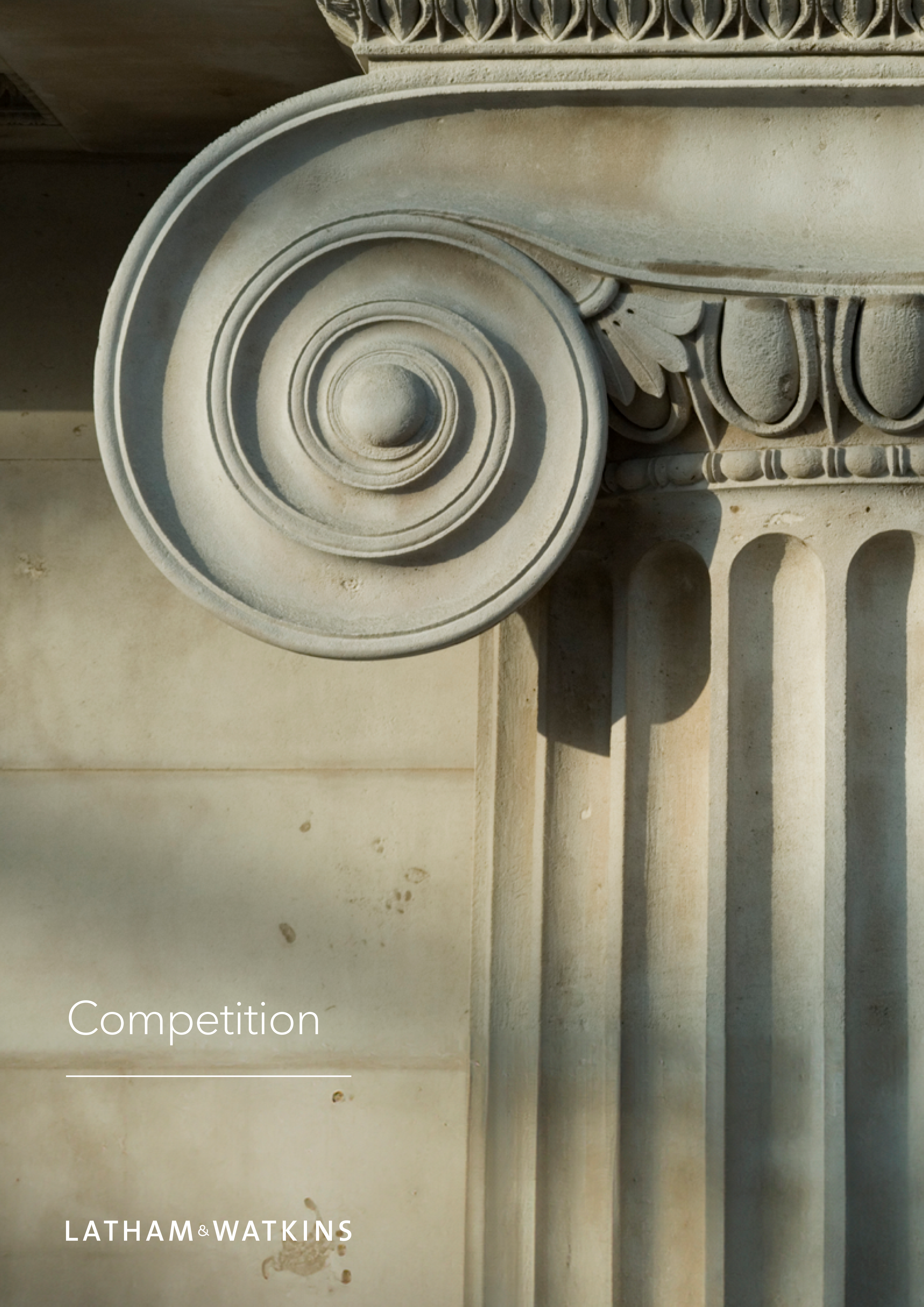
Reputational damage, supply chain disruptions, contractual breach, regulatory action, and runoff litigation can all be mapped out ahead of time, which can enable businesses to better plan to protect themselves from the very worst consequences. New acquisitions can onboard legacy and aging technologies, some of which will carry the risk of security vulnerabilities and substantially raise the risk of intrusion and attack. Thorough diligence, pre- and post-acquisition, can help avoid this risk.

3. Assess, develop, and execute a plan

An honest and critical appraisal of the company's approach to cybersecurity and data protection will identify areas for improvement. Cybersecurity frameworks (e.g., NIS, ISO) outline requirements for certain sectors, and risk assessments are widely offered by cybersecurity vendors and generally required by cyber insurers. The board should be familiar with the company’s key people, processes, and technologies from a cyber perspective, as well as understand how this experience is filtered down to roll out security awareness education and training. The board should discuss the plan regularly at board meetings, record minutes (subject to privilege

rules), and pay careful attention to progress and potential roadblocks. It is important to know who "owns" cyber risk and cyber resiliency, and to dedicate appropriate resource and funding to protect against these potentially business-breaking risks.

1. https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland.
2. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/.
3. https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok.
4. https://www.legislation.gov.uk/ukpga/2023/50/enacted.
5. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023.
6. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/uk-information-commissioner-issues-preliminary-enforcement-notice-against-snap/; https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847.


Competition
LATHAM & WATKINS

By Gregory Bonné, Oliver E. Browne, Ludmilla Le Grand, Anna Kullmann, and Edd Rarity

The CMA has taken a proactive approach to ESG, Big Tech, and PE roll-ups, while the UK government reviews the NSIA and class actions continue to rise.

The Competition and Markets Authority (CMA) has continued to actively enforce across both merger control and behavioural matters. Leaving aside its headline-grabbing review of merger transactions, the CMA has launched several initiatives showing a growing focus on consumer-facing sectors and continues to take an expansive view of its powers and mandate.

ESG, Big Tech, and PE roll-ups are all enforcement priorities for which the CMA has signalled intent and/or introduced initiatives mirroring steps that global regulators have taken in the US and the EU.

Ongoing concerns with the cost-of-living-crisis have led to the launch of market information gathering inquiries, studies, or investigations in consumer-facing segments such as groceries and veterinary services, potentially creating significant burdens for market participants.

An increased focus on consumer market functioning perhaps also reflects a slower M&A pipeline resulting in less of the CMA's resources being tied up in reviewing transactions. That said, the UK remains a complex jurisdiction for dealmakers to navigate from a merger control perspective. Adding to the complexity is the coming into force of the UK National Security Act 2021, which within two years has already been tabled for review after some commentators claimed it has "chilled" UK investment.

> That said, the UK remains a complex jurisdiction for dealmakers to navigate from a merger control perspective.

ESG and Competition Law — New CMA and European Commission Guidance

The CMA and the European Commission, along with other national European competition authorities, have issued guidance on the application of competition law to environmental sustainability agreements. With this guidance, regulators are seeking to tackle climate change and facilitate the transition to a net zero economy. The guidance brings more legal certainty, as it confirms that regulators will take a more permissive approach in relation to collaborations between companies that advance sustainability objectives.

> With this guidance, regulators are seeking to tackle climate change and facilitate the transition to a net zero economy.

The CMA's guidance, which applies only to environment, biodiversity, and climate agreements, is narrower in scope than the EU guidelines, which apply to agreements with a broader social objective. However, the CMA's guidance is more permissive in other senses, as it acknowledges that sustainability agreements benefit the public at large rather than just the parties to the agreement or the relevant consumer pool.

The question remains as to whether US regulators that are currently debating the role of sustainability agreements will follow suit. Protection of the US fossil fuels industry has led to some Republican congressional action against ESG-focused industry associations and their participants in a sign that the debate remains highly politicised on the other side of the Atlantic.

Introduction of the Digital Markets, Competition and Consumers Bill

The Digital Markets, Competition and Consumers Bill (DMCC Bill) is the UK's contribution to the proliferation of regulating Big Tech. It will identify firms with "Strategic Market Status" — i.e., firms that have amassed sufficient market power in the digital sector — as the target of the CMA's expanded review powers. It also introduces revised turnover and share of supply thresholds, which are intended to more readily capture "killer acquisitions" in which a prominent market incumbent acquires a smaller innovative company to eliminate the threat of future competition.

Under the DMCC Bill, the CMA's powers to investigate anti-competitive conduct will include conduct implemented outside the UK that is likely to affect UK trade. Previously, the unlawful agreement or conduct had to be implemented in the UK. Possible fines for breaches of antitrust laws remain at up to 10% of worldwide turnover, however, in the case of failure to comply with CMA information-gathering requests, or failure to provide a complete response, the agency's previously very limited fining powers will substantially increase to up to 1% of global turnover and up to 5% of daily global turnover.

Enhanced Consumer Law Powers and the CMA's Use of Market Studies and Investigations

Under its new CEO, Sarah Cardell, the CMA announced in its 2023 work plan its intention to focus on consumers.

Under the DMCC bill, the CMA will acquire the power to sanction companies that breach consumer laws. Following the conclusion of an investigation, the CMA will have the power to issue infringement notices, impose sanctions, and negotiate consumer compensation. Sanctions for consumer law breaches will include a maximum fine of up to 10% of global annual turnover for companies and up to £300,000 for individuals. Previously, the CMA did not have fining powers and could only take enforcement action by pursuing a case in the High Court.

The CMA has already launched information-gathering inquiries into important consumer-facing markets, such as the veterinary services market, which may ultimately result in a market study or investigation. Following a market investigation, the CMA has significant powers to remedy any features of a market which result in an adverse effect on competition, including through ordering structural divestments.

According to the CMA, its decision to review the veterinary services market was a result of its (i) significance to UK consumers (approximately two-thirds of UK households have a pet, representing an almost 9% increase from 2022), and (ii) heightened concentration within the market as a result of a number of acquisitions by PE houses and other major corporations of small veterinary practices.

Going forward, and under the CMA's new regime, companies can expect a growing number of market studies and investigations, especially in significant consumer markets (such as dentistry and elderly

care) that may have increased in concentration as a result of piecemeal M&A activity.

Focus on PE Roll-Up Strategies

The CMA has turned its attention to enforcement against roll-up acquisitions, which involve financial investors, like PE firms, acquiring multiple (often small) targets within the same sector.

The CMA has wide discretion to review deals. In recent cases, it has applied its "share of supply" test broadly to assert jurisdiction over local transactions that would not meet the £70 million UK turnover test.

Following a market investigation, the CMA has significant powers to remedy any features of a market which result in an adverse effect on competition, including through ordering structural divestments.

Further, the CMA has found competition concerns over completed transactions which occurred in some cases several years ago, resulting in investors having to sell businesses they had acquired some time ago.

While the CMA's primary focus has been on consumer-facing sectors, transactions involving a series of small deals in a short time frame or in sectors that have seen significant consolidation are also likely to face increasing scrutiny. PE firms and their portfolio companies should therefore consider the increased regulatory risk and how those risks can be mitigated.

NSIA — Annual Report and Reflections Two Years On

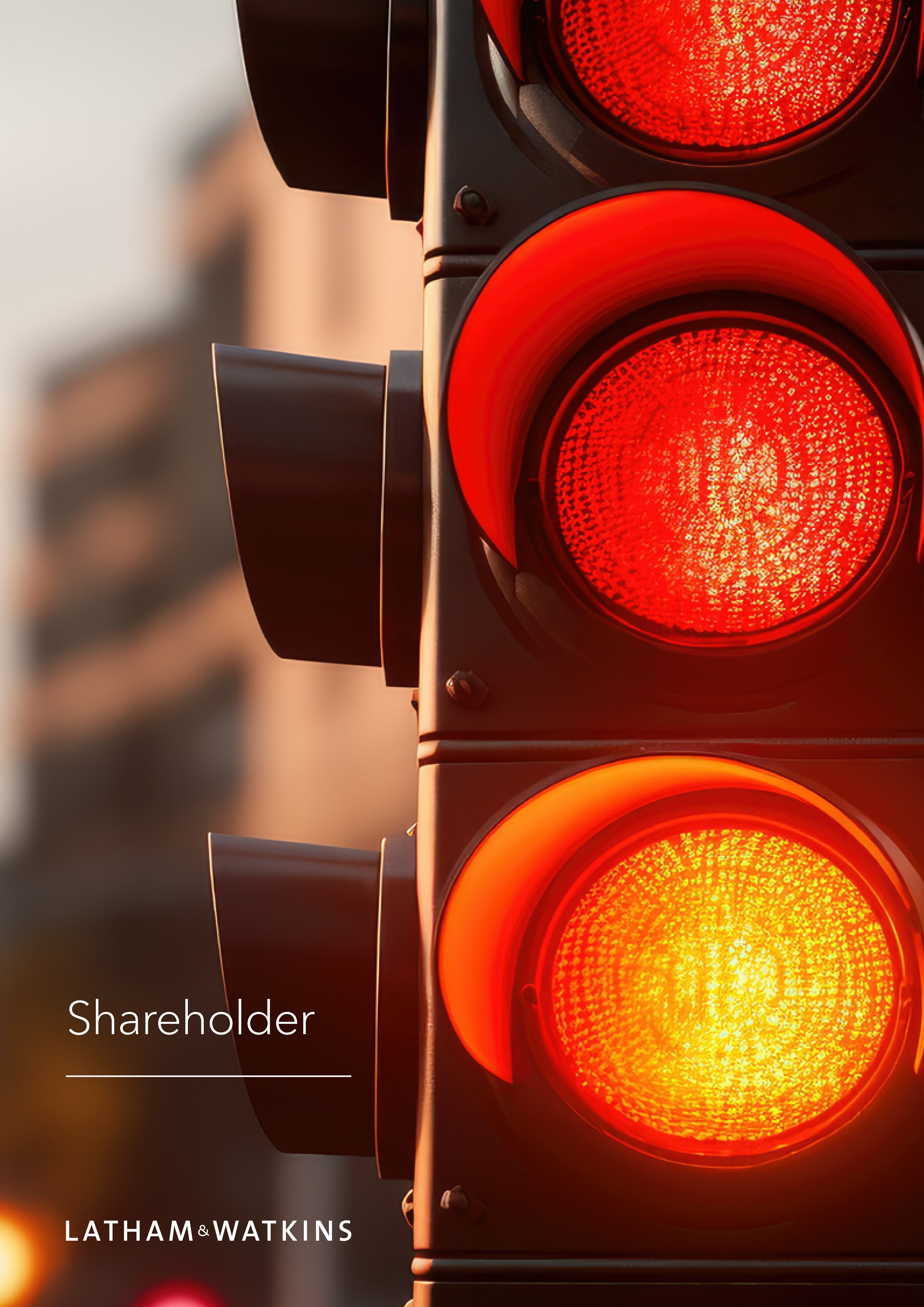
The UK announced a review of the National Security and Investment Act (NSIA) less than two years after it came into force, with the intention of making it "more business friendly". Proposed changes include watering down mandatory notification obligations for internal reorganisations and updates and clarifications to the 17 mandatory sectors.

The review follows the UK government's second annual report on the NSIA. The report notes fewer filings than anticipated but highlights specific areas including defence, critical suppliers, and AI with the most notifications. While most transactions are ultimately cleared without conditions, the government is willing to intervene in transactions outside mandatory thresholds. Though the government is agnostic to acquirer nationality, Chinese investors accounted for less than 5% of notifications but more than 40% of "call-in" notices, with the corresponding figure being 32% for acquirers associated with the UK and 20% with the US.

Continued Increase in Class Actions

The Supreme Court's judgment in *Merricks v. Mastercard*, handed down in December 2020, lowered the threshold for making a collective proceedings order (CPO). This fuelled the perception that the floodgates for collective actions in the UK were open, with more than 30 collective proceedings or CPO applications currently live before the Competition Appeal Tribunal (CAT).

Recent judgments have clarified the CAT's remit, including its role as gatekeeper for collective actions. In *O'Higgins and Evans*, the Court of Appeal confirmed the CAT has discretionary powers to strike out CPO applications of its own volition and certify CPOs on an opt-in basis, even when the class action was brought on an opt-out basis. The Court of Appeal confirmed that it also has the power to amend the terms of a CPO. In 2023, five applications for CPOs were refused (although the applicants were invited to reformulate their claims) — see *Gormsen v. Meta* and *CICC I to IV.*


Shareholder
LATHAM & WATKINS

By Oliver Middleton and Duncan Graves

Companies should carefully consider the possibility of securities claims, engage with activists, and respond to shareholder concerns to mitigate litigation risks.

Shareholder and investor claims against companies undoubtedly rose this year, with material court decisions issued around how such claims can proceed through the English courts.

Causative factors include the macroeconomic environment, the availability of a wide range of litigation funding, and growing investor interest in having an active say in corporate governance. Two growth areas with parallels to more established jurisdictions in the US are "securities" claims arising from drops in share prices under the Financial Services and Markets Act 2000

(FSMA), and litigation brought by or relating to activist shareholders.

Causative factors include the macroeconomic environment, the availability of a wide range of litigation funding, and growing investor interest in having an active say in corporate governance.

Sections 90 and 90A FSMA

Background

Sections 90 and 90A FSMA provide remedies to investors who have an "interest in securities" in listed companies and have suffered loss because of misleading statements or omissions in public disclosures. Although the legislation is not new, proceedings under these statutory provisions have substantially risen in recent years, and almost all of these claims are funded class actions brought by large groups of institutional investors. Only one claim has reached trial to date, which was a Section 90A claim by a single shareholder that had purchased a listed company which it then claimed successfully had knowingly withheld financial information. Several interim decisions have clarified aspects of the relevant tests, and two class action claims are scheduled for trial in 2024.

Section 90 FSMA

Section 90 FSMA covers claims for loss caused by misleading statements or omissions in listing particulars or prospectuses. It is a defence for the issuer company to show that it reasonably believed that the statement was true or that the matter was properly omitted.

Section 90A FSMA

Section 90A FSMA covers claims for loss caused by misleading statements or omissions in published information, including annual reports. It imposes a higher threshold for claimants, including that they must show a person discharging managerial responsibility knew that the statement was untrue or the omission concealed a material fact, and that each claimant read and relied upon the published information when making a decision on whether to buy, hold, or sell shares, and the decision caused the loss.

Trends

Claims often arise out of regulatory settlements, whether in the UK, the US, or elsewhere, or out of company reports of historic issues in which the issue is alleged to have been omitted from prior published information. The loss claimed usually arises from immediate drops in the company's share price as the market initially considers the news.

Litigation funders have been more willing to pursue these claims, often persuading institutional investors to commit to claims on the basis of impending limitation deadlines.

Funders, and in some instances solicitors and counsel, will usually take a share of any return from the litigation, although the economic terms of these agreements are more prescribed following the recent decision of the UK Supreme Court regarding damages-based agreements.

How these claims are case-managed has been the subject of several decisions this year as a number of these claims are currently being pursued in the English High Court. Multiple decisions relate to whether issues should be bifurcated for trial, how much work the claimants should put in the initial stages, decisions on the standing of claimants and title to sue issues (as well as the right to amend claimant names after the limitation period has expired), and all manner of decisions relating to how these cases are pleaded.

Two recent claims were brought using the "Representative Claimant" procedure under the Civil Procedure Rules, in part due to the hurdles that funders and lawyers face in building a book of claimants and demonstrating that claimants meet the requisite statutory criteria. This approach was rejected by the court in a recent judgment following strike out applications by the respective defendants, but the decision was fact-specific and other claims may attempt to take a similar approach. Depending on the success of this approach, we could see many more of these claims being pursued (not least as they will be much more easily financially viable for litigation funders to pursue and claimant law firms will be queuing up).

Takeaways

Companies listed in the UK should consider carefully the possibility of claims against them arising from disclosures and adverse regulatory findings, and take proactive steps to mitigate litigation risk and capture institutional knowledge immediately after such events.

Activist Shareholders

Background

Shareholder activism remains prominent in the UK, accounting for 44% of all campaigns in Europe. The term "activist shareholder" covers a broad range of investors that can be grouped into two main categories: (i) those who are principally investors, and activism is a means to an end, such as private equity investors, institutional investors, and activist hedge funds; and (ii) those who are principally campaigners, and so acquire shareholder status to advance their campaign, such as charities and NGOs.

Conflict and Litigation Risk

The UK is a target destination for activists because of its strong disclosure and transparency requirements, along with a supportive legal framework for shareholders. Once an activist acquires shareholder status, it is immediately equipped with various legal rights and can ensure its voice is heard, regardless of the size of its stake in the company. For example, a shareholder may requisition a general meeting to consider resolutions or use its power to circulate members' statements. It could also threaten legal action through a derivative or unfair prejudice claim if it feels the company has committed some wrongdoing.

In conjunction with exercising their legal rights, activist shareholders may employ non-legal strategies of engagement. They may consult boards privately to express their concerns or, if those concerns are not addressed, mount public campaigns to demand change.

> In conjunction with exercising their legal rights, activist shareholders may employ non-legal strategies of engagement.

Trends

Environmental and Climate Change Activists

ESG factors are now at the forefront of corporate decision-making. Significant governance developments in the UK, such as new regulations requiring disclosure of climate-related financial information and reporting on how stakeholder interests have been considered, encourage companies to embrace sustainable and responsible practices.

These developments result in a more informed and empowered shareholder base within companies. The enhanced transparency allows activist shareholders to take more proactive steps on environmental issues, and the usual forum to make these proposals is via the AGM. Traditional institutional investors will also latch on to ESG themes if they think the proposals are reasonable. As a result, ESG activist organisations have had directors appointed to the boards of major energy and commodities companies in the last two years, and motions for increased disclosures on work towards climate targets have gained support from a substantial minority of investors.

In contrast, ClientEarth, holding only 27 shares in Shell, brought a derivative claim against the company in 2022 for its failure to adopt and implement an energy transition strategy in line with the 2015 Paris Agreement. ClientEarth argued that this violated Shell's directors' duties to promote the company's success and to act with care, skill, and diligence. The claim gained support only from members holding 0.17% of Shell's shares and was dismissed by the High Court in strong terms. Equivalent actions would also likely fail, but such litigation can nonetheless expose the target company to significant potential legal liability and reputational damage.

> ESG activist organisations have had directors appointed to the boards of major energy and commodities companies in the last two years, and motions for increased disclosures on work towards climate targets have gained support from a substantial minority of investors.

Governance and Value Creation Activists

Activist investors seek to release shareholder value and often focus on M&A activity to provide opportunities to do so, with 57% of campaigns in the first quarter of 2023 having an M&A-related goal. For example, activist shareholders may call for the company to renegotiate a deal or dispose of a non-core part of its business.

Shareholders may take issue with how the business is being run and raise concerns over the company's financials, capital allocation, or remuneration policy. The activist shareholder may then garner support from other shareholders to appoint or remove directors, which is perceived as evidence of campaign "success". When activist investors are perceived as achieving improvements in corporate governance, fellow shareholders are more likely to welcome their presence.

Takeaways

Management should acknowledge activists as playing an important role, take time to listen to their recommendations, and line up external advisers to respond appropriately.

There is a need to strike a balance: anticipating and attending to activist strategies can draw attention away from the day-to-day running of the company. However, if management does not engage proactively with reasonable requests from shareholders, the activist's viewpoint may resonate with shareholders and make the company more susceptible to challenge, including through the courts for breaches of directors' duties or derivative actions.

This article was prepared with the assistance of Emma Bunting in the London office of Latham & Watkins.

1. *ACL Netherlands BV and others v. Michael Lynch and another* [2022] EWHC 1178 (Ch).
2. *R (PACCAR Inc and others) v. Competition Appeal Tribunal and others* [2023] UKSC 28.
3. *Client Earth v. Shell Plc and others* [2023] EWHC 1897 (Ch); permission to appeal to the Court of Appeal was refused.

Crypto

LATHAM & WATKINS

By Samuel Pape, Nell Perks, and Matthew Unsworth

New crypto regulation on the horizon, and the extension of the UK financial promotions regime to cryptoassets, could lead to more regulatory disputes.

The English courts and international arbitral institutions have observed a steady uptick in crypto disputes (especially fraud claims) as investment in cryptocurrencies has become more widespread.[1] The value of these disputes is on the rise, and they increasingly involve sophisticated commercial entities such as crypto exchanges and lenders, not just individuals.[2] Familiar substantive and procedural points of law have had to be applied to a novel digital context, with judges asked to determine, for example, whether Bitcoin constitutes

personal property (yes),[3] whether it can be provided as security for costs (no),[4] and whether individuals engaging in the trading of cryptoassets may qualify as consumers under consumer protection legislation (yes).[5]

Below, we discuss some hot topics in crypto litigation and arbitration as well as our predictions for 2024.

Hot Topics in 2023

Service permitted via NFT alone[6]

Traditional methods of service are likely to be unavailable in crypto fraud claims, in which the defendant's identity (e.g., postal / email address) is often unknown, and courts have therefore shown a willingness to permit proceedings to be served by unconventional means. Most recently, a claimant was allowed to serve proceedings solely by uploading a non-fungible token (NFT) to a cryptoasset wallet that she believed to be held by the defendant (with hyperlinks to the claim form, particulars of claim, and supporting documents).

Developers may owe fiduciary duties to crypto holders[7]

In February 2023, the UK Court of Appeal dismissed an application to set aside service out of the jurisdiction, holding that there was a serious issue to be tried as to whether Bitcoin software developers owed fiduciary duties to Bitcoin holders. In the leading judgment, Lord Justice Birss accepted that developers could conceivably owe a negative fiduciary duty not to introduce a feature to their own advantage that compromised holders' security. The claimant had also presented a realistic argument that developers owed positive duties, e.g., to fix software bugs or transfer stolen Bitcoin back to its rightful owner — although this would involve "a significant development of the common law on fiduciary duties".

Successful challenge to injunction against crypto exchange[8]

The UK High Court (for the first time) discharged an injunction requiring a crypto exchange to preserve cryptocurrency alleged to have been obtained by fraud. Given that crypto deposits were pooled by the exchange (with each customer receiving credit in lieu), the High Court found that it would have been a "futile… and possibly impossible exercise" to isolate and preserve the claimant's sum of cryptocurrency. The injunction therefore served no useful purpose and a bona fide purchaser defence was likely available to the exchange (a point the claimant had omitted to explain at an earlier "without notice" hearing).

A new crypto tort?

As part of its Final Report on "digital assets", the Law Commission concluded that the existing law on causes of action and associated remedies can adequately address disputes that are likely to arise in the crypto sphere. However, it also warned of a possible gap in the law in relation to wrongful interferences with digital assets, such as when a crypto token is "burned" (removed from circulation) without the holder's consent. To plug this gap, it recommended that the common law develop "specific and discrete principles of tortious liability by analogy with… the tort of conversion".

Arbitration

Arbitration remains a popular means of settling crypto and other digital asset-related disputes. This is particularly so for crypto exchanges and lenders, which can benefit from the procedural flexibility, confidentiality, and broad international enforceability of arbitration awards. Recent developments serve as a timely reminder to closely review the terms of arbitration agreements and the procedural rules they incorporate, particularly with respect to the possibility of class arbitration in the US and suitability of arbitration as a dispute resolution mechanism with consumers in the UK and the EU.

Arbitration remains a popular means of settling crypto and other digital asset-related disputes.

Class arbitrations in the crypto space are on the rise

Parties must be mindful of the possibility of class arbitrations, particularly in the US. Many claimants have sought to pursue class arbitrations against crypto exchanges and lenders in the past two years and a number of cases remain on foot. Both parties must expressly consent to class arbitration; however, arbitration agreements typically incorporate a host of procedural rules through the choice of a supervising arbitral institution. Such rules can be extensive, complex, and subject to change, and they can vary widely on the issue of class arbitrations. For example, the American Arbitration Association's consumer arbitration rules allow for individual claims to be heard in batches of up to 100. On the basis of such rules, 96 claimants brought a consolidated arbitration demand in October 2022 against a crypto exchange over an alleged "wallet-draining" scam. In contrast, many other arbitral institutions do not permit class arbitrations, and parties must carefully consider the issue when deciding which arbitration to select in any terms of service.

Disputes with individuals in the UK and the EU may not be arbitrable under mandatory consumer protection legislation

Parties must carefully draft arbitration agreements that may apply to individuals qualifying as consumers, particularly in the EU and the UK. Courts in those jurisdictions may refuse to enforce arbitral awards that are contrary to mandatory consumer protection law. Indeed, for this reason, an English court took the rare step of refusing to enforce a foreign award related to a crypto dispute in July 2023. A crypto exchange had won an arbitral award of damages against one of its customers, a lawyer based in the UK. Pursuant to the exchange's terms of service, the arbitration was overseen by JAMS, the California-based arbitral institution, and subject to California law. The English court refused to enforce the award because it considered the English lawyer to be a consumer under the UK Consumer Rights Act (CRA). Through the lens of the CRA, the court found that the contract's requirement that disputes be resolved through arbitration in California was an "unfair term" and was therefore not binding

on the consumer. The case serves as a reminder that in order to ensure enforceability of awards, adaptations need to be made for clients in the UK and the EU or appropriate carveouts for them included.

The case serves as a reminder that in order to ensure enforceability of awards, adaptations need to be made for clients in the UK and the EU or appropriate carveouts for them included.

Looking Ahead

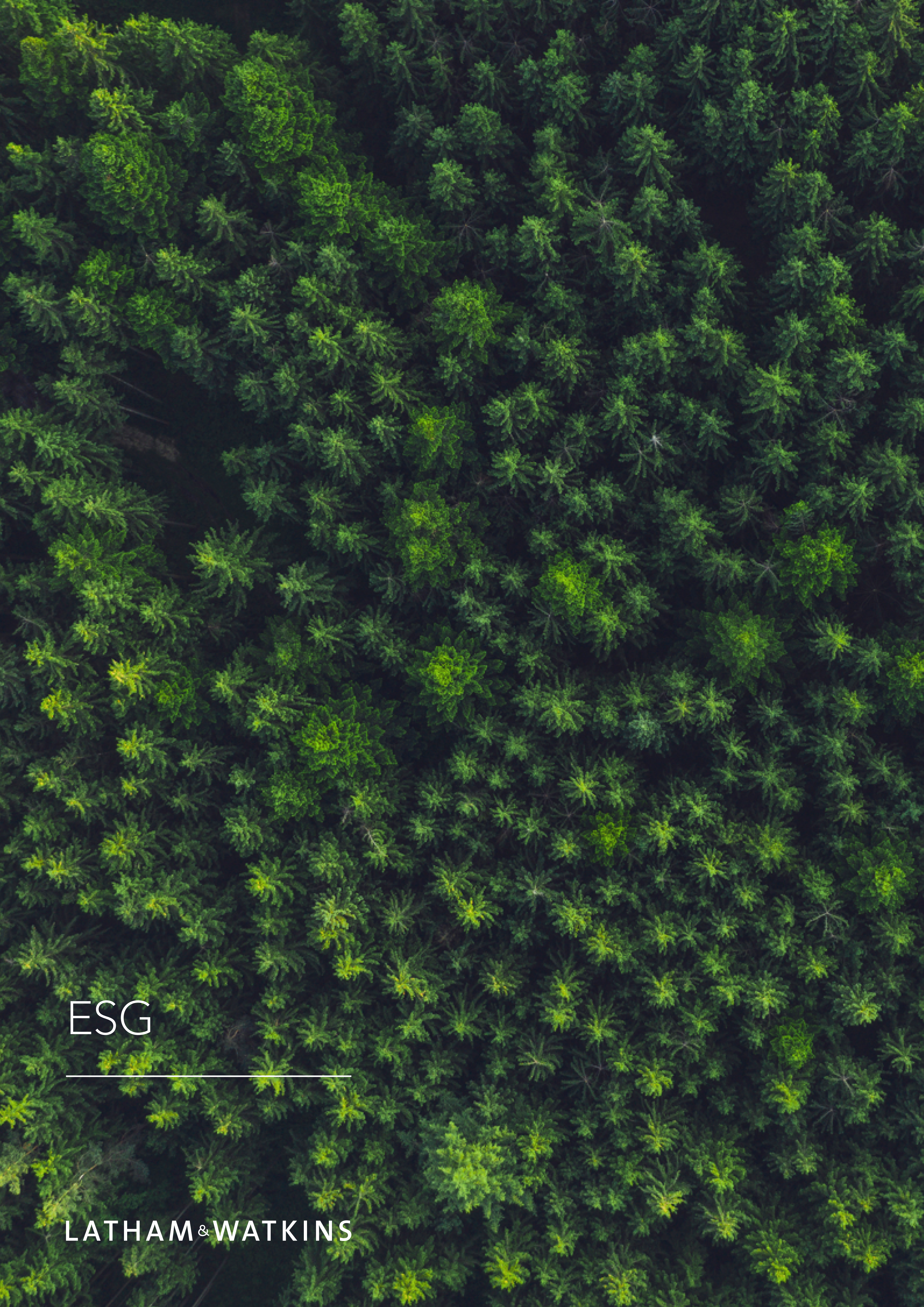
Cryptoasset promotions

On 8 October 2023, the financial promotions regime was extended to cryptoassets. Since then, all cryptoasset promotions made by non-authorised persons have required approval under Section 21 FSMA from an authorised person, unless they are exempt or the promoter is registered as a cryptoasset business under the MLRS[9] and 143 market participants were added to the FCA's "warning list" overnight for non-compliance. We expect this change will lead to regulatory proceedings involving the FCA but also potentially commercial disputes between crypto exchanges and their newly engaged Section 21 approvers.

Further crypto regulation in the pipeline

The UK government announced plans at the end of October 2023 to regulate cryptoassets in the same way as other investments, including requiring crypto firms to be FCA-authorised. We anticipate a fertile ground for regulatory disputes as participants in the crypto industry get to grips with these new rules.

1. https://www.judiciary.uk/speech-by-judge-mark-pelling-qc-issues-in-crypto-currency-fraud-claims/.
2. https://www.judiciary.uk/speech-by-hhj-pelling-issues-in-crypto-currency-fraud-claims-an-update/.
3. *Example: AA v. Persons Unknown* [2019] EWHC 3556 (Comm).
4. *Tulip Trading Limited v. Bitcoin Association for BSV* [2022] EWHC 141 (Ch).
5. *Payward, Inc.; Payward Ventures, Inc. and Payward Limited v. Maxim Chechetkin* [2023] EWHC 1780 (Comm).
6. *Osbourne v. Persons Unknown Category A* [2023] EWHC 39 (KB).
7. *Tulip Trading Limited (a Seychelles company) v. Bitcoin Association for BSV* [2023] EWCA Civ 83.
8. *Piroozzadeh v. Persons Unknown* [2023] EWHC 1024 (Ch).
9. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.


ESG
LATHAM & WATKINS

By Sophie J. Lamb KC and
Aleksandra Dulska

How current and future ESG litigation has, and likely will, impact crowdfunding and liability for costs in the ESG litigation space.

There was a continued rise throughout 2023 in large-scale cases brought against government climate policies and against corporate actors focusing on ESG issues arising from their operations. These claims were spearheaded by a number of actors, most notably non-governmental organisations (NGOs), consumers, and regulators.

The complex web of ESG best practice guidelines and binding regulations in areas such as sustainable reporting, consumer protection, supply chain due diligence, and sustainable finance increase contentious risk for UK and EU companies. Indeed, high-profile cases are already being brought in front

of the domestic courts, as well as the European Court of Human Rights, including *Duarte Agostinho and Others v. Portugal.*[1]

These disputes invite discussions around a company's business purpose, reputation, corporate values, approach to risk management, and relationships with investors, suppliers, customers, employees, and other stakeholders.

There was a continued rise throughout 2023 in large-scale cases brought against government climate policies and against corporate actors focusing on ESG issues arising from their operations.

The following list highlights the top seven forms that ESG litigation has taken to date and focuses on trends we expect will continue to develop. Some of the patterns further elaborated on below include:

- Rising number of cases brought against both private and state actors
- Progressively complex regulatory environment impacting multinational companies
- Growing regulatory and enforcement focus on greenwashing
- Increasing ESG claims funding
- Ongoing policing of commitments under the Paris Agreement by NGOs

1. Government ESG Litigation

Challenges to states' climate policies have historically formed a majority of ESG litigation cases and continue to be filed at pace, despite their varied success. To date, more than 70 challenges have been launched globally, driven by a diverse range of plaintiffs, including NGOs, municipal governments, and trade associations. These challenges to government climate policy or operations are usually based on well-known legal principles, including tort law, human rights and constitutional law, and international law.[2]

In the UK, one of the more recent challenges was aimed at the carbon budget set by the government to limit emissions in line with the Paris Agreement. In the July 2022 High Court of England and Wales case *R. (on the application of Friends of the Earth Ltd) v. Secretary of State for Business, Energy and Industrial Strategy,* the budget setting out the UK's net zero strategy was found to lack detail under the Climate Change Act 2008.[3] The court ordered the Secretary of State to prepare a revised budget, which was published in March 2023 and is now facing another challenge from the NGOs.

One criticism is that there is no legally sufficient basis for the government to conclude that the proposals and policies will enable the carbon budgets to be met. The cases, which are expected to be heard by the High Court in February 2024,

illustrate clearly that the NGOs are closely monitoring the government's commitment to its net zero policies.

More clarity on the scope of a government's international obligations with respect to climate change is needed and may be provided in the foreseeable future. Notably, this includes questions around the legal consequences for the states when they, by their acts and omissions, have caused significant harm to the climate system and other parts of the environment with respect to other states and individuals, including both present and future generations. The International Court of Justice is due to deliver an opinion on states' obligations under international law with respect to climate change, and several cases that address the human rights impacts of climate change are pending before the European Court of Human Rights.

2. Infrastructure ESG Litigation

A second category of ESG litigation relates to the various challenges to government approval of, or financial support for, significant infrastructure projects, most often on a basis that a decision-maker has acted outside its authority.

This type of challenge has increased in recent years, with cases concerning large-scale projects from claimants all around the world, including Mexico,[4] South Africa,[5] Argentina,[6] and Norway,[7] and particularly fossil fuels projects.

These cases have had limited success to date. Indeed, English courts in particular have found that the government has broad discretion when deciding on such matters, and courts should be cautious of second-guessing the executive's decision-making.[8]

However, claimants have succeeded when there is clear evidence that a government has overstepped its authority, including in *EarthLife Africa Johannesburg v. Minister of Environmental Affairs.*[9]

Based on the outcome of these cases, companies should be live to how their projects (especially in the greenhouse gases (GHG) intensive industries) fit within the nationwide net zero targets and be prepared for their environmental assessments to face detailed scrutiny rather than a "tick-box exercise". The NGOs are keen to challenge governmental permits as a tool to raise the profile of climate change issues and engage the public opinion, which increases the contentious and reputational risks involved in large-scale energy projects.

3. ESG Litigation Relating to Company Operations

The third area of growth is ESG claims from various NGOs against private companies in a wide range of sectors, including transport, food and agriculture, energy, and finance. Claimants are challenging companies for the conduct of their subsidiary or supply chain,[10] their internal policies,[11] failure to reduce GHG emissions,[12] or environmental harm.[13]

One high-profile example is the challenge brought against Shell in the Dutch courts, where claimants successfully argued that the company had a duty of

care and due diligence obligations under Dutch tort law to take action to reduce its GHG emissions.[14] The first instance court in The Hague ordered Shell to reduce its net carbon dioxide emissions by 45% by 2030. The legal basis for this type of claim will vary depending on jurisdiction, but it has included tort law, consumer protection law, and company law, as well as human rights law and corporate due diligence standards.

In parallel, some jurisdictions such as the EU are introducing stricter rules in order to regulate international business conduct, which in turn will only increase the scrutiny of companies' operations going forward.

4. ESG Litigation Relating to Corporate Governance and Directors' Duties

Corporate directors in various jurisdictions owe certain legal duties and responsibilities, and claimants are increasingly targeting directors for allegedly failing to exercise these duties when considering ESG issues. In the UK, two claims of this nature have recently been unsuccessful, signalling that directors have broad discretion to manage a company, including taking decisions on its climate change objectives.[15]

5. ESG Litigation Relating to Corporate Disclosures

Regulators around the world are introducing broader disclosure requirements that will have significant impact on the companies that will have to implement due diligence programmes for their entire value chains. In parallel, regulators are also turning their focus to ESG-related enforcement in connection with corporate disclosures, especially in the US.[16] Similar claims have not yet been brought in the UK, but claimants have targeted regulators for failing to properly assess disclosures.[17]

A number of regulatory developments are expected in 2024, which will contribute to the rising enforcement trend. At an EU level, consultations are ongoing regarding improvement of the Sustainable Finance Disclosure Regulation, whilst the Corporate Sustainability Reporting Directive significantly expanded the non-financial reporting requirements to apply to a wider range of companies. Meanwhile, in the UK, the FCA is due to publish the final rules and policy statement for its Sustainability Disclosure Requirements regime.

On the international level, in September 2023, the Taskforce on Nature-related Financial Disclosures published a reporting framework establishing a voluntary method to identify, assess, and report on material nature-related risks and opportunities. We are waiting to see whether and how this will translate into binding obligations on the state level. Moreover, the first two IFRS Sustainability Disclosure Standards issued by the International Sustainability Standards Board will become effective for annual reporting periods starting from 1 January 2024.

6. Marketing ESG Litigation

Litigation in the marketing space has historically targeted industries with reputations as heavy polluters, but as more companies have sought to distinguish themselves using green credentials, the

A number of regulatory developments are expected in 2024, which will contribute to the rising enforcement trend. NGOs are increasingly keen to bring test cases and induce public debate around some of the most hotly debated ESG issues facing the world today.

so-called greenwashing claims have proliferated across various industries, including banks, sports organisations, airlines, and fashion brands.

Regulators around the globe are very active in the greenwashing space, and we have seen an increase in enforcement actions, forcing companies to rethink their marketing strategies.

In the UK, two regulators are particularly alert to greenwashing. The last couple of months saw a number of important Advertising Standards Authority (ASA) rulings in sectors including finance, aviation, and oil and gas, in which the ASA found breaches of its codes on the grounds that the various adverts exaggerated the business's overall environmental credentials compared to its overall environmental impact. On the other hand, in September 2021, the CMA published the Green Claims Code and has launched investigations into major fashion brands and the fast-moving consumer goods sector.

In the EU, the focus has also been on protecting consumers from misleading advertising. In March 2023, the European Commission published the first draft of a directive on green claims outlining the initial set of detailed EU rules on the substantiation of voluntary green claims made in the context of business-to-consumer commercial practices.

Companies should be mindful of any divergence between their marketing efforts and what is achievable, what can be proved, and what is done in practice. Moreover, one of the key challenges facing companies will be adapting their internal procedures to the ever-evolving expectations of regulators worldwide.

7. Soft Law and Other Mechanisms

An increasing number of ESG disputes are being brought before soft law forums such as National Contact Points (NCPs), established under the Organisation for Economic Cooperation and Development (OECD), or mechanisms under the UN Guiding Principles on Business and Human Rights.

By way of an example of the role of a soft law forum and the corresponding reputational risk that may materialise, BP had to withdraw its ad

campaign after ClientEarth publicly filed a complaint concerning the marketing of BP's low-carbon energy activities.[18] ClientEarth claimed that the campaign misled the public, most notably in how it presented BP's low-carbon energy activities ccompared to the scale of its fossil fuel extraction activities.

We expect soft law forums to become an even more commonly used tool, given they are more affordable and lack the usual legal obstacles that may prevent bringing a court claim.

Conclusion

In the past, ESG litigation largely focused on the failings of the government climate policy or claims for damages following catastrophic environmental events. However, that is no longer the case. Indeed, there has been an increase in cases brought against corporate actors focusing on a wide range of issues, including sustainability disclosures, board decision-making, operations across entire value chains, marketing efforts, and infrastructure projects.

The days in which companies could brush these issues aside are long gone; instead they must look at their business holistically and be aware of a number of contentious risks on a global scale.

Future cases likely will elaborate on well-established principles of contract and tort law and raise interesting questions about crowdfunding and liability for costs in the ESG litigation space. As demonstrated above, NGOs are increasingly keen to bring test cases and induce public debate around some of the most hotly debated ESG issues facing the world today. Given how much is at stake, we expect this to be a significant area of expansion occupying courts and soft law forums all around the world.

1. *Duarte Agostinho and Others v. Portugal and Other States* (no. 39371/20), *Union of Swiss Senior Women for Climate Protection v. Swiss Federal Council and Others* (no. 53600/20) *and Carême v. France* (no. 7189/21).
2. *VZW Klimaatsaak v. Kingdom of Belgium, et al.* 2015/4585/A *(Brussels Court of First Instance) and Urgenda Foundation v. State of the Netherlands* ECLI:NL:HR:2019:2007.
3. *R. (on the application of Friends of the Earth Ltd) v. Secretary of State for Business, Energy and Industrial Strategy* [2022] EWHC 1841 (Admin).
4. *CEMDA v. Comisión Reguladora de Energía Amparo* 232/2021.
5. *Africa Climate Alliance et. al., v. Minister of Mineral Resources & Energy et. al. 2021* Case No. 56907/21
6. *Fundación Greenpeace Argentina y Ots. v. Estado Nacional y Ots* 2022 FMP 105/202.
7. *Greenpeace Nordic and others v. Norway* HR-2020-2472-P.
8. *R (on the application of Friends of the Earth Ltd and others) v. Heathrow Airport Ltd* [2020] UKSC; *R (Friends of the Earth Ltd) v. Secretary of State for International Trade/Export Credits Guarantee Department (UK Export Finance)* 2023 EWHC Civ 14.
9. *EarthLife Africa Johannesburg v. Minister of Environmental Affairs and Others* (case no. 21559/2018); *Friends of Buckingham v. State Air Pollution Control Board* 947 F.3d 68 (4th Cir. 2020).
10. *Vedanta v. Lungowe & Ors* [2019] UKSC 20 ; *Okpabi and others v. Royal Dutch Shell Plc and another* [2021] UKSC 3; *Municipo de Mariana v. BHP Group (UK) Ltd and BHP Group LTD* [2022] EWCA Civ 951; *Nevsun Resources Ltd v. Araya and others* [2020] 1 S.C.R. 166.
11. *National Center for Public Policy Research v. Schultz* No. 22-cv-00267 (E.D. Wash. 2022).
12. *Milieudefensie v. Royal Dutch Shell plc.* ECLI:NL:RBDHA:2021:5339.
13. *Illinois v. 3M Co.,* No. 2023L000996 (Ill. Cir. Ct. 2023).
14. *Milieudefensie v. Royal Dutch Shell plc.* ECLI:NL:RBDHA:2021:5339.
15. *McGaughey v. Universities Superannuation Scheme Limited and others* [2023] EWCA Civ 873; *Client Earth v. Shell plc and others* [2023] EWHC 1137 (Ch).
16. *Sec. & Exch. Commission v. Vale S.A., No. 22-cv-2405* (E.D.N.Y 2022); Activision Blizzard, Inc., Exchange Act Release No. 34-96796.
17. Client Earth challenge to Financial Conduct Authority's assessment of Ithaca Energy plc IPO prospectus.
18. *ClientEarth v. BP* (UK NCP, 2020).

Banking

LATHAM & WATKINS

By Andrea Monks, Nell Perks, and Alex Cox

How key cases of 2023 will inform the 2024 outlook, including the Quincecare duty, shareholder and bondholder claims, sanctions, and crypto.

Quincecare Duty

What happened?

In July 2023, the UK Supreme Court handed down its landmark judgment in *Philipp v. Barclays Bank UK plc*, which confirmed that when a customer gives a valid payment instruction, the bank's only duty is simply to execute that order. The Supreme Court declined to extend the scope of the Quincecare duty, holding that a bank's duty to refuse to comply with a payment instruction is limited to instructions given by a customer's agent if the bank has reasonable grounds to believe the instruction is an attempt to defraud the customer.

Outlook

More broadly, the Supreme Court confirmed that the Quincecare duty continues to form part of a bank's general duty of skill and care, and the duty may arise whenever payment instructions are given by one person as agent for another. The Supreme Court gave the examples of situations involving joint bank accounts and cases in which a bank is on notice that a customer lacks mental capacity to manage their financial affairs. The question remains whether these kinds of scenarios will give rise to Quincecare claims in future.

Tackling authorised push payment (APP) fraud (and financial crime more generally) continues to be a priority for the Financial Conduct Authority (FCA), which found in a recently published review that many firms' systems for detection and prevention of fraud are insufficient to ensure that they are delivering good consumer outcomes under the Consumer Duty.

Group Shareholder Actions

What happened?

Claims under Sections 90 and 90A of the Financial Services and Markets Act 2000 continue to be a major source of risk for corporates, including financial institutions. These provisions enable shareholders to seek damages from companies that publish misleading information to the market. So far, only one of these cases has reached trial: the well-known litigation arising out of Hewlett-Packard's acquisition of Autonomy. Following a lengthy liability judgment handed down in May 2022, the UK High Court has given directions for the parties in *Autonomy* to submit additional evidence on the complex quantum questions that have arisen.

More generally, last year featured various hearings and judgments dealing with the proper case management of Sections 90 and 90A claims, which tend to be complex, multi-party, and high-value proceedings. Most recently, the High Court struck out the first attempt by a claimant to bring a claim under Sections 90 and 90A as a representative action under CPR 19.8. In doing so, the court reaffirmed the importance of active case management of these claims and held that its ability to manage such cases should not be curtailed by the bifurcated approach to proceedings that a representative action would involve.

Outlook

In 2024, the first trial in the litigation brought by various investors against Serco is due to take place. This will be the first multi-claimant Section 90A claim to reach trial, and will provide important clarity on how the statutory liability regime works in large, multi-party cases.

Also expected for 2024 is a decision on quantum in the *Autonomy* litigation, which would be the first judgment on quantum in any Sections 90 and 90A litigation.

Finally, we may see various side disputes arising from the Supreme Court's decision in *Paccar Inc v. Road Haulage Association Ltd,* which found that litigation funding agreements providing for a funder to be paid a share of damages are unenforceable damages-based agreements. Since the great majority of multi-claimant Sections 90 / 90A cases are funded, and the general assumption is that *Paccar* will affect the majority of litigation funding agreements currently in place, there is a good chance of satellite litigation arising from funding agreements being rendered unenforceable.

The government has indicated that it is looking at a legislative solution to clarify the law in relation to litigation funding agreements, but has yet to reach a decision on the wording and scope of the relevant legislation.

Sanctions

What happened?

During 2023, sanctions-related disputes between banks and Russian counterparties proliferated. In Russia, the courts are increasingly using their powers to override jurisdiction clauses (including arbitration agreements) in cases allegedly affected by sanctions and imposing wide-ranging orders injuncting parties from commencing or continuing proceedings outside of Russia.

In England, banks that have withheld payments from Russian counterparties on the basis of sanctions are facing challenges to the validity of this approach. For example, EuroChem has brought claims in the High Court against Société Générale and ING, challenging their refusal to make payment under various performance and advance payment guarantees.

These proceedings raise important questions about whether and how sanctions affect the enforcement of such bonds, the interpretation of industry-standard provisions such as the Uniform Rules for Demand Guarantees, and also the scope of the illegality defence under English law (particularly in situations in which the illegality in question arises under foreign laws).

Otherwise, dicta in the Court of Appeal's recent judgment in *Mints v. PJSC National Bank Trust* appeared to give a potentially very broad scope to the UK sanctions regime. The regime provides that a party may be subject to the sanctions regime if it is "owned or controlled" by a sanctioned person.

The Court of Appeal held (albeit obiter) that "control" is not limited to situations in which a person has an economic or ownership interest in a company and that, because Vladimir Putin is the "apex" of a command economy, the consequence may well be that every company in Russia is "controlled" by Mr Putin and therefore caught by UK sanctions.

Subsequent statements by the Office of Financial Sanctions Implementation (OFSI) and Foreign, Commonwealth & Development Office (FCDO) clarified that this is not the intent of the UK sanctions regime, and a more recent decision of the High Court in *Litasco SA v. Der Mond* appears

to have retreated from the broad interpretation reflected in *Mints*.

Outlook

The sanctions imposed on Russia show no sign of letting up, and sanctions-related disputes will therefore likely continue to impact banks and other financial institutions in 2024. These disputes are likely to have important implications for key components of the international banking system, such as the approach taken to on-demand guarantees.

2024 may also see disputes arising from the question of the meaning of "control", following the Court of Appeal's *Mints* judgment and subsequent *Litasco* decision.

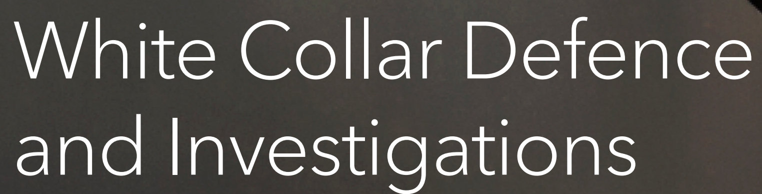
The sanctions imposed on Russia show no sign of letting up, and sanctions-related disputes will therefore likely continue to impact banks and other financial institutions in 2024.

Quickfire Hotspots

The crypto disputes space has noted some interesting activity, with the courts showing a nimble approach and a willingness to make new law. In 2023, we saw the challenges of applying old law to new products, such as disputes about whether crypto staking products fall foul of the collective investment scheme regime.

The FCA has had an unhappy time at the Upper Tribunal, which we expect will galvanise the willingness of those disaffected by FCA decisions to take the fight to the Upper Tribunal.

We have not heard the last of Credit Suisse and related AT1 bonds. While bondholder claims against the Swiss government and others took up a lot of airtime in 2023, we expect more individualised claims to emerge as the dust settles in 2024 against banks and fund managers who put their investors into significant AT1 positions.



LATHAM & WATKINS

By Pamela Reddy, Nathan Seltzer, Mair Williams, and Matthew Unsworth

New SFO leadership and changes to corporate crime laws in the UK marked some of the most notable developments in 2023.

Despite a turbulent few years, the SFO chalked up a significant victory in November 2022 when it imposed the UK's largest ever fine on Glencore: £183 million, in addition to a £93.5 million confiscation order. The fine resulted from Glencore's conviction for bribery in relation to payments that its West Africa desk made to obtain preferential access to oil, but the consequences for individuals remain to be seen.

In November 2023, the SFO again delayed its decision on whether to charge any individuals in the case — this time until July 2024.

The arrival of new SFO Director Nick Ephgrave signals a new era for the agency and a chance to kickstart corporate enforcement. Ephgrave is the first non-lawyer to hold the position, and his early priorities include bolstering the SFO's investigation capabilities and issuing updated enforcement guidance. The UK is likely to see a more active SFO under Ephgrave's tenure; indeed, three new investigations have already been announced since he arrived, one of which involved the SFO's most significant dawn raid in recent years, with over 80 investigators searching nine sites across South East England accompanied by the Metropolitan Police. The SFO has several more ongoing investigations into companies from a broad spectrum of sectors, which may lead to more criminal charges or deferred prosecution agreements.

The arrival of new SFO Director Nick Ephgrave signals a new era for the agency and a chance to kickstart corporate enforcement.

Last year, for example, the SFO brought bribery charges against three former employees of a now-defunct mining company and fraud charges against three former directors of an ethical investment scheme. The agency also recently charged four individuals with fraud offences in connection with the collapse of a UK café chain.

The Economic Crime and Corporate Transparency Act 2023

Ephgrave's efforts to open more new cases may be helped by changes introduced by the Economic Crime and Corporate Transparency Act 2023 (ECCTA). In particular, the ECCTA removes restrictions on the SFO's pre-investigation powers under Section 2 of the Criminal Justice Act 1987, permitting them to be used for all potential cases (and not just those relating to international bribery and corruption). The ECCTA also replaces the controversial "directing mind and will" test for corporate liability, which, many argue, was in practice ill-suited to prosecuting large organisations with decentralised management structures. A company can now be found liable if one of its senior managers commits an offence while acting within the actual or apparent scope of their authority.

Among the most significant aspects of the ECCTA was the creation of a new offence of "failure to prevent fraud", following similar offences in relation to bribery and the criminal facilitation of tax evasion. The offence is a little different to its predecessors, most notably in that the jurisdiction is different (the focus is on the location of the victim rather than the company and its operations) and the exemption of SMEs. Like the other "failure to prevent" offences, failure to prevent fraud does not impose any individual liability, but companies found guilty can be sentenced to an unlimited fine. However, a defence will be available if the organisation had "reasonable procedures" in place to prevent fraud, which contrasts with previous failure to prevent offences. We recommend that

larger companies look at their existing policies and procedures to determine how they can be updated to help prevent fraud and strengthen a defence of reasonable procedures.

Whistleblowing

Whistleblowing is another area ripe for reform. The government is reviewing the existing UK whistleblowing framework (governed by the Public Interest Disclosure Act 1998) and considering enhancements to encourage and protect whistleblowers. By comparison, the EU Whistleblowing Directive[1] protects a considerably broader range of would-be whistleblowers from retaliation, including non-executive directors, self-employed contractors, and "facilitators" (e.g., family members of a whistleblower). It also requires organisations above a certain size to establish internal reporting channels. One proposal that may be revisited in the UK is the creation of an "Office of the Whistleblower", a public body with a range of proposed powers, including the ability to amend relevant regulations and offer whistleblowers financial support. Any changes to legislation may require companies to do more to encourage and support those who make whistleblowing reports.

Reforming fraud laws could also feature on a future legislative agenda. In October 2023, the Home Office announced the Independent Review of Disclosure and Fraud Offences[2] to scrutinise whether the "disclosure regime is working in a digital age and if fraud offences, including those specified in the Fraud Act 2006, meet the challenges of investigating and prosecuting modern fraud". The review was promised as part of the Home Office's Fraud Strategy and will also consider how the criminal disclosure rules can be streamlined for cases with large volumes of digital material. There could even be a rethink of the SFO's role and remit, pending the conclusions of a parliamentary inquiry into the independence and accountability of UK regulators.

A US Perspective

Across the Atlantic there have been high-profile policy changes, with the US Department of Justice (DOJ) taking steps to further incentivise voluntary self-disclosure (VSD) of misconduct by corporate defendants. The DOJ's Criminal Division revised its Corporate Enforcement Policy (CEP) to provide enhanced incentives for VSD and to clarify that "aggravating circumstances" — e.g., involvement of senior management in the misconduct — is not a bar to a declination. Under the revised CEP, a declination will still be available if the company can demonstrate: (1) immediate VSD; (2) an effective compliance program; and (3) "extraordinary" cooperation. Even if a company does not benefit from a declination, the revised CEP also provides for more generous reductions in fines for VSD (now up to 75% off the lower end of the applicable US Sentencing Guidelines range).

A new M&A Safe Harbor policy also allows an acquiring company to receive a declination for misconduct at the target, conditional on: (1) prompt VSD within six months of closing; (2) full cooperation with the ensuing investigation; and (3) engagement in requisite, timely, and appropriate remediation, restitution, and disgorgement.

Preparing for the Year Ahead

Companies may wish to demonstrate to a renewed and recharged SFO that they are not only taking compliance seriously, but also they are actively working to prevent bribery, tax evasion, fraud, and the other offences included in the ECCTA. It remains crucial for companies to stay alive to any economic crime risks within their business, ensuring adequate internal processes are in place to help report and manage potential issues.

It remains crucial for companies to stay alive to any economic crime risks within their business, ensuring adequate internal processes are in place to help report and manage potential issues.

Below are key steps that we recommend boards and compliance teams consider taking now, particularly in preparation for the new offence, which is likely to come into effect in early 2024.

- Reevaluate internal policies and procedures, including training, to address any gaps in relation to the specified fraud offences
- Check that dawn raid manuals or training are up to date and that key personnel are prepared should any issues arise
- Ensure that third-party onboarding due diligence is thorough and that due diligence is regularly reviewed, as failure to prevent offences renders companies liable for acts committed on their behalf
- Check that third-party contracts are up to date with market standards and that any bribery and corruption provisions are extended to include the new offence when it comes into force
- Establish the correct tone and messaging from the top down, not just in relation to new offences, and encourage employees to speak up with concerns or issues

1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937.
2. https://www.gov.uk/government/collections/independent-review-of-disclosure-and-fraud-offences.

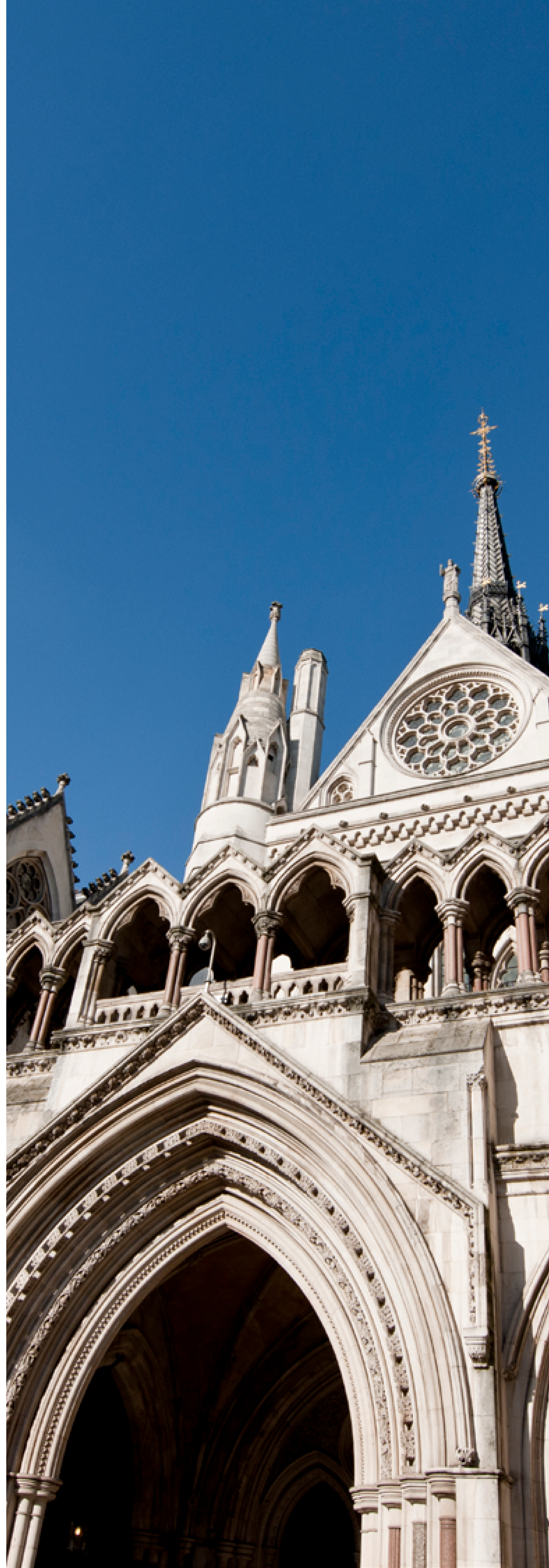
About Latham's London Litigation & Trial Practice

Our litigation practice regularly secures major victories and favourable settlements in high-stakes disputes in the UK courts and globally.

We pair industry fluency with unrivaled foresight from the outset of any dispute, always staying ahead of the opposition. Our pragmatic approach emphasises delivering results and resolving our clients' most complex and mission-critical disputes.

We litigate at the forefront of emerging market, business, legal, and regulatory trends. Our preeminent London litigation team works seamlessly with colleagues throughout Latham's unmatched global platform to skillfully resolve the most complex disputes across industries and jurisdictions.

We take on a wide range of high-value cases, including banking disputes, contract litigation, class actions, internal and regulatory investigations, as well as defamation, fraud, insolvency, privacy, and trade secrets matters.



Contributors

Gregory Bonné
Partner
London
T +44.20.7710.4762
E greg.bonne@lw.com

Andrea Monks
Partner
London
T +44.20.7710.4767
E andrea.monks@lw.com

Aleksandra Dulska
Associate
London
T +44.20.7866.2706
E aleksandra.dulska@lw.com

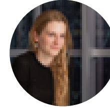
Oliver E. Browne
Partner
London
T +44.20.7710.1825
E oliver.browne@lw.com

Samuel Pape
Partner
London
T +44.20.7710.1113
E samuel.pape@lw.com

Duncan Graves
Associate
London
T +44.20.7710.5845
E duncan.graves@lw.com

Martin Davies
Partner
London
T +44.20.7710.3058
E martin.davies@lw.com

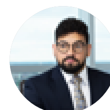
Nell Perks
Partner
London
T +44.20.7710.4749
E helennell.perks@lw.com



Anna Kullmann
Associate
London
T +44.20.7710.1135
E anna.kullmann@lw.com

Ian Felstead
Partner
London
T +44.20.7710.4733
E ian.felstead@lw.com

Pamela Reddy
Partner
London
T +44.20.7710.1027
E Pamela.Reddy@lw.com



Sami Martin Qureshi
Associate
London
T +44.20.7710.4711
E sami.qureshi@lw.com

Sophie J. Lamb KC
Partner
London
T +44.20.7710.3012
E sophie.lamb.kc@lw.com

Nathan H. Seltzer
Partner
London
T +44.20.7710.1020
E nathan.seltzer@lw.com

Edd Rarity
Associate
London
T +44.20.7710.3081
E edd.rarity@lw.com

James Lloyd
Partner
London
T +44.20.7866.2668
E james.lloyd@lw.com

Ludmilla Le Grand
Counsel
London
T +44.20.7710.4508
E ludmilla.legrand@lw.com

Matthew Unsworth
Associate
London
T +44.20.7866.2760
E matthew.unsworth@lw.com

Oliver Middleton
Partner
London
T +44.20.7710.4780
E oliver.middleton@lw.com

Alex Cox
Associate
London
T ++44.20.7710.1873
E alex.cox@lw.com

Mair Williams
Associate
London
T +44.20.7710.4781
E mair.williams@lw.com

LATHAM & WATKINS

Austin
Beijing
Boston
Brussels
Century City
Dubai
Düsseldorf
Frankfurt
Hamburg
Hong Kong
Houston
London
Los Angeles
Madrid
Milan
Munich
New York
Orange County
Paris
Riyadh
San Diego
San Francisco
Seoul
Silicon Valley
Singapore
Tel Aviv
Tokyo
Washington, D.C.

LW.com

Latham & Watkins is the business name of Latham & Watkins (London) LLP, a registered limited liability partnership organised under the laws of New York and regulated by the Solicitors Regulation Authority (SRA No. 203820). A list of the names of the partners of Latham & Watkins (London) LLP is open to inspection at its principal place of business, 99 Bishopsgate, London EC2M 3XF, and such persons are either solicitors, registered foreign lawyers or European lawyers. We are affiliated with the firm Latham & Watkins LLP, a limited liability partnership organised under the laws of Delaware. © Copyright 2024 Latham & Watkins. All Rights Reserved.