

Digital Markets and Corporate Power – The DMCCA 2024



Procurement and Supply Chain Management Made Simple.

Foreword

Economic power was once measured most visibly through factories, physical distribution networks, property, workforce scale and conventional market share. Increasingly, however, commercial influence is exercised through digital platforms, algorithms, data and interfaces that determine what consumers see, which businesses reach them and how choices are presented. In 2024, the UK Digital and Technology sector generated an estimated £408 billion of turnover and £158 billion of gross value added.

That shift is visible in everyday behaviour. The Office of Communications (Ofcom) reported that UK adults spent an average of four-and-a-half hours online each day in 2025, with Alphabet and Meta services accounting for 51% of that time. YouTube alone reached 94% of UK adults. Control over attention at this scale gives platform operators extraordinary influence over advertising, discovery, recommendation and purchasing, even where consumers pay nothing directly for the underlying service.

The same dependency is increasingly apparent across public services. The UK public sector spends more than £26 billion annually on digital technology and employs nearly 100,000 digital and data professionals. G-Cloud 15, launched in 2026, carries an estimated four-year value of about £14 billion, with roughly £3 billion of annual public-sector cloud expenditure expected through the framework. Digital infrastructure has therefore become fundamental to government delivery and private commerce alike.

Power in these markets often arises from architecture rather than ownership. Search rankings determine visibility, app stores determine distribution, defaults influence behaviour, data improve personalisation, and algorithms determine which options are promoted or suppressed. A platform can therefore act simultaneously as marketplace operator, rule-maker, competitor, and gatekeeper, so control over access conditions can matter as much as prices, physical assets, or sales volumes, particularly once participation becomes commercially unavoidable.

The CMA has begun testing that power directly, designating Google with SMS in general search and search advertising, and Apple and Google with SMS in their respective mobile platforms, while extending its scrutiny into enterprise software through an SMS investigation of Microsoft's business-software ecosystem. The Digital Markets, Competition and Consumers Act 2024 (DMCCA) supplies the legal architecture behind that shift, and the chapters that follow trace how gateways once treated as background infrastructure have become a defined subject of UK economic regulation.

The Digital Economy and Corporate Power

The digital economy has become part of the infrastructure through which UK households, businesses and public bodies communicate, advertise, buy, sell and obtain information. Department for Science, Innovation and Technology (DSIT) estimates indicate that the Digital and Technology sector generated around £408 billion of turnover and £158 billion of gross value added (GVA) in 2024, equivalent to about 6% of UK GVA, while employing approximately 1.33 million people nationally.

Digital platforms can occupy several commercial roles at once. A search engine may connect users with information while selling advertising; an app store may distribute applications while operating competing applications; and an online marketplace may host independent sellers while retailing its own products. Social platforms similarly control access to audiences while monetising attention and data, creating conflicts where a platform sets rules for markets in which it also competes.

The economic significance of those gateways is visible in everyday behaviour. Ofcom reported that UK adults spent an average of four-and-a-half hours online each day in 2025, with Alphabet- and Meta-owned services accounting for more than half of total online time. Office for National Statistics (ONS) data also show that internet sales represented 27.4% of Great Britain's total retail sales during 2025, underlining how digital interfaces increasingly shape which businesses consumers encounter.

Gatekeeper power therefore extends beyond headline market share. Control over rankings, default settings, app approvals, advertising auctions, payment systems, data access and interoperability can influence whether another business reaches customers at all. The commercial consequences affect private enterprise and public services alike, because government, local authorities, universities, National Health Service (NHS) bodies and regulated industries increasingly depend on cloud, mobile, search and software ecosystems supplied by a comparatively small number of global technology companies.

Why Traditional Competition Law Was Being Challenged

Traditional competition law remains essential, but digital markets exposed limitations in enforcement models designed around slower-moving industries and identifiable transactions. Network effects can strengthen a platform as more users join, because participation makes the service more valuable to other users, advertisers or sellers. That feedback loop can produce rapid concentration before an investigation concludes, leaving competitors facing a market in which scale itself becomes a barrier to entry or expansion.

Data can reinforce the same process. Large platforms may observe billions of searches, clicks, purchases or interactions, improving algorithms, advertising tools and personalisation in ways unavailable to smaller rivals. The CMA's 2020 digital advertising study found that Google had generated at least 90% of UK general-search traffic for many years, and that in 2019 it earned more than 90% of the £7.3 billion UK search-advertising market.

Economies of scale add another layer. Digital services often require substantial expenditure on software engineering, data centres, cyber security, artificial intelligence (AI) and global distribution. At the same time, the marginal cost of serving an additional user can be comparatively low. Successful platforms can therefore spread high fixed costs across immense user bases. In cloud infrastructure, the CMA reported a UK market worth about £9 billion in 2023, growing by more than 30% annually.

Lock-in can be equally powerful. Customers may accumulate purchased applications, stored data, learned workflows, subscriptions and technical integrations that make changing providers costly, even where an alternative exists. The CMA's cloud investigation identified egress charges, technical barriers and committed-spend discounts as impediments to switching, finding that Amazon Web Services and Microsoft each accounted for up to 40% of UK customer spending on cloud services during the review.

Speed completes the challenge. Digital products, interfaces and AI features can change in weeks, whereas conventional competition cases may require lengthy evidence gathering, legal analysis and appeals. By the time a remedy arrives, consumer habits, developer investment and market structure may have shifted materially. The policy response was therefore not to abandon established competition law, but to supplement it with a forward-looking regime addressing entrenched power before harm becomes effectively irreversible.

The Digital Markets, Competition and Consumers Act 2024

The DMCCA received Royal Assent on 24 May 2024 and created a wide-ranging reform package rather than a single technology rulebook. Its three principal strands address competition in digital markets, broader competition-law and merger-control reform, and stronger consumer protection. The digital-markets competition regime commenced on 1 January 2025, while the principal direct consumer-enforcement and unfair-commercial-practices provisions took effect on 6 April 2025, giving businesses a transitional period before the new consumer regime fully applied.

The competition reforms modernised several existing powers. Among them, the ordinary UK merger turnover threshold increased from £70 million to £100 million. In comparison, a new acquirer-focused jurisdictional test can capture transactions where one party has at least a 33% UK share of supply and UK turnover exceeding £350 million. A small-merger safe harbour generally removes transactions from the share-of-supply test where each party's UK turnover is £10 million or less.

Consumer enforcement changed just as significantly. The CMA can now determine certain consumer-law infringements administratively rather than depending solely on court proceedings, with penalties for relevant infringements reaching the greater of £300,000 or 10% of worldwide turnover. Taken together, the three strands connect market structure, corporate conduct and consumer outcomes, treating digital power not as an isolated technology issue but as a competition, governance and consumer-protection concern across the economy.

From Reactive Enforcement to Proactive Regulation

Conventional competition enforcement usually asks whether conduct has already infringed established legal prohibitions, leaving regulators examining yesterday's behaviour while technology, interfaces and commercial strategies keep changing. The DMCCA adds a more anticipatory model. Once a business has SMS for a designated digital activity, the CMA can establish tailored conduct requirements and investigate pro-competition interventions without first proving a conventional abuse of dominance in every instance.

The distinction matters because digital markets can tip. A default setting, exclusive distribution arrangement or discriminatory ranking practice may influence millions of users, while developers and advertisers adapt investment decisions around platform rules. If a challenger loses access during a critical growth phase, later compensation may not recreate the competitive opportunity already lost to a faster-moving rival. Forward-looking regulation therefore aims to preserve contestability while a market can still respond.

Statutory tests nevertheless constrain the regime. SMS requires substantial and entrenched market power, a position of strategic significance, a UK link and satisfaction of the turnover condition. Conduct requirements must be proportionate and pursue fair dealing, open choices, or trust and transparency, while pro-competition interventions require an investigation and an adverse effect on competition. These safeguards distinguish targeted digital regulation from a power to redesign successful businesses simply because they are large.

The CMA has also emphasised participation and sequencing. Its statutory SMS investigation period is nine months, during which it gathers evidence from the business under investigation, customers, competitors, trade bodies and interested parties. During the regime's first wave of investigations, the CMA reported meeting more than 170 stakeholders. This evidence-led

structure matters because the economic effects of defaults, interoperability limits, data access and ranking systems can differ markedly between search, mobile, cloud and business software.

Google search demonstrates the shift from diagnosis to rules. The CMA opened its first SMS investigation in January 2025, designated Google's general search and search-advertising activities on 10 October, and subsequently moved to specific requirements rather than reopening a conventional dominance case for each concern. By June 2026, the CMA had imposed publisher, fair-ranking and data-portability requirements, illustrating how the regime can progress from designation to detailed obligations within a defined structure.

The approach can also influence behaviour without immediately imposing every available statutory measure. In April 2026, Apple and Google implemented commitments on app review, ranking, data use and, for Apple, requests for interoperable access to operating-system features. The CMA described these as immediate improvements following SMS designation. Such outcomes show proactive regulation that combines formal requirements, commitments, monitoring, and consultation, selecting whichever mechanism is proportionate to the concern identified.

Strategic Market Status

SMS is the gateway into the DMCCA's digital-markets regime. It is not a general label attached to a corporation, nor a finding that every activity it undertakes is anti-competitive. Under section 2, the CMA designates an undertaking for a digital activity linked to the United Kingdom, so obligations connect to the specific activity that generated the regulatory concern rather than to the business as a whole.

Designation requires both substantial and entrenched market power and a position of strategic significance. The CMA must assess power on a forward-looking basis over at least five years, considering foreseeable developments if designation did not occur, without conducting a formal market-definition exercise. The approach recognises that rapidly evolving digital ecosystems may not fit comfortably within rigid product boundaries, particularly where operating systems, browsers, applications, advertising and data services interact.

A separate turnover condition limits the regime to businesses of exceptional economic scale. The threshold is met where the relevant undertaking or group has more than £25 billion in global turnover or more than £1 billion in UK turnover during the relevant period. Meeting the financial threshold does not itself establish SMS; it merely permits consideration of designation where the remaining conditions concerning power, strategic significance and UK connection are also satisfied.

An SMS designation ordinarily lasts five years unless revoked earlier, giving the CMA time to monitor conduct and implement measures while preventing designation from becoming permanent by default. Before expiry, the CMA must reassess the position through a further investigation if designation may continue. Apple and Google's October 2025 mobile-platform designations therefore concern operating systems, native app distribution, mobile browsers and browser engines specifically, rather than every product those groups supply.

What Makes a Business Strategically Powerful?

Strategic power is broader than being large. Section 6 allows strategic significance to arise where a digital activity has significant size or scale, is used by a significant number of other businesses in conducting their activities, enables the undertaking to extend market power into other activities, or allows it to influence how other businesses conduct themselves. A gateway can therefore be strategically important even where users pay little or nothing directly for access.

Search illustrates the gateway effect particularly clearly. Google handles more than 90% of UK general search queries, and the CMA reported that more than 200,000 UK businesses collectively spent over £10 billion on Google search advertising in the year preceding its

January 2026 proposals. Search rankings and advertising access consequently affect not only Google's revenues, but also the visibility, customer acquisition costs and growth prospects of businesses across the wider economy.

Mobile ecosystems create similar leverage. The CMA found that around 90–100% of UK mobile devices run on Apple or Google mobile platforms. The UK app economy is estimated to generate around 1.5% of gross domestic product (GDP) and support about 400,000 jobs, while app-store commissions can reach 30% on some in-app purchases. Control over app approval, ranking, payment routes, browser technology and device functionality can shape commercial opportunities far beyond the platform operator itself.

Strategic power can also arise through enterprise technology that public and private organisations depend upon daily. The CMA's fourth SMS investigation, opened in May 2026 and examined in detail later, is testing whether a major business-software ecosystem raises the same gatekeeping concerns. The case shows that gatekeeping is not confined to consumer smartphones: procurement, cloud migration, and AI adoption can equally depend on workplace software architecture.

Barriers to entry complete the picture. A challenger may need capital, data, developer participation, consumer trust, compatible technology and access to distribution before competing effectively, and these requirements can reinforce one another, making entry theoretically possible but commercially difficult. Strategic significance therefore reflects both present scale and the ability to influence the competitive environment around it, shaping the opportunities available to customers, suppliers and would-be competitors alike.

Conduct Requirements

Once the CMA establishes an SMS, it may impose tailored conduct requirements relating to the designated digital activity. These are not a uniform code applied identically to every designated business. A requirement must fall within the permitted statutory types and be proportionate to one or more objectives: fair dealing, open choices, or trust and transparency, allowing regulation to target a specific source of market power.

Permitted requirements can oblige an SMS business to trade on fair and reasonable terms, run effective complaints processes, or provide information users need. They can also prevent discriminatory treatment, self-preferencing or restrictions that stop users from choosing competing services where the statutory conditions are met. The emphasis is practical: the CMA converts broad competition concerns into observable operating rules that developers, advertisers and customers can understand and challenge.

Google's fair-ranking requirement shows how that tailoring works in practice. It obliges Google to rank organic results using objective, non-discriminatory criteria, including within generative-AI search features, and to provide greater transparency about ranking changes. A companion data-portability requirement enables authorised third parties to receive UK consumers' search data free of charge. Together, the measures address visibility and switching without prescribing Google Search's design in every respect.

Pro-Competition Interventions

Conduct requirements focus mainly on behaviour; pro-competition interventions can address deeper features of a digital market. Following SMS designation, the CMA may investigate whether a factor or combination of factors relating to the designated activity is producing an adverse effect on competition. If that test is met, it can impose measures to remedy, mitigate or prevent the effect, in an investigation that normally runs for up to nine months.

Potential interventions can reach structural features that everyday compliance rules may not resolve. CMA guidance identifies possibilities such as improving interoperability, enabling data portability or changing technical arrangements that make switching difficult. The legislation permits a broad remedial approach derived from the Enterprise Act framework, subject to proportionality and procedural safeguards, and the CMA can test or trial interventions before

embedding a remedy across a changing market.

Cloud services illustrate why deeper intervention can matter. Building on the market investigation discussed earlier, the CMA found an adverse effect on competition in 2025, identifying switching barriers, concentration and software-licensing concerns and recommending that it consider digital-markets investigations relating to major providers. The subsequent response combined engagement on egress fees and interoperability with the scrutiny that later became a dedicated SMS investigation into enterprise software.

That sequence also demonstrates an important boundary between tools. A market investigation can diagnose sector-wide problems, whereas an SMS designation creates an ongoing framework for targeted obligations concerning a strategically powerful digital activity. In March 2026, the CMA said Microsoft and Amazon were taking material steps on interoperability and cloud egress fees following engagement, while its Board separately decided to open the wider ecosystem investigation described later in this discussion.

Pro-competition interventions are not designed to guarantee competitors' success. Their purpose is to improve the competitive process where market characteristics prevent effective rivalry. This distinction matters for investment incentives because successful innovation and scale are not infringements in themselves. The regulatory question is whether entrenched control over data, technical standards, access points, or customer switching restricts competitive pressure enough to justify proportionate intervention that targets the obstacle rather than success.

For UK public procurement, the implications are significant. Central government departments, local authorities, NHS organisations, universities and housing providers increasingly purchase cloud, software, cyber-security and digital-platform services whose interoperability can affect long-term switching costs. Measures that lower technical or contractual barriers may strengthen future tender competition and reduce dependency risk, extending the relationship between digital-market regulation and procurement policy well beyond household consumers, into resilience, value for money and supplier choice across publicly funded services.

The Digital Markets Unit and the CMA

The Digital Markets Unit (DMU) operates within the CMA rather than as a separate statutory regulator. It was launched in shadow form in April 2021, before the DMCCA supplied the legal powers needed for the new regime. The CMA Board retains overall responsibility, while a Digital Markets Board Committee oversees and takes delegated decisions, placing digital-market expertise alongside established merger, competition and consumer-enforcement capabilities within one national authority.

The scale of that wider institution is material. For 2025–26, the CMA had a resource budget authorised at £148.4 million and reported resource outturn of £136.1 million, including total staff costs of approximately £105 million. Its impact assessment estimated average annual direct consumer benefits of £3.3 billion over the three years to 2025–26, equivalent to about £25 of measurable consumer benefit for every £1 spent on its operations.

Day to day, the DMU's work looks less like a courtroom than a standing conversation. Caseworkers spend months in meetings with engineers, publishers, developers and rival businesses before a single obligation is drafted, because a ranking algorithm or a billing default cannot be understood from a filing alone. That patient, technically literate style of regulation is itself part of what the DMCCA was designed to introduce alongside its formal powers.

Digital regulation is also increasingly collaborative. The CMA works alongside sector and cross-economy regulators including Ofcom, the Information Commissioner's Office (ICO) and the Financial Conduct Authority (FCA) through mechanisms developed for digital regulation, and cloud services illustrate the value of that interaction: Ofcom's market study referred the CMA for an in-depth competition investigation. Digital ecosystems frequently cut across

competition, communications, privacy, financial services, cyber security and procurement, making institutional coordination particularly important.

The Act in Practice -- Google, Apple and the Emerging SMS Regime

The regime moved from legislation to operational reality during 2025, with Google and then Apple and Google together designated with SMS in quick succession, as already noted. Designation itself creates no immediate obligation, however; it simply opens the door to tailored measures. What those measures actually require once decided, rather than merely when they were announced, is where the practical character of the regime becomes clearest, and where its real test lies.

The publisher requirement imposed on Google is particularly significant as generative AI reshapes search. It requires Google to give publishers effective controls over the use of their search content in generative-AI features, clearer information about that use, engagement metrics and appropriate attribution. The CMA described the opt-out capability as a world first. For news organisations and specialist publishers, the measure addresses bargaining power where material can feed AI-generated answers that reduce direct visits.

Apple and Google's mobile commitments address a different gateway. In April 2026, both companies implemented measures covering app review, ranking and data use, with Apple additionally providing a route for developers to request interoperable access to operating-system functionality. These measures target predictability and access rather than attempting to determine which applications ultimately succeed, reflecting the proportionality that constrains every conduct requirement under the statutory framework.

Further intervention remains under development. In June 2026, the CMA consulted on steering requirements intended to let developers direct users toward alternative transaction routes on fair and reasonable terms, potentially reducing dependence on app-store payment arrangements. The emerging regime is iterative: designation identifies strategic power, evidence determines priorities, and legal process shapes each intervention that follows, whether through binding requirements, negotiated commitments or continued monitoring of voluntary change.

Google and Apple provide practical tests of whether the regime's iterative flexibility can improve competition without suppressing innovation. In contrast, the Microsoft investigation will test whether similar concerns arise within enterprise software. In these cases, the CMA has translated findings of strategic market power into obligations directed at specific commercial practices, rather than applying a uniform regulatory template regardless of how market power operates within each digital activity.

Where the Regime Goes Next

The next frontier is enterprise software. On 14 May 2026, the CMA opened its fourth SMS investigation, examining Microsoft's business-software ecosystem across productivity software, personal-computer and server operating systems, database management systems and security products. The CMA says hundreds of thousands of UK businesses and public-sector organisations use Microsoft software daily, with more than 15 million commercial users across the ecosystem, making its competitive structure economically significant.

The investigation is considering whether bundling, default settings and limits on interoperability may make it harder for customers to switch providers or combine Microsoft products with competing services. The timing matters because generative and agentic AI is increasingly embedded in familiar workplace tools such as Microsoft 365 and Copilot. The CMA is therefore examining whether ecosystem advantages could influence which competing AI products can integrate effectively with software already used throughout organisations.

Public-sector dependency makes the inquiry especially relevant beyond conventional technology markets. Hospitals, councils, universities and central-government bodies use productivity suites, identity tools, operating systems, security products and cloud services as

operational infrastructure. A 2025 procurement notice from Kettering General Hospital and Northampton General Hospital, for example, estimated Microsoft licensing at about £2.44 million excluding Value Added Tax (VAT) over three years, illustrating how ecosystem choices become long-term procurement commitments.

The CMA has not yet concluded that Microsoft has SMS. The statutory investigation must be completed within nine months, with a decision indicated by February 2027. Its significance lies in the question being tested: whether gatekeeping can arise not only where consumers search, download apps or use smartphones, but where organisations depend upon interconnected software, security, cloud and AI tools whose compatibility can materially affect switching, resilience and competition.

A New Era of Consumer Enforcement

Consumer enforcement changed fundamentally on 6 April 2025. Under the DMCCA, the CMA can investigate suspected breaches of specified consumer legislation, issue provisional and final infringement notices, impose directions, accept undertakings and levy financial penalties through an administrative process. Courts retain an important role, but the CMA no longer needs a court judgment to decide that certain consumer laws have been infringed, substantially increasing the immediacy of regulatory exposure for businesses.

The sanctions alter the economics of non-compliance. For an infringement, the maximum penalty is the greater of £300,000 or 10% of worldwide turnover. Breaching undertakings or directions can attract penalties up to the greater of £150,000 or 5% of turnover, while information failures can trigger separate sanctions. Consumer law therefore shifts from a potentially remote litigation risk into an exposure that can affect earnings, reputation, customer remediation and board-level risk management.

The first year demonstrated how quickly those powers could translate into enforcement. The CMA opened investigations into 14 businesses, settled with two, issued 159 advisory and warning letters and published or updated 20 guidance documents during 2025–26, with early priorities including drip pricing, fake reviews and online choice architecture. The AA, Marks Electrical and StubHub cases examined later in this discussion each grew out of that same first-year enforcement drive.

Unfair Commercial Practices

Part 4 of the DMCCA replaced and updated the Consumer Protection from Unfair Trading Regulations 2008 for commercial practices occurring from 6 April 2025. Much of the previous framework remains recognisable, including prohibitions on misleading actions, misleading omissions, aggressive practices and conduct contrary to professional diligence. The change is therefore evolutionary as well as reforming: established consumer-protection principles continue, but now sit within legislation supported by stronger direct enforcement.

The regime also sharpens particular obligations. Where a trader makes an “invitation to purchase”, specified material information must be supplied or be apparent from context, and omitting it can itself make a practice unfair. The Act addresses drip pricing directly and bans fake reviews, so commercial teams must evaluate the customer journey, since legality can depend on what consumers are told before they decide, not merely what appears at checkout.

The practical reach is broad. The rules can apply to advertising, websites, apps, marketplaces, social-media promotions, call centres and other commercial communications before, during and after a transaction. The CMA’s November 2025 cross-economy review examined more than 400 businesses across 19 sectors and identified potential pricing or sales-practice concerns in 14 of them, showing how widely these obligations already reach in ordinary commercial life.

Unfair commercial practices are consequently not a specialist retail issue confined to a handful of well-known sectors. A membership website, a business-to-business software provider, a local tradesperson’s booking page and a national retailer can each fall within the same rules

if they shape how a consumer decides to transact. That breadth is why the sections that follow examine specific practices: drip pricing, fake reviews, and interface design.

Misleading Pricing and Drip Pricing

Drip pricing occurs when consumers are shown an initial price and unavoidable charges are introduced later in the purchasing journey. Under the DMCCA, invitations to purchase must present the total price, including mandatory fees, taxes and charges, or explain how it will be calculated where the total cannot reasonably be calculated in advance. Optional extras remain distinct, but must not be presented in a way that disguises what a consumer actually has to pay.

The economic scale is substantial. Department for Business and Trade (DBT) research published before commencement found that 46% of online businesses used hidden or dripped fees. It estimated that consumers could spend up to £3.5 billion extra online each year because of them. Service, booking and processing charges were particularly problematic because they were frequently unavoidable yet disclosed late, weakening consumers' ability to compare competing offers on a genuinely like-for-like basis.

The CMA responded with final price-transparency guidance, CMA209, on 18 November 2025, explaining mandatory charges, taxes, drip pricing and partitioned pricing, where component prices are displayed without making the overall payable amount sufficiently clear. On the same day, as part of the wider sweep already described, the regulator opened investigations into eight businesses and sent advisory letters to 100 more across 14 sectors, immediately translating general guidance into targeted casework.

Enforcement quickly produced outcomes. In April 2026, Automobile Association Developments Limited (AA) admitted infringements involving a mandatory £3 booking fee at its AA Driving School and BSM Driving School businesses, and the CMA imposed a £4.2 million penalty, reduced from £7 million for early settlement, alongside orders to refund more than £760,000 to over 80,000 learner drivers, the first use of the new powers to secure both a penalty and direct refunds together.

StubHub UK followed in June 2026. The ticket marketplace had added mandatory delivery and service fees only at the final checkout stage rather than in its headline ticket price. The CMA fined the business £889,200, again reflecting a settlement discount, and ordered refunds exceeding £590,000 to more than 50,000 customers. Both cases show how a charge worth only a few pounds per transaction can still generate a multi-million-pound liability once repeated at scale.

Price transparency also has competitive consequences. A business advertising £95 plus a mandatory £5 charge may appear cheaper than a competitor honestly advertising £100, even though both transactions ultimately cost the same. The law therefore protects more than individual purchasing decisions: it helps prevent compliant businesses being undercut by artificially low headline prices, supporting comparison, customer trust and fair competition across the market as a whole.

Fake Reviews and the Economy of Trust

Online reviews have become commercial infrastructure. The CMA estimates that as much as £23 billion of UK consumer spending each year is potentially influenced by reviews, while Which? research cited by the regulator found that 89% of consumers use online reviews when researching products or services. Ratings can influence search visibility, conversion rates and marketplace rankings, meaning manipulated reviews can shift demand between competing businesses and mislead individual purchasers.

Government research illustrates the scale of distortion. Across three common e-commerce product categories, an estimated 11% to 15% of reviews were likely fake. Consumers were 3.1% more likely to buy a product carrying well-written fake reviews, rising to 9.2% where the product cost more than £80. Fake review text alone was estimated to cause between £50

million and £312 million of annual UK consumer harm, excluding inflated star ratings and services.

The DMCCA therefore goes beyond prohibiting somebody from simply writing a fabricated review. Banned practice 13 covers submitting or commissioning fake reviews, concealing incentives, misleading publication and offering fake-review services. Businesses publishing reviews must also take reasonable and proportionate steps to prevent and remove fake or concealed incentivised reviews. CMA guidance issued on 4 April 2025 expects risk assessment, published policies, detection processes and appropriate responses to complaints.

Enforcement has already reached major platforms. Google gave undertakings requiring stronger detection and sanctions, including warnings on the profiles of UK businesses abusing reviews. Amazon followed in June 2025, committing to enhanced systems addressing fake reviews and “catalogue abuse”, where unrelated products inherit favourable ratings. After reviewing more than 100 websites, the CMA found potential compliance shortcomings at 54 businesses and opened investigations into five organisations, including Autotrader, Just Eat and Feefo, by March 2026.

Online Interfaces, Choice Architecture and Dark Patterns

Online choice architecture describes how websites and apps structure the environment in which consumers make decisions. Rankings, defaults, button prominence, colour, friction and the order in which information appears can all influence behaviour without changing the underlying product. Design is therefore not legally neutral: the CMA has identified practices sometimes described as dark patterns or sludge, where interface architecture can steer consumers towards outcomes they might not otherwise choose.

Urgency claims provide a familiar example. Countdown clocks, “only two left” messages, popularity statements and limited-time discounts can convey useful information when genuine, but become problematic when scarcity or deadlines are artificial. Behavioural evidence reviewed by the CMA found that scarcity messages can increase perceived value, purchase intentions and speed of purchasing while reducing further searching, compressing the time available for deliberation and honest comparison.

Emma Sleep became a UK case study, though one that reached its conclusion through the courts rather than the CMA’s newer administrative powers. Following a CMA investigation opened in 2022, the High Court in May 2026 endorsed a settlement after the retailer admitted that misleading countdown timers, false high-demand messages, and certain discount claims breached consumer law, reminding us that older enforcement routes remain available alongside the DMCCA’s faster procedures.

Defaults also play a role because consumers often accept pre-selected settings rather than actively changing them. Between April and November 2025, Marks Electrical automatically opted purchasers into paid appliance-recycling or packaging-removal services without obtaining their express agreement, affecting nearly 40,000 customers. The CMA imposed a £720,000 penalty, reduced for early settlement, and ordered around £600,000 in refunds, underlining that consent for paid extras must be genuinely expressed rather than engineered.

Cancellation journeys can create a similar asymmetry. A service may make joining possible in seconds but require multiple screens, repeated retention offers or offline contact to leave, preserving revenue through inertia rather than customer preference. The forthcoming subscription regime, discussed shortly, addresses this directly, while existing consumer law may already apply where design misleads or unfairly pressures consumers into remaining subscribed against their genuine preference.

None of this depends on any single villain. A product manager may set a default while solving an unrelated problem; a developer may build a countdown timer by following a template; a scarcity message may be inherited from a competitor’s site years earlier. That ordinariness is

precisely the governance challenge: harmful patterns rarely announce themselves, which is why testing outcomes matters more than assuming good intentions were enough.

Subscription Business Models

The dedicated DMCCA subscription-contract regime is not yet in force. Following consultation, the Government said in April 2026 that it expects to begin in spring 2027, with implementing regulations and guidance still required. The scale explains the policy interest: the UK has approximately 155 million active subscriptions, representing around £26 billion of consumer spending annually, with the average person holding about three subscriptions and spending approximately £500 each year across them.

The forthcoming rules are intended to make recurring contracts easier to understand and leave. Traders will face enhanced pre-contract information duties, reminder notices, and straightforward exit requirements; where consumers subscribe online, an online exit route must be available. A 14-day renewal cooling-off right is planned after a trial or a contract of at least 12 months automatically renews, with Government estimates suggesting the package could deliver around £400 million of consumer benefit each year.

The regime balances convenience with protection from inertia. Consumers will receive specified reminders and cooling-off information, while rules are intended to prevent terms that make cancellation disproportionately difficult. For digital content, the Government intends proportionate refunds during the renewal cooling-off period, so providers retain payment for supply already consumed. Businesses using subscription revenue should treat spring 2027 as an operational deadline for billing, notifications and cancellation workflows.

Consumer Redress

Enforcement is more effective when it restores losses in addition to stopping misconduct. Under the DMCCA framework, the CMA can require redress alongside directions and penalties, including refunds or compensation for affected consumers, though the regulator itself does not process those payments; the business subject to the order administers them. Public enforcement therefore supplements rather than replaces individual consumer rights and small-claims routes that remain available in parallel.

By June 2026, the CMA said its new powers had secured more than £1.95 million in refunds across its consumer cases, a figure that becomes more meaningful once broken down. The AA's refund programme, for instance, is returning an average of around £9 to each of more than 80,000 learner drivers, a sum few individuals would ever pursue alone but which becomes a serious corporate liability when multiplied across an entire customer base.

The other two cases follow the same pattern with different averages. Marks Electrical's nearly 40,000 affected customers are receiving roughly £15 each, while StubHub's more than 50,000 ticket buyers are due an average of £10.33 per transaction. Regulatory redress aggregates this kind of low-value, high-volume harm, turning thousands of individually trivial losses into a single, meaningful, enforceable liability for the responsible business, rather than leaving each customer to chase a claim alone.

Public enforcement does not extinguish the wider private-law framework. Depending on the circumstances, consumers may still possess contractual, statutory or common-law remedies, while other enforcers and courts retain functions under the consumer-protection system generally. The significance of CMA redress is therefore institutional: it addresses systemic practices affecting large groups, while individual rights remain available for disputes outside an order or for losses requiring separate assessment or evidence.

Redress also changes the financial logic of compliance. A business cannot assume its maximum exposure is the regulatory penalty, because remediation may require identifying transactions, contacting customers, processing repayments and reporting progress to the CMA; StubHub, for example, must report on its refund process for six months. The real cost of infringement therefore combines penalties, refunds, administration and reputational

damage, making prevention considerably cheaper than correction after the fact.

Financial Penalties and the Economics of Compliance

Turnover-linked penalties are designed to remain meaningful regardless of corporate scale. For direct consumer-law infringements, the CMA can impose up to the greater of £300,000 or 10% of worldwide turnover. That percentage matters because a fixed statutory maximum can become commercially trivial for a multinational group, whereas linking exposure to global revenue creates a sanction capable of influencing executive decisions even where the unlawful conduct concerns comparatively small charges imposed on individual UK consumers.

The architecture also penalises obstruction and broken commitments. Breaches of consumer undertakings or CMA directions can attract up to the greater of £150,000 or 5% of turnover, with potential daily penalties for continuing non-compliance. In comparison, certain information failures can attract penalties up to the greater of £30,000 or 1% of turnover. Compliance therefore includes cooperating accurately with investigations and implementing promised remedies, not merely correcting the original practice once scrutiny begins.

The digital-markets regime contains similarly powerful incentives. An SMS undertaking that breaches a conduct requirement can face a fixed penalty of up to 10% of worldwide turnover, and breaches of orders or commitments can generate daily penalties of up to 5% of daily worldwide turnover. For globally scaled technology groups, those ceilings represent substantial GBP-equivalent exposure, so compliance with market-opening obligations cannot rationally be treated as a routine operational cost.

Penalties need not approach the statutory ceiling to affect behaviour. The AA's £4.2 million sanction, Marks Electrical's £720,000 penalty and StubHub UK's £889,200 penalty were all discounted for early settlement, yet still accompanied by refunds and corrective obligations that outlasted the headline figure. The economics reward credible compliance systems twice: first by reducing infringement risk, and secondly by improving an organisation's ability to detect and correct problems before regulatory exposure escalates further.

Corporate Governance and Compliance

Consumer compliance can no longer sit exclusively within a legal department. Commercial teams may control pricing architecture, marketing may review it, product managers may own websites, agencies may run advertising, and data scientists may run recommendation systems. Each function can create evidence relevant to a CMA investigation, so boards and executive committees need assurance that legal requirements translate into operational controls, ownership, testing and escalation processes across the complete digital customer journey.

Governance should begin with clear accountability. Organisations need named owners for headline pricing, mandatory fees, optional extras, review moderation, promotional claims, subscriptions and cancellation processes. Material changes should be reviewed before release and monitored afterwards, because dynamic websites can behave differently from approved screenshots or specifications. Audit trails should record who approved a claim, what evidence supported it, how an algorithm was tested, and whether complaints revealed a failing control.

Third-party technology does not remove responsibility. Retailers may use external checkout software, review platforms, advertising tools, payment services or AI applications, yet the consumer experiences the resulting journey as part of the trader's offering. Procurement therefore becomes a compliance function: specifications should define lawful defaults, pricing visibility, data access, testing rights, and change-control obligations, and contracts should allocate responsibility for correcting defects without assuming liability can be outsourced.

Ongoing supervision matters as much as headline penalties. The CMA has reported that around 90% of businesses it contacted about fake reviews changed their behaviour, evidence that guidance, advisory letters and sector sweeps can shift practice well beyond the handful

of organisations formally investigated. A mature compliance programme should therefore track that broader supervisory activity, rather than waiting for a formal infringement notice before reassessing commercial practices.

Artificial intelligence adds another governance layer because pricing, recommendations and promotional content can increasingly be generated or adjusted automatically. A model may optimise conversion rates without understanding that a scarcity message lacks evidential support or that personalised wording creates a misleading impression. Human accountability remains essential: organisations need controls over training data, prompts, deployment objectives, approval thresholds and override mechanisms wherever automated systems influence consumers' transactional decisions.

Artificial Intelligence and AI-Assisted Selling

Artificial intelligence is moving from analytical support into direct commercial interaction. Businesses already use AI to answer customer queries, recommend products, process refunds and manage marketing campaigns, while agentic systems can increasingly plan and take actions with limited human intervention. On 9 March 2026, the CMA published dedicated guidance for businesses using AI agents, reflecting a market in which automated systems may increasingly shape purchasing decisions, contractual choices and customer outcomes.

The CMA's central principle is deliberately straightforward: consumer law does not change because an organisation substitutes software for an employee. A business remains responsible for what its AI agent does, even when a third-party developer designs or supplies the technology. If an agent misleads consumers, withholds material information or unfairly pressures them, enforcement can follow against the business using it, with potential penalties reaching 10% of worldwide turnover and consumer redress.

Transparency becomes especially important where a consumer might mistake an automated system for a person or misunderstand its capabilities, and CMA guidance advises businesses to consider whether an agent should be identified as such. Organisations should also avoid exaggerating what AI can do or obscuring how a comparison tool works, disclosing how much of a market it searched, what data it examined, how it ranked options, and what commercial relationships shaped the result.

The commercial opportunity remains considerable. DSIT estimated that UK AI companies generated £23.9 billion of revenue in 2024, up 68% from 2023, while AI-related employment reached 86,139, with Amazon, Google DeepMind, IBM and Meta among the organisations contributing substantially to that growth. As adoption spreads through retail, financial services and travel, compliance-by-design will increasingly determine whether automated selling builds confidence or generates scalable consumer harm.

AI, Personalisation and the Future of Consumer Manipulation

Personalisation can make digital markets more useful by reducing search costs and presenting relevant products, but the same capabilities can be used to influence consumers with increasing precision. Recommender systems may combine browsing histories, previous purchases, location, demographic information and engagement data to determine what consumers see and when they see it. The CMA has long recognised that algorithms can personalise rankings, promotions, notifications and prices, creating benefits while also increasing the potential for manipulation.

Personalised pricing requires careful distinction from dynamic pricing. Dynamic pricing adjusts prices rapidly in response to conditions such as demand, capacity or timing; personalised pricing may instead use information about an individual to estimate willingness to pay. Neither practice is automatically unlawful, but transparency, fairness and data-protection requirements can become relevant. The CMA warned in 2025 that increasingly sophisticated AI could make dynamic pricing more prevalent and complex, strengthening the need for clear customer communication.

Agentic AI could take persuasion further by negotiating, recommending and acting autonomously on behalf of sellers or buyers. The CMA expressly warns that an agent which steers, pressures or misleads consumers in ways that harm their economic interests is likely to breach consumer law. A sales system optimised solely for conversion could learn behaviours that outperform safer alternatives while producing misleading scarcity or excessive pressure unless objectives and outputs are properly constrained.

The competitive consequences can extend beyond individual transactions. Recommendation engines decide which products receive visibility, while personalised rankings can favour higher-margin offerings, affiliated suppliers or paid placements. Smaller businesses may struggle to reach customers if opaque systems consistently privilege established participants. The regulatory challenge is dual: ensuring personalisation does not manipulate consumers unfairly while preventing algorithmic gatekeeping from becoming an entrenched competitive advantage in its own right.

Most shoppers will never know why they were shown a particular price, product or countdown clock. That invisibility is not a side effect of personalisation; it is close to the point of it, since a system that reveals its own persuasion tends to work less well on the people subjected to it. Regulating something designed not to be noticed is a genuinely different task from regulating a misleading advertisement placed in public.

Innovation Versus Regulation

Regulation inevitably creates costs. Large technology businesses may need new compliance teams, technical controls, audit processes and legal review, while smaller suppliers can face proportionately heavier burdens when interpreting unfamiliar rules. Excessive intervention could also reduce incentives to test new products or business models if organisations expect lengthy approvals or unpredictable obligations, concerns that are particularly acute in AI, where product cycles can be measured in weeks rather than years.

The counterargument is that weak competition and low consumer trust can suppress innovation just as effectively. A dominant gateway may prevent challengers from reaching customers, while deceptive interfaces or unreliable AI can make consumers less willing to adopt unfamiliar technologies. The CMA's 2026–29 strategy therefore links effective competition with productivity, investment and innovation, arguing that clear rules can help legitimate businesses compete fairly while protecting households from exploitation and avoidable economic harm.

The scale of the wider opportunity makes that balance consequential. DSIT identified 5,862 UK AI companies in 2024, 58% more than in 2023, with an estimated £11.8 billion of gross value added attributable to the sector. Dedicated AI companies attracted around £2.9 billion of investment over the same period. Regulation that unnecessarily slows this ecosystem could impose real economic costs, while ineffective regulation could allow market concentration to harden just as quickly.

Government policy also shows that regulation sits alongside substantial efforts to stimulate growth. By January 2026, the Government reported completing 38 of the AI Opportunities Action Plan's 50 actions. Five AI Growth Zones had been designated, Isambard-AI had launched at the University of Bristol, up to £250 million was earmarked for additional cloud capacity, and a Sovereign AI Unit was established with backing of up to £500 million.

The CMA has responded by emphasising pace, predictability, proportionality and process, collectively described as its "4Ps". The approach is intended to minimise unnecessary burdens, engage businesses early and select interventions capable of producing benefits without overreaching. That does not remove disagreement about individual decisions, but it acknowledges a central economic reality: regulation can itself influence investment decisions, so credible digital policy must weigh the harm of inaction against the cost of intervening at all.

Sustainable innovation consequently depends on more than regulatory restraint. It requires

markets where new entrants can reach customers, consumers can trust digital transactions, and successful businesses can invest without arbitrary rules. The DMCCA's challenge is to preserve those conditions simultaneously: targeted intervention that lowers switching barriers and improves transparency can support innovation, while poorly calibrated intervention could raise costs and discourage the experimentation the strategy is meant to protect.

Corporate Power in the Digital Economy

Corporate power in digital markets increasingly depends upon control over gateways rather than ownership of a physical asset. Search rankings determine visibility; app stores determine distribution; operating systems determine technical access; marketplaces determine presentation; and data determine how effectively services learn and personalise. Defaults can channel millions of users towards one option without explicit exclusion, which is precisely the kind of influence the DMCCA was built to address.

Google and the Apple and Google mobile designations, both examined earlier, illustrate the point at the consumer end of the economy: a handful of gateways can shape how hundreds of thousands of businesses reach their own customers. The Microsoft investigation extends the same logic into the workplace, asking whether productivity software, operating systems and security tools can collectively create dependency even where several competing products remain theoretically available on paper.

Consumer-facing rules address another dimension of power: the ability to shape choices at scale. A misleading price, false review, pre-selected charge or manipulative countdown timer can be replicated across millions of transactions almost instantly, and AI makes that capability even more powerful because messages and offers can be personalised automatically. Regulation therefore reaches not only market structure, but the digital mechanisms that organise attention and purchasing decisions.

The resulting framework is broader than conventional ideas of monopoly control. The DMCCA examines who controls access, information, data, interfaces and the rules governing participation, while retaining legal thresholds and proportionality safeguards before its stronger powers apply. Corporate size remains relevant, but scale alone is not the issue; the deeper concern is whether control over important gateways lets an organisation shape outcomes that normal market pressure cannot adequately discipline.

What the Act Means for Business Leaders

For business leaders, the practical implication is that digital compliance must be designed into products rather than reviewed only after launch. Boards should understand which services depend upon personalised pricing, recommender systems, reviews, subscription mechanics, automated marketing or AI agents. Senior management does not need to supervise every interface decision, but it does need assurance that accountable owners, testing standards and evidence trails exist for customer-facing systems carrying material legal or reputational risk.

Third-party oversight is equally important because outsourcing technology does not outsource legal responsibility. Procurement teams should examine how suppliers generate recommendations, process customer data, moderate reviews, vary prices and update models after deployment, with contracts addressing transparency, audit access, incident notification and evidence retention. Where an AI agent interacts with consumers, the CMA specifically warns that responsibility remains with the business using it, even where another organisation built the technology.

Leadership should treat both algorithmic testing and regulatory engagement as part of ordinary resilience planning. Organisations may need pre-deployment scenario testing, monitoring of live outcomes and documented thresholds for intervention, since evidence should show how a system actually behaved rather than merely that it was intended to comply. Businesses that can rapidly reconstruct decisions and explain system logic are consistently better placed to respond when complaints or investigations arise.

The Future of UK Digital Regulation

UK digital regulation is becoming a network rather than a single regime. The CMA now combines SMS powers with direct consumer enforcement, while Ofcom administers the Online Safety Act 2023, the ICO oversees data protection, and the FCA regulates conduct in financial services. Through the Digital Regulation Cooperation Forum (DRCF), these authorities coordinate work where algorithms, platforms, advertising, personal data, consumer protection and competition increasingly overlap within the same products.

The Online Safety Act adds an important parallel layer. Ofcom published its register of categorised services on 30 June 2026, identifying major platforms subject to additional transparency, accountability and user-choice duties, and its July 2026 consultation covers matters including user empowerment, identity verification and fraudulent advertising. The same recommender systems that influence competition and purchasing can therefore attract separate scrutiny because they also shape exposure to content and safety risks.

Data governance is evolving alongside platform regulation. The Data (Use and Access) Act 2025 amended the UK data-protection framework and created a more permissive basis for some solely automated decisions while retaining safeguards, including information, opportunities to make representations and access to human intervention for significant decisions. For AI-driven businesses, commercial optimisation can therefore engage consumer, competition and data-protection obligations simultaneously, making regulatory mapping essential before deploying automated systems at scale.

Artificial intelligence will intensify these interactions further. The AI Security Institute researches risks from advanced systems but is not itself a regulator, while sector regulators apply existing and newer legal powers within their respective remits. The CMA's agentic-AI guidance, discussed earlier, demonstrates how general consumer law can govern emerging technology without waiting for bespoke legislation, and future questions will include autonomous purchasing and machine-to-machine negotiation.

Near-term milestones will test the framework's coherence. The CMA expects to conclude its Microsoft investigation by February 2027, while the dedicated DMCCA subscription-contract regime is anticipated to commence in spring 2027. Ofcom continues implementing enhanced duties for categorised online services over the same period. Each development adds another operational layer for organisations whose products combine platforms, subscriptions, personal data, advertising and AI capability, increasing the value of coordinated guidance and proportionate sequencing between regulators.

The central challenge will be keeping regulation technologically durable. Rules tied too closely to today's interfaces can become obsolete as voice assistants, autonomous agents and new distribution models emerge. Principles on fair dealing, transparency, contestability, and consumer autonomy offer greater adaptability, but only if enforcement remains predictable, depending on continued collaboration among regulators, businesses, and technologists to identify genuine harms without treating every technological change as a separate prohibition.

Summary -- Rebalancing Digital Markets

The DMCCA marks a shift in how the United Kingdom responds to economic power in digital markets. Rather than relying solely on retrospective competition cases or individual consumer claims, it combines targeted regulation of strategically powerful digital activities with stronger competition tools and direct consumer enforcement. The underlying principle is both preventative and remedial: intervention can address market conditions and commercial practices before harm becomes embedded at scale.

That shift reflects digital market economics. Network effects, data advantages, defaults, ranking systems, app distribution and ecosystem integration can create power without traditional ownership of a physical bottleneck. Search, mobile platforms, cloud services and enterprise software demonstrate how access to customers increasingly depends upon digital

infrastructure controlled by comparatively few organisations, and the SMS regime responds by focusing on strategic activities where statutory tests for entrenched power are satisfied.

Consumer protection has undergone an equally important transformation. The CMA can now investigate, decide infringements, impose directions, obtain redress and levy penalties reaching 10% of worldwide turnover for relevant breaches. The AA, Marks Electrical and StubHub cases together show how apparently modest charges can generate substantial penalties and refunds once repeated across thousands of transactions, turning pricing, reviews, interface design and consent mechanisms into enterprise governance issues rather than peripheral compliance matters.

Artificial intelligence extends that logic into future commerce. AI agents may recommend, negotiate, sell, refund and communicate with consumers, but responsibility remains with the organisations deploying them. Personalisation can improve relevance and efficiency, yet it can also increase the capacity to steer behaviour or invisibly optimise persuasion. The future regulatory question is therefore not simply what an algorithm decides, but whose commercial interests it serves and how transparently it discloses its influence to the people it affects.

Rebalancing digital markets does not require choosing between innovation and regulation. Competitive access, consumer confidence and predictable rules can themselves support investment and experimentation, while disproportionate intervention can impose real costs. The enduring task is to preserve the benefits of scale and technological progress without allowing control over gateways, data or interfaces to become immune from competitive pressure or consumer accountability, with earlier intervention and proportionality at the centre of that balance.

Additional articles can be found at [Procurement and Supply Chain Management Made Simple](#). This site looks at procurement and supply chain management issues to assist organisations and people in increasing the quality, efficiency, and effectiveness of their product and service supply to the customers' delight. © Procurement and Supply Chain Management Made Simple. All rights reserved.

Further Reading

- Digital Markets, Competition and Consumers Act 2024, legislation.gov.uk
- Competition and Markets Authority, “Digital markets competition regime: guidance on the CMA’s approach”, gov.uk
- Competition and Markets Authority, case page: “Google’s general search and search advertising services”, gov.uk/cma-cases
- Competition and Markets Authority, case page: “Apple and Google mobile platforms”, gov.uk/cma-cases
- Competition and Markets Authority, case page: “Microsoft’s business software ecosystem”, gov.uk/cma-cases
- Competition and Markets Authority, “Price transparency guidance for businesses” (CMA209), November 2025
- Competition and Markets Authority, “Guidance for businesses using AI agents”, March 2026
- Competition and Markets Authority, Annual Report and Accounts 2025–26
- Competition and Markets Authority, “Digital advertising market study”, July 2020
- Department for Business and Trade, research on online pricing practices and drip pricing, gov.uk
- Department for Science, Innovation and Technology, “AI Sector Study” and UK Digital

and Technology sector economic estimates, gov.uk

- *Ofcom, “Online Nation” report and register of categorised services under the Online Safety Act 2023, ofcom.org.uk*
- *Office for National Statistics, “Retail sales, Great Britain” statistical bulletins, ons.gov.uk*
- *Data (Use and Access) Act 2025, legislation.gov.uk*
- *Whish, R. and Bailey, D., “Competition Law” (Oxford University Press, current edition)*

Gov.uk news releases:

- *“CMA orders the AA and BSM driving schools to refund learner drivers over drip pricing” (April 2026);*
- *“CMA fines Marks Electrical for unfair online pricing practices” (June 2026);*
- *“CMA orders StubHub UK to refund customers over hidden fees” (June 2026);*
- *“Court endorses CMA action as Emma Sleep agrees to change sales practices” (May 2026)*