RADIUS LAW

COMMERCIAL BULLETIN

Your guide to the latest legal updates from the team at Radius Law.

JULY 2024

Nº 84

COMMERCIAL & CORPORATE

Liability for inducing a contract breach.

The Court of Appeal has confirmed in a recent case[1] that companies may be liable for inducing another company to breach a contract in circumstances where they know their actions will induce that breach.

This case concerned a supplier that was supplying companies in breach of an exclusivity agreement. The third-party recipient companies knew they were being supplied in breach of an exclusivity agreement. The Court, following a precedent from a 1949 case[2], ruled that simply placing orders with the knowledge that it would cause the exclusivity obligation to be breached was sufficient to make such recipient companies liable for inducing the breach.

Force Majeure

Force majeure clauses commonly provide that the party wishing to rely on it must first use reasonable endeavours to overcome the force majeure event.

A recent Supreme Court decision[3] considered a shipping case where the contract provided that the shipping company would be paid in USD, however due to sanctions restrictions imposed by the U.S. Treasury, payments in USD were prohibited. The customer offered to resolve the problem by payment in Euros.

The Supreme Court however ruled that ***a reasonable endeavours proviso does not require a party to accept a non-contractual solution.***

Directors: personal liability.

The Supreme Court has given guidance[4] on the circumstances in which directors may incur personal liability for a tort committed by the company.

A tort is otherwise known as a civil wrong (e.g. by negligence or misrepresentation) that has caused another party to suffer a loss.

The key takeaway from the case is that the ***law does not exempt directors from personal liability for torts committed by their companies.*** The directors may be personally liable where they knew the essential facts which made the company's conduct unlawful and intended to procure that conduct or to participate in a 'common design' to that end.

Directors Duties

The Institute of Directors ('IoD') is consulting on a new voluntary Code of Conduct for directors. You can access a link to the consultation document on the IoD website and it is open until the 16th August.

Staying on the theme of directors duties, an independent legal opinion commissioned by the Pollination and Commonwealth Climate Law Initiative, has confirmed that nature-related risks are relevant to directors' duties under the Companies Act and that to fulfil these legal duties directors must:

1. Identify any nature-related risks facing the company;
2. Assess which risks are relevant and not trivial, taking expert advice where appropriate;
3. Decide in good faith whether a course of action should be taken to mitigate those risks and take the relevant steps, if so; and
4. Record all decision-making in writing.

Changes at Companies House.

The second tranche of significant company law provisions in the Economic Crime and Corporate Transparency Act 2023 ('ECCTA') that expand the powers of Companies House came into force at the start of May.

Companies House now has the power to fine businesses (up to £10,000) for most offences under the Companies Act 2006[5]. According to the explanatory memorandum on the powers, Companies House will publish guidance before it starts issuing financial penalties.

Companies House has also issued new fees[6]. Fees have increased significantly to take account of the additional requirements from the ECCTA. The new list of fees is available on the Government website.

Changes at the Company Names Tribunal

Brand owners will be pleased to learn other changes[7] made by the ECCTA will make it easier to challenge companies at the Company Names Tribunal where they have been established with similar name to the brand owner and where the company name has been registered for the primary purpose of preventing someone else with legitimate interest from registering it, or demanding payment from them to release it.

Previously companies that had set up with a similar name to a brand owner could defend their actions by saying that it has already operated under that name and it had incurred substantial start-up costs in preparation. This defence has now been removed.

CONSUMER

New Digital Markets, Competition & Consumer law

Following the announcement of the election the Digital Markets, Competition & Consumers Bill ('**DMCC**') was pushed through and passed by Parliament on the 23rd May. It is expected to be in force in the Autumn.

The new law brings changes in four key areas:

- Consumer protection

- The Competition and Markets Authority ('CMA') will have new direct enforcement action powers and be able to impose fines of up to 10% of global turnover.
- Fake reviews will be added to the list of prohibited commercial practices. Hidden fees and unavoidable drip pricing will be prohibited.
- There will be new rules to protect consumers from subscription traps.

- Digital markets
  - There will be special rules for large digital firms that are deemed as having 'strategic market status' ('SMS').
- Merger control
  - There are changes to the merger controls rules including a change in the turnover threshold to £100m and there will be a new 'safe harbor' for small mergers.
- Competition law
  - There will be tougher powers to investigate and enforce competition laws.
  - This includes more powers to gather evidence located overseas and on domestic premises.
  - New fining powers (up to 1% of annual turnover) for companies failing to comply with a CMA investigation.

COMPETITION

Wage fixing and no poach agreements

The European Commission published a policy brief in May echoing statements by other regulators (including the UK Competition and Markets Authority) that competitors colluding to fix wages or agreeing to not poach each other's staff will breach competition laws (subject to some small exceptions).

The key takeaways of the policy brief are:

- that such actions are 'by object' infringements – meaning that the Commission would not have to prove that they actually damaged competition;
- that competitors for these purposes means anyone competing to secure the same talent so could be businesses in different business sectors.

DATA SECURITY

Cyber Risks

We all know that cyber risks are a major threat to any business. Two recent Government surveys[8] have emphasised that the risks are high but that the preparedness of companies is lacklustre.

In the last 12 months, 74% of large businesses experienced a breach or attack (up from 69% the year before), with phishing attacks being the most disruptive kind (making up 91% of incidents). A separate report published by Statista estimated that the annual cost of cybercrime in the UK was ***£250m in 2023***. This is projected to increase to over ***£1.424trn by 2028***.

Despite this immediate threat the surveys found that ***only 28% of medium businesses and 48% of large businesses review cyber risks in relation to their immediate suppliers***.

In the light of these increasing threats and reports of a cyber breach at the Ministry of Defence, the Information Commissioner has issued a new practical guide titled 'Learning from the mistakes of others'.

Subject access requests

The High Court has recently provided clarification[9] that when faced with a subject access request, an organisation may withhold information about the recipients of personal data for responding to subject access requests[10], unless the recipients have consented to the disclosure of the data, or it is reasonable to disclose the recipients' information without their consent. In this case the High Court agreed that the organisation was right to refuse to provide the recipient information as the person seeking the data had made threatening remarks and the organisation feared for the safety of anyone whose personal data was disclosed.

Assessing the data risks of AI

Last month, the ICO announced that it would not take enforcement action against Snap for its ChatGPT powered "MyAI" chat-bot - despite its Preliminary Enforcement Notice issued in October 2023.

The ICO had found that Snap had failed to adequately complete a privacy impact assessment on its AI tool, but it appears that its pro-active approach and willingness to cooperate with the ICO has helped it to avoid any penalties.

The ICO has now published a 62 page decision which provides helpful guidance to any other organisations assessing similar tools.

It provides worked analysis in key areas, including on:

- the assessment of whether an organisation is a separate or joint controller;
- extraterritorial risks;
- information needed about data sharing with other entities; and
- mitigation measures.

EMPLOYMENT

Settlement agreements can settle future unknown claims across Great Britain

In the March issue we reported that the Scottish Court of Session held that settlement agreements can settle future unknown claims if those future claims are explicitly identified in the agreement with ***clear and unambiguous wording***. Recently, the Employment Appeal Tribunal (EAT) in England and Wales agreed with the Scottish Court of Session.

The EAT went further and held that ***future claims can be settled irrespective of whether the employment relationship continues, or it has ended.***

Employer could not withdraw lifelong benefit discontinued by a third-party provider

In this case[12], Heathrow Express Operating Company Ltd (HEOC) offered a ***contractual right to a life-long discount*** on rail travel if employees were made redundant after five years' service. The benefit was provided by a third party, RST Ltd (RST). The agreement between HEOC and RST allowed for withdrawal of the benefit. In 2019,

RST gave notice to HEOC withdrawing the benefit for employees employed after 1996. The Claimants were made redundant in 2020. They had five years' service but were employed after 1996 and were told the benefit had been withdrawn. They claimed breach of contract.

The EAT found that the Claimants' contracts did not incorporate the withdrawal provisions of the agreement between HEOC and RST because:

- The terms and conditions issued to employees about the benefit did not refer to the agreement between HEOC and RST or to the right to withdraw the benefit.
- The Claimants were not given a copy of the agreement.
- HEOC did not, therefore, have a contractual right to withdraw the benefit.

Former employee prevented from soliciting or dealing with former employer's customers

When employees breach restrictive covenants, employers can seek an interim injunction preventing employees from doing so, provided there is ***a risk of significant harm to their business that would not be adequately compensated by damages.***

In this case[13], Mr Mogford's (M) employment contract contained an express duty of confidentiality and covenants preventing solicitation of and dealing with customers during employment and for 12 months post-termination. The employer, a supplier of fire safety goods and services, sought an interim injunction because M had allegedly:

- Provided fire safety services to the employer's customers on his own behalf before and after he resigned.
- Used the employer's confidential information (e.g. customer details and pricing information).
- Approached customers offering his services.

The High Court concluded that:

- there was a strong argument that the covenants were reasonable and therefore enforceable
- damages would not be an adequate remedy, and
- the balance of convenience favoured granting the interim injunction.

Worker victimised and subjected to detriment because of historical complaints

Workers who blow the whistle are protected from detriment and dismissal. Workers who have done a 'protected act' (e.g. bringing a discrimination claim), are also protected from victimisation.

Mr Moussa (M)[14] supervised passengers at ticket barriers. In 2013, M was dismissed and claimed unfair dismissal and victimisation. M was reinstated and in 2018 claimed a passenger had assaulted L, a colleague. The employer found no evidence of assault, conducted a flawed investigation, kept M suspended, but allowed L to return to work and later issued a first written warning despite dismissing most allegations. M claimed victimisation and detriment.

The Tribunal (and the EAT, on appeal) found that M was subjected to detriments and victimised in 2018 because of the 2013 claims:

- there was a negative 'collective memory' of M, who was labelled an 'agitator'.
- HR influenced the decision maker, who was unaware of the 2013 claims, which led to M being treated unfairly.

UPCOMING EVENTS

31st July, 2024

Senior Counsel Event – AI Part 2: Focussing on Integrating AI in Legal Settings
Online

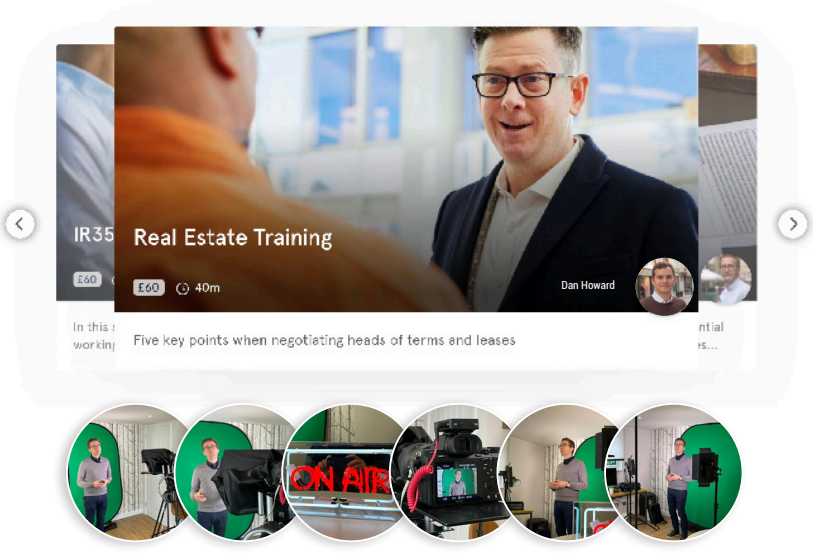
Our interactive virtual sessions are an opportunity for in-house counsel to share experiences, insights and best steps to protect your organisations.

Book Now >>

RADIUS LAW TRAINING HUB

Online and in-person courses starting from *only* £50+VAT

Learn more



Cases, laws, decisions referred to in this Bulletin

1	Northamber PLC v Genee World Ltd & Ors (Rev1) [2024] EWCA Civ 428
2	British Motor Trade Association v Salvadori [1949] Ch 556
3	RTI Ltd (Respondent) v MUR Shipping BV (Appellant), Case ID: UKSC 2022/0172
4	Lifestyle Equities CV v Ahmed [2024] UKSC 17
5	Economic Crime and Corporate Transparency Act 2023 (Financial Penalty) Regulations 2024
6	Registrar of Companies (Fees) (Amendment) Regulations 2024
7	Section 69(1)(b); 69(3) and 69(4) Companies Act 2006
8	"Wave Three" of its Cyber Security Longitudinal Survey & 2024 Cyber Security Breaches Survey
9	Harrison v Cameron and ACL [2024] EWHC 1377 (KB),
10	'Rights of others' exemption under paragraph 16 of Schedule 2 to the DPA 2018
11	Clifford v IBM United Kingdom Ltd [2024] EAT 90
12	Adekoya and ors v Heathrow Express Operating Company Ltd [2024] EAT 72
13	Morgan Fire Protection Limited v. Robert Peter Mogford and General Fire Protection Limited [2024] All ER (D) 79 (May)
14	Moussa -v- First Greater Western Limited [2024] EAT 82