CMS
law·tax·future

Gaming Risk

Spring 2025

Nadia Latti
Profile >

Sam Oustayiannis
Profile >

Joel Vertes
Profile >

*In **Gaming Risk*** we look at risks and challenges relevant to the billion-dollar global games industry. The games industry has grown rapidly in recent years, it is now at a point where consolidation is underway, and the industry has reached a level of maturity in respect of the size and professionalism of the companies involved. Games are increasingly becoming the dominant form of entertainment and it can be easy for those outside the sector to not fully appreciate its scale and reach, both culturally and economically.

It is time to reframe games as big business and address the risks that come with it. This selection of articles sheds light on familiar and less-known risks, offering insights and guidance based on our experience. We aim to alert you to challenges early, allowing you to implement strategies to identify or deter those risks.

We hope you find this publication insightful and informative. If you have any questions or would like to discuss any of the topics in more detail, please don't hesitate to reach out to our team. We're here to partner with you in navigating the complexities of the evolving and maturing games industry, to ensure your business thrives in this environment.

AUTHORS

Sam Oustayiannis
Profile ›

Sarah Hopton
Profile ›

Carter Rich
Profile ›

Is it game over or the next level?

The risks of AI implementation in the gaming industry

Artificial intelligence ("**AI**") has become a cornerstone of innovation for many industries, including the gaming industry. AI has existed in various forms for decades, with one of the first examples of AI being the mathematical game *Nim* in the early 1950s. Although AI is not new to the gaming industry, recent advances in generative AI have the potential to transform how games are developed and experienced. For example, generative AI can enhance the player experience, streamline the development process and create safer environments for players through algorithmic monitoring of in-game chats and interactions.

It is important that game publishers are aware of the legal and commercial risks associated with generative AI. This article provides a high-level summary of some of the key risks associated with generative AI along with some potential mitigations (with references to AI in the rest of this article meaning generative AI).

Play by the rules: Potential risks of non-compliance with legislation:

EU AI Act

The EU AI Act came into force in August 2024, with some obligations starting to apply from as early as February 2025. It takes a risk-based approach, with certain AI systems banned altogether, and different obligations applying for different risk categories.

For example, certain transparency obligations would apply where a chatbot is used to enable non-player characters ("**NPCs**") to interact directly with individual players or where AI systems are used to generate image, audio or video content constituting a deep fake (which can reduce the costs of producing a virtual character based on a celebrity). Emotional AI is already used by some in the gaming industry to recognise a player's emotions and adapt gameplay accordingly; under the EU AI Act, this is likely to be subject to obligations for high-risk AI systems as well as transparency obligations.

The EU AI Act has extra-territorial scope, so can apply to UK businesses in certain circumstances. Failure to comply with the EU AI Act can lead to fines of up to 7% of total worldwide annual turnover. Game publishers and developers will need to assess the extent to which they need to comply with the EU AI Act and prepare for compliance accordingly.

UK AI legislation

In contrast with the EU, the previous UK government did not put in place AI-specific legislation and instead proposed a sectoral approach to regulating AI, which was still in its relatively early stages when the general election was announced. The new UK government announced in July 2024 that it intends to introduce AI legislation to impose requirements on those entities developing "*the most powerful artificial intelligence models*", although the draft AI legislation has not been published yet. Instead, the UK government ran a consultation on copyright and AI between December 2024 and February 2025.

As a result, the UK government stated in February 2025 that any AI legislation would not be published before all evidence (including responses to the consultation) had been considered. (A private member's bill on AI has been reintroduced in the House of Lords, although it is unclear if this will survive scrutiny by the House of Commons. Some AI-related provisions were also added by the House of Lords into the draft Data (Use and Access) Bill, but the removal of these provisions has already been proposed and will be debated during the House of Commons Committee stage.) Game publishers and developers will need to monitor AI-related regulatory developments and assess the extent to which they need to comply with any new AI-related requirements.

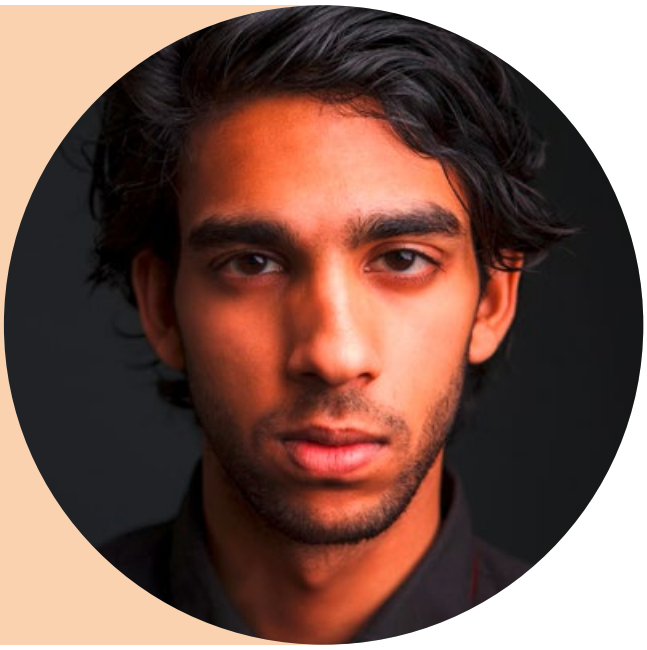
AI fallout:
Risk of reputational harm

The use of AI may enable a more immersive gaming experience, for example, by using AI to generate reactive and dynamic NPC dialogue. However, there is a risk of hallucinations or bias within the AI system, which could result in offensive, inappropriate or harmful NPC dialogue being generated and could therefore cause the relevant game publisher or developer reputational damage. To mitigate this risk, game developers need to ensure that appropriate safety filters and guardrails are in place.

Pixel perfect:
Risk of image rights claims

There is no standalone image, publicity or personality right in the UK. However, there are a patchwork of laws on which individuals may try to rely in order to object to the unauthorised use of their name, image, likeness or voice in a game.

To mitigate this risk, game developers should ensure they have obtained appropriate permissions from all relevant individuals.



Copyright not found:
Risk of AI-generated output not being protected by copyright

Although using AI to generate code, content or assets for a game may reduce production costs, it is not yet clear whether AI-generated code, content or assets can be protected by copyright.

Under UK copyright law, where literary, dramatic, musical or artistic works are generated by AI in the absence of a human author, the author is taken to be the person "*by whom the arrangements necessary for the creation of the work are undertaken*". However, it is unclear how that should apply in practice, as different people may be involved at different stages of the creation process.

In addition, a literary, dramatic, musical or artistic work cannot be protected by copyright unless it is "*original*". This means the work must be the "*author's own intellectual creation*" and the author must have been able to stamp the work with their "*personal touch*".

It is not clear how literary, dramatic, musical or artistic works generated by AI would satisfy this originality requirement. For many of the people involved in the creation process, their contribution to the AI-generated work may be too remote to be considered a "personal touch". For the person providing the prompt, although their prompt results in the work being generated, it is not clear if this is enough for the resulting work to constitute their intellectual creation.

> **If AI-generated outputs cannot be protected by copyright, third parties may be able to use those outputs without obtaining consent from the relevant game developer. To mitigate this risk, game developers should keep AI-generated code confidential and impose contractual restrictions on the use of AI-generated content or assets.**

Objection!
Risk of third-party intellectual property infringement claims

There is a risk that code, content or assets generated by AI for use in connection with a game could infringe third-party intellectual property rights.

Game developers using (or allowing players to use) **non-proprietary AI tools** should make sure they have appropriate contractual protections from the relevant AI company in relation to potential third-party claims.

Game developers using (or allowing players to use) **proprietary AI tools** should make sure they can rely on appropriate exceptions or have obtained any necessary consents and, where possible, they have appropriate guardrails in place to prevent prompts resulting in third-party copyright infringement. In addition, game developers should have in place an internal company policy governing the use of AI in connection with game development.

For more articles on AI-related topics, including the interaction between AI and copyright and key considerations for internal company policies on AI, please visit our AI webpage.

TL;DR

AI, especially generative AI, is revolutionising the gaming industry by enhancing player experiences, improving development efficiency, and ensuring safer environments. However, AI adoption comes with legal and commercial risks.

Key concerns include: compliance with evolving regulations like the EU AI Act (which imposes transparency and risk-based obligations) and the UK's forthcoming AI laws, reputational risks if AI generates harmful content, potential image rights claims, and uncertainty around copyright protection for AI-generated works. Developers face the risk of third-party IP infringement from AI-generated content.

> **To mitigate these risks, game developers should implement safety filters, secure relevant permissions/ consents, stay updated on legal changes, and adopt robust internal policies around content ownership for AI usage in game development.**

AUTHORS

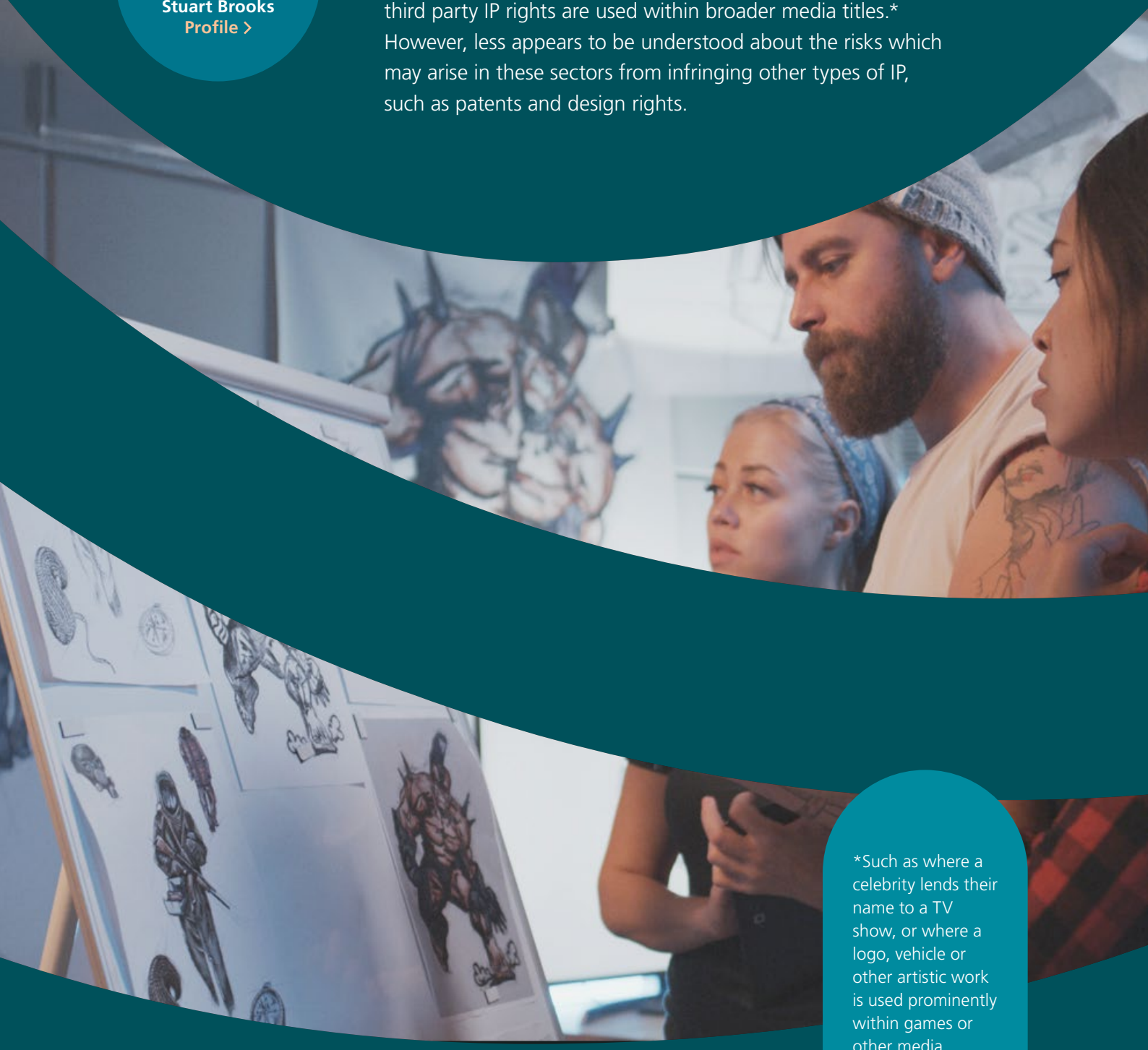
Caitlin Heard
Profile ›

Stuart Brooks
Profile ›

IP litigation levels up

The risk to gaming and streaming platforms in 2025

Most in the creative industries are aware that Intellectual Property ("IP") rights, such as copyright protection, can protect the work of authors, writers, designers and other creatives from being copied. Most will also understand the need to obtain a licence where third party IP rights are used within broader media titles.* However, less appears to be understood about the risks which may arise in these sectors from infringing other types of IP, such as patents and design rights.



*Such as where a celebrity lends their name to a TV show, or where a logo, vehicle or other artistic work is used prominently within games or other media.

We predict that gaming and media streaming platforms will become an increasing area of focus for patent litigation vehicles and for the enforcement of design rights.

As technologies like AI help rightsholders to detect potential claims, to evaluate their chances of success, and even to secure litigation funding far more easily than before, actors in these spaces should turn their focus to the threats of potential IP litigation, and consider whether they are doing enough to protect against the risks.

Patent battles:
The rising tide of patent litigation and licensing demands

Companies utilising streaming technologies to deliver content have seen a marked increase in the number of threats against them from patent portfolio owners, and there is an uptick in licensing approaches and patent litigation claims being brought against companies utilising streaming and content delivery technology. This uptick is being driven by a number of factors, but one of the primary drivers is existing serial licensors/ litigants looking to secure patent licensing revenue in new verticals coupled with divestment of portfolios.

Having amassed large portfolios of diverse patents in recent decades, these and other rights owners historically pursued telecommunications companies and mobile device makers.

The successful enforcement of their patent rights has secured lucrative licensing payments from, for example, the sale of mobile devices and networking equipment.

These companies are re-evaluating the strengths of their patent portfolios in other areas, and are looking for other ways to monetise their assets. Some have turned to media streaming technologies and to technologies underpinning interconnectivity within the automotive industry, but we predict that such cases are just the beginning.

Power-up:
The role of the UPC, SEPs and FRAND

The introduction of the Unified Patent Court ("**UPC**") in 2023 has streamlined the process of bringing a patent-based challenge in Europe. Data published by the UPC in November 2024 suggests that patents covering software and digital hardware technologies are the most popular class of patent relied upon in infringement actions, so those making use of such technologies may find themselves most at risk of a complaint.

Standard Essential Patents ("**SEPs**") play a crucial role in the current IP litigation landscape. Where patents protect technologies that are essential to meeting technical standards (i.e. the technology must be used to ensure interoperability with other systems) they must be licensed on Fair, Reasonable, and Non-Discriminatory ("**FRAND**") terms. The upside is that the party utilising the patented technology is protected from the threat of an injunction, but only if it is willing to negotiate towards taking a licence on FRAND terms.

In reality, agreeing to FRAND licensing terms is fraught with complexity. If you receive a letter demanding that you pay a FRAND licence fee to a patent holder, it can be challenging to evaluate the fairness of the offer and to negotiate for fairer terms.

Here's why

1 Unlike regular patents, SEPs cannot be designed around due to the need to adhere to technical standards, so those receiving a demand often have a weak negotiating position to start with.

2 The licensor will typically hold far more information about the fair market value of a particular licence than a would-be licensee, which has the potential to result in inflated pricing.

3 Challenging a FRAND offer often involves a lengthy court battle, with looming uncertainty and hefty legal costs.

Epic showdowns:
Key cases and the technologies under the spotlight

In recent years, patent portfolio owners have increasingly sought to enforce rights in cloud-based media storage and delivery, media streaming services, streaming hardware, audio streaming, video compression methodologies, and other interconnectivity technologies. Some examples include:

Nokia brought multiple patent infringement claims in 2023-2024, with one case resulting in in an injunction in Germany against Amazon, prohibiting the sale of Fire Sticks with High Efficiency Video Coding ("HEVC") technology. This injunction is currently being appealed.

Interdigital, traditionally a major player in the telecoms space, has shifted its focus to streaming, aiming for a $1 billion revenue target from streaming licensing.

Avanci has also launched 'Avanci Video,' a dedicated streaming technology licensing arm.

Adeia launched patent infringement proceedings in the US, targeting streaming apps, including Hulu and ESPN.

Given that the gaming sector has evolved to rely on many of the same technologies, could those bringing innovation to the world of games also be sleepwalking into a litigation minefield? And if so, what should gaming companies be prepared for?

Firstly, if a letter alleging infringement or seeking a licensing deal arrives, it is crucial not to ignore it, and to obtain legal advice before responding.

In the meantime, all companies focused on technical innovation should consider a robust patent risk management policy, which aims to minimise the inadvertent infringement of patents. Smaller companies may prefer to licence off-the-shelf technologies from companies who offer indemnification against patent infringement claims, particularly for the communication-focused technologies which have historically made up the bulk of patent claims, and are mentioned in the previous paragraphs.

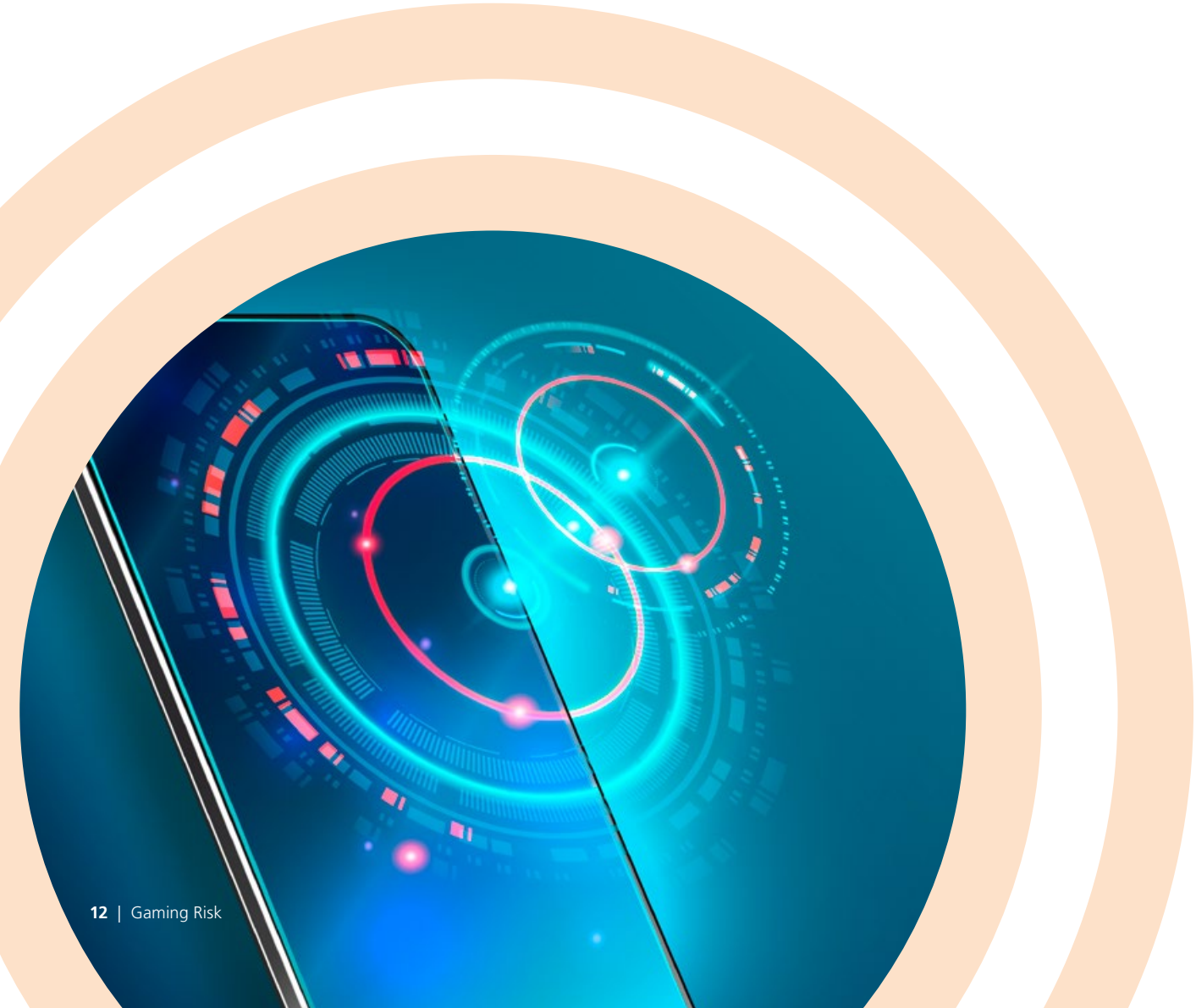
Unlocking the risks:
Infringement of registered designs for graphical user interfaces

In addition to patent litigation, gaming and streaming platforms face the risk of infringing registered designs, which can protect the visual depictions of characters, graphical user interfaces and other artifacts used within the gaming and wider media sector.

There has been a notable increase in the number of designs filed for the look and feel of casual mobile games and of key user interface elements within games. This indicates that many key players in this space see the value in registering their design rights, paving the way for a future involving the greater enforcement of these rights.

The uptick in activity at design registries underlines the importance of ensuring that when new games are designed, they do not borrow too heavily from earlier released titles.

Alternatively, where game creators or their investors detect some inspiration has been drawn from a competitor, it is also worth performing searches of prior registered designs which can help to understand the rights a competitor may be able to assert. This can be a complex process due to the different rules in force around the world, but is an important risk mitigation step. Larger game developers may also wish to evaluate their own design registration strategy and to consider the merits of increasing the size of their design portfolio. Much like patents, parties with large portfolios may be able to use them to improve bargaining power in the event of a claim. Chinese applicants are particularly alive to the power of design registrations, frequently topping the lists of most-filed design applications at IP registries around the world. Their western counterparts may wish to consider levelling up or risk falling behind.



Endgame:
Navigating the evolving landscape of IP litigation in gaming

The IP litigation landscape in 2025 presents significant risks for gaming and streaming platforms:

The aggressive strategies of patent portfolio owners, the rise of SEPs and FRAND terms, and the establishment of the UPC are key factors which have driven the current increase in patent litigation.

Rightsholders have already turned their attention to media streaming companies, and since the gaming sector shares key technologies with the media streaming services, it may be next in the firing line.

Similarly, those working in these creative sectors should remain alive to the risk of design right infringement, as well as the traditional copyright, trade mark and patent infringement risks.

As parties put renewed energy into protecting the unique visual and interactive elements of digital products through design registrations, an increase in attempts to enforce those rights is likely to follow.

By staying informed and proactive, gaming and streaming platforms can navigate these challenges and mitigate the risks associated with IP litigation.

TL;DR

Gaming and media platforms are likely to see an increasing amount of IP litigation, particularly concerning patent and design rights infringement.

As technologies evolve, patent portfolio owners are shifting their focus from telecoms and mobile device companies, leading to an increase in licensing demands and patent litigation claims being brought against media streaming and gaming technologies.

The introduction of the Unified Patent Court in 2023 has streamlined patent challenges in Europe, with software and digital hardware technologies being the most common patent class relied upon in infringement actions.

Additionally, we anticipate a growing trend in the enforcement of registered designs, especially for graphical user interfaces and visual elements in games.

> **Companies in these sectors should adopt robust IP risk management policies and evaluate their design registration strategies to mitigate these risks.**

AUTHORS

Tim Sales
Profile >

Carter Rich
Profile >

Andrew Wilson

UK regulators step up their game

Analysing the impact of growing regulation in the video games industry

The past few years have seen significant development in the level of regulation placed on the games industry. This trend continued in May 2024 with the introduction of the Digital Markets, Competition and Consumers Act (the "**DMCC**"), with many provisions coming into force next month. Whilst it might not be as headline-grabbing as the EU AI Act, or as well publicised as the UK's Online Safety Act, the DMCC might yet become the one of the most impactful pieces of legislation for the UK games industry in recent years.

Within the context of increasing to consumer protection in UK legislation, the DMCC represents a further tightening of the regulatory landscape and a game-changing development in the Competition and Market Authority's powers.

In this article we consider the steps you can take to ensure you comply and make the regulatory environment work for you.

Unfair commercial practices: DMCC's Consumer Regulations

Banned practices

One of the key functions of the DMCC is the migration of the rules in the Consumer Protection from Unfair Trading Regulations 2008 (the "**CPRs**"), including the list of banned practices, which are considered unfair *under any circumstances*. The DMCC has added a number of new practices to the banned list, including:

— **Drip pricing and pricing transparency:** The DMCC specifically calls out the importance of pricing transparency, clarifying rules on "drip pricing" (where a customer is shown an initial price prior to purchase, and is then faced with unavoidable further charges once they have committed to the purchase). Businesses must state the total price of a transaction, including any mandatory additional fees. Whilst not yet tested, this could mean that games featuring a virtual currency could need to display prices for in-game items in fiat currency (as well as the virtual currency).

— **Fake reviews:** The DMCC also cracks down on the creation or commissioning of fake reviews of products or services and the publication of fake reviews without first taking reasonable and proportionate take steps to avoid them. The CMA has issued and consulted on draft guidance on what 'reasonable and proportionate' means in this context, with finalised guidance expected by April 2025.

> **The banned practices set out in the DMCC are treated as strict liability offences, meaning that there is no need to prove consumer harm for companies to be found in breach.**

Crucially, in order to give the regulations more flexibility to react to market changes, the DMCC gives the Secretary of State powers to add to the current list using secondary legislation. This means that businesses will need to stay on top of any changes to ensure that their commercial practices remain compliant as the DMCC continues to evolve.

Subscription Provisions

In a market in which subscriptions are so common, the DMCC's focus on increasing transparency in subscription services will be significant. Given the seismic shift with the new subscription rules, they will not be coming into force until 2026 at the earliest.

Guidance is still awaited, meaning planning for compliance is still very challenging, but in summary, the new provisions include:

Pre-contractual requirements:
Companies will be required to provide clear and accessible information to consumers before they enter a subscription contract, such as details of the amount and frequency of payments (including the minimum amount payable), costs to apply after the end of a free (or discounted) trial period, details of auto-renewal mechanisms and instructions on how to terminate contracts.

Renewal reminders:
Companies must provide customers with reminders prior to renewals, clearly stating the cost of the renewal payment, the date on which payment will be taken, any changes from the cost of previous renewals, and cancellation options.

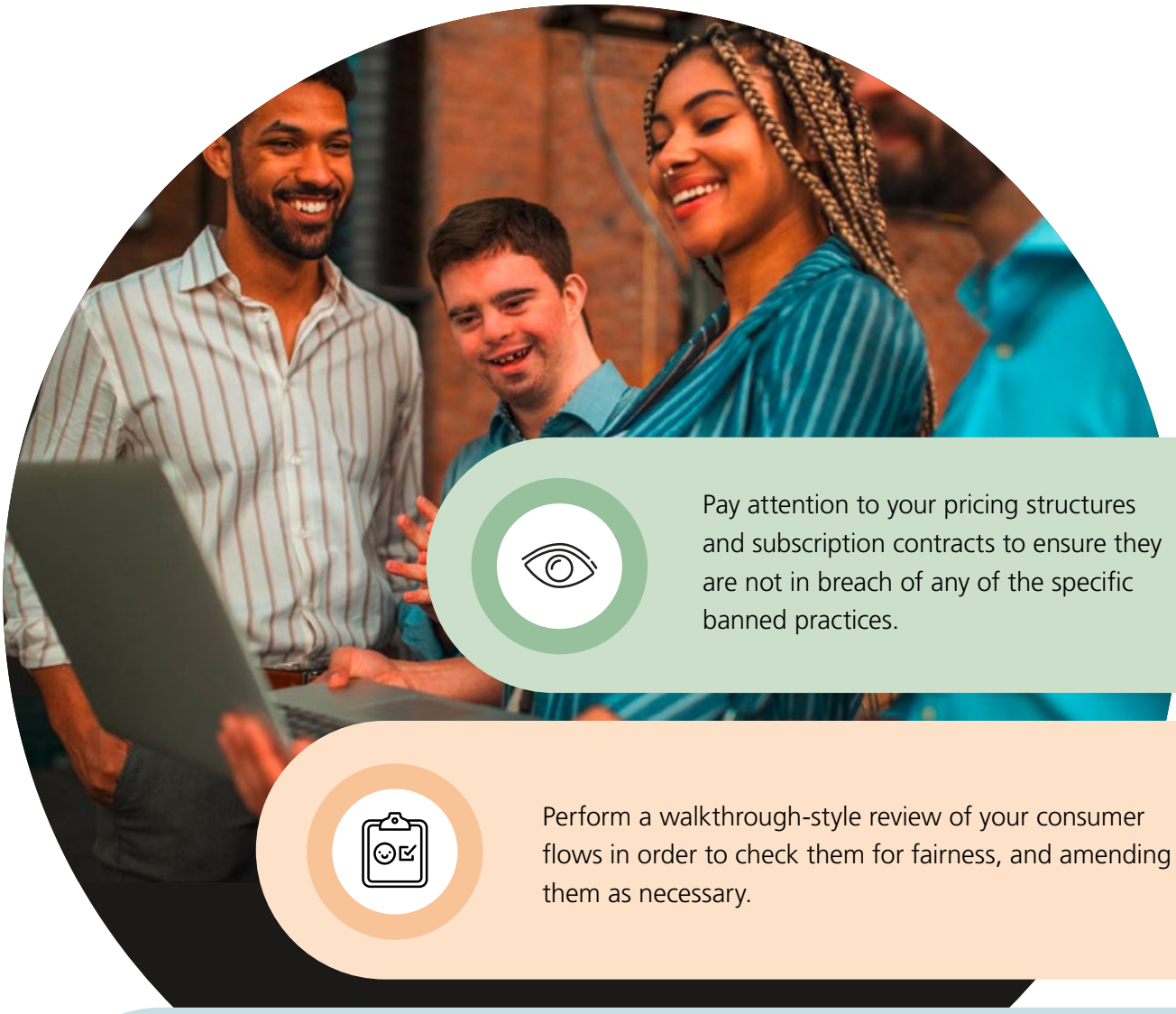
Cancellation and cooling-off rights:
Companies must make it possible for subscriptions to be cancelled through a single communication in a "straightforward" manner. Consumers will also have a 14-day cooling off right following the start of the contract, after any free or concessionary trial period, and at the start of any renewal period of more than 12 months.

Potential consequences of non-compliance

Under the DMCC, the CMA has new powers to directly enforce non-compliant commercial practices. It can, without having to go to the courts, decide for itself whether consumer protection laws have been broken, give directions (e.g. changes in behaviour/practices going forwards), impose redress (e.g. consumer compensation schemes) and levy substantial fines of up to 10% of the business's global annual turnover or £300,000 (whichever is higher). Appeals of the CMA's decisions will be heard by the High Court.

Staying ahead of the game:
How the games industry can stay compliant

In light of the new regime implemented by the DMCC, businesses will need to stay aware to stay ahead. It is important to remember that whilst there will not be significant changes to the substantive law, there will be major changes to its enforcement and we therefore recommend that businesses:



Pay attention to your pricing structures and subscription contracts to ensure they are not in breach of any of the specific banned practices.

Perform a walkthrough-style review of your consumer flows in order to check them for fairness, and amending them as necessary.

Consider introducing more opportunities for consumer engagement, collaboration with other platforms, and working alongside indie developers. In addition to the direct benefits of doing so, this will align with the aims of the DMCC and keep you ahead of disruptive interventions.

There have been several consultations on the DMCC including two major consultations on draft guidance published by the CMA; the first in relation to the direct consumer enforcement guidance and rules permitted under the DMCC and the second on the DMCC's unfair commercial practices provisions. Whilst both consultations are now closed, reviewing the CMA's updated and final versions when they are released will help you to understand the regulators interpretation of the DMCC and how to implement the provisions in practice.

The Department for Business and Trade's consultation regarding the new regime for subscription contracts is also under review following the closing of submissions, with implementation expected not before Spring 2026.

The UK Government has already announced that the DMCC will be implemented in parts by various new pieces of secondary legislation over the next few months and years. The first of these, focused on empowering the CMA to carry out investigations into potentially anti-competitive behaviour by companies with SMS, has already been implemented. The next phase, including both unfair commercial practices and new enforcement regime, will come into force on 6 April 2025.

TL;DR

The UK gaming industry is facing tougher regulations under the DMCC which come into effect in April 2025.

The CMA now has extra muscle to enforce rules such as a ban on drip pricing, where customers are initially shown a low price but are later hit with additional fees, and a crack down on fake reviews.

New subscription rules won't take full effect until at least 2026, but will require clearer information upfront, renewal reminders, and hassle-free cancellation options.

Non-compliance could lead to hefty fines of up to 10% of global turnover or £300,000, with the CMA able to enforce charges without going through the courts.

> **To stay ahead, gaming companies must review their pricing, subscription models, and consumer practices and, with the DMCC rolling out in phases, it's essential to stay on top of the ongoing legislation to avoid penalties down the line.**

AUTHORS

Nadia Latti
Profile ›

Alex Danchenko
Profile ›

Legit OP strats

Powerful weapons of the English court to protect and preserve gaming assets

As the games sector grows and matures, the risk posed by wrongdoers will need to be met by an increasingly sophisticated response, including utilising powerful tools available from the English courts. We outline some of the heavy-hitting options available from the courts that can be mobilised to protect intellectual property and confidential data or used to unmask perpetrators hiding behind pseudonyms and anonymous accounts.

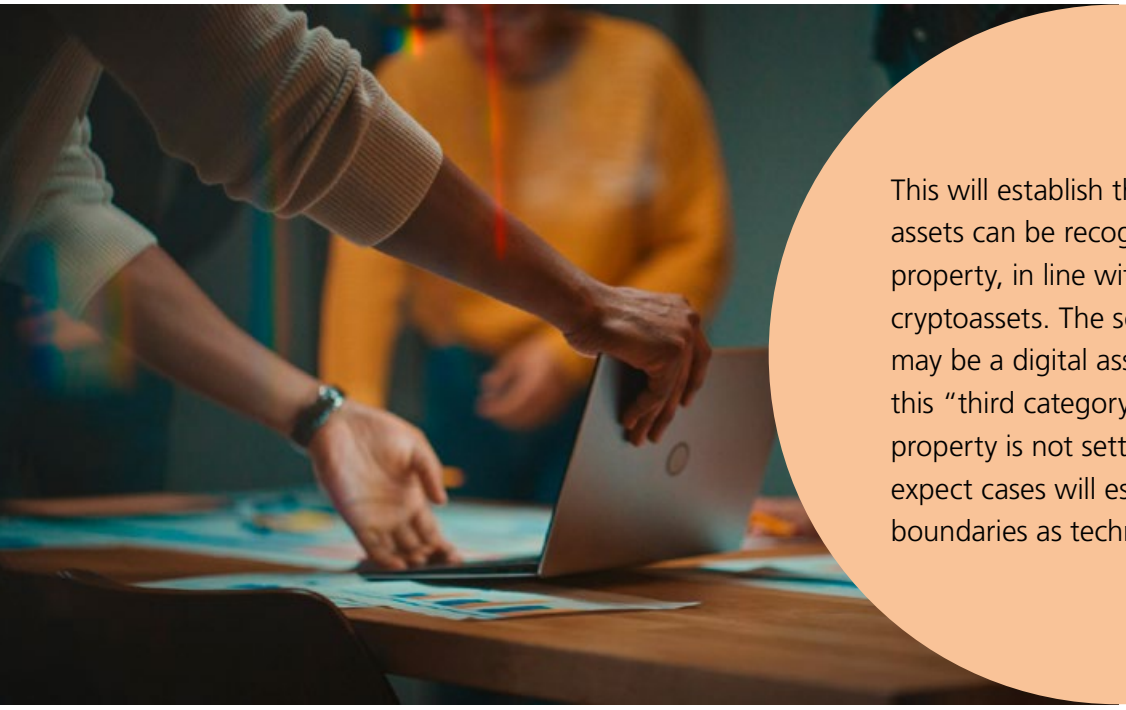
Leaks are almost predictably commonplace now, particularly regarding hotly anticipated releases or where a game ecosystem contains valuable in-game assets. It does not have to be a mysterious hacker or even any external hostile agent – the more global and successful the industry becomes, the more vectors there are for leaks, breaches of confidentiality, siphoning of company property, and malicious breaches of terms of service. Some reported examples of damage caused to game ecosystems include leaks by a QA contractor, streamers, and cheaters: both software distributors and end users. The causes of action in these cases are many and varied, reflecting the developing state of jurisprudence in this area.

Some insight into the future of litigation in England can be gained by looking at the body of law relating to cryptocurrency. Over half of the issued claims involve alleged fraud, hacks or otherwise missing assets and of the cases that have proceeded to judgment, an overwhelming majority have been judgments on applications for interim remedies such as injunctions, most of which were unopposed.* As the legal position in relation to digital assets becomes clearer, it is likely that we will see more cases expanding on this area of law.

For matters that have a connection to England, the law here provides a powerful array of investigatory and enforcement tools which can be used both to stop ongoing infringement of rights, as well as to pursue the wrongdoers, both in England and abroad.

While some of these weapons – such as injunctions – may be a final remedy, very often they are used as emergency or interim measures to stop a bad actor from concealing its identity, location and assets, as well as the location and movements of any misappropriated property.

*See CMS Crypto Disputes Report 2024 for further detail.



This will establish that certain digital assets can be recognised as personal property, in line with case law on cryptoassets. The scope of what may be a digital asset that falls into this "third category" of personal property is not settled and we expect cases will establish the boundaries as technology develops.

Piercing the fog of war: Information gathering

You may need more information to understand the scope of the issue you are dealing with, or to follow and retrieve assets that have been misappropriated. Information orders are powerful tools that can be used to compel disclosure of specific information or document relevant to a case or to recover materials from an alleged wrongdoer while your case is heard.

There are a range of options available to the English court to enable this:

1. Search and imaging orders

This is described as one of the "nuclear weapons" of the English court. They can allow an applicant to enter the respondent's premises to search for, copy, remove and detain documents, information or material (including from electronic devices, servers, social media and email accounts and so on).

> **The key driver behind such an order is *preservation* of evidence or property where there is real risk of it being destroyed or hidden away.**

While the threshold to get such an order is high (for instance, you will have to show that you are likely to have a very strong claim), the English courts are well-versed in handling cases where the evidence may be limited or circumstantial, which is often the case where wrongdoing is surreptitious and repeated, as is often the case with copyright infringement.

2. "Norwich Pharmacal" orders ("NPOs)

Sometimes the information you need is in the hands of a third party who has gotten mixed up in the wrongdoing. This could be a bank having information about the transfer of misappropriated funds, or an ISP holding information about pirated content or leaked information and you need this information to properly identify the defendants to your claim.

> **NPOs compel that third party to give you the missing piece of the jigsaw you need to start your action.**

Where there isn't a need for secrecy or urgency, information can be requested under voluntary disclosure, but often respondents are not able to provide disclosure unless subject to a court order, perhaps due to their own confidentiality obligations. The applicant for a NPO typically covers all costs of obtaining and also complying with the order. Non-compliance can be pursued as contempt of court, which can result in serious penalties including imprisonment and fines.

These orders can be of critical importance where you need more information to know who to sue or whether it is worth pursuing litigation in England, allowing you to make the best strategic decision at each stage of an unfolding situation.

Hitting the pause button
Injunctions

Injunctions are powerful tools in the English court's arsenal. They can be orders to not do, or to stop doing, a certain thing – such as stopping an ongoing infringement of intellectual property or contractual rights.

> **There are also other, more specific, powers to grant injunctions e.g., a website blocking order which has been successfully used in England to block users from accessing websites providing pirated copies of games*.**

The English court has a very wide discretion to grant an injunction in any case where it is just and convenient to do so, particularly where damages would not be an adequate remedy for the infringement – these are situations where, for example, the possible harm is existential to your company, or otherwise extremely serious and/or hard to quantify in monetary terms.

Some types of claims are more suited to seeking an injunction, like piracy, cheating and counterfeiting. Cases in the US – where the test for injunctions has similar requirements – include publishers and developers obtaining injunctions in respect of distributors of cheating software to stop its use.

> **One important point to note is that injunctions have been obtained against "persons unknown" – which is particularly common in cases involving cyber breaches and digital assets where pseudonyms and anonymous accounts are de rigueur. The case law in England is rapidly developing in this area, bolstered by cases dealing with crypto and other digital assets.**

*Copyright, Designs and Patents Act 1988, section 97A. This provision was the basis for the injunction ordered in *Nintendo Co. Ltd v British Telecommunications Plc et al* [2021] EWHC 3511 (Ch) in which six major UK broadband and mobile internet service providers were required to block or attempt to block access to two websites that infringed Nintendo's trademarks and copyright by offering pirated Nintendo games.

Sub-zero:
Freezing injunctions

When the purpose of litigation is to make a recovery and particularly when you have identified assets to enforce against, an important part of your litigation strategy may be to ensure those assets are still there at the end of your case. This is where a freezing injunction can come into play.

It is a distinct and extremely powerful interim remedy which aims at restricting the bad actor's ability to move and deal with assets, primarily to stop it from hiding or dissipating them, and thus making them available to the victim to claim against. Obviously, this would also prevent it from moving any assets misappropriated because of fraud.

Breaching such an injunction would be a contempt of court, which is potentially punishable by imprisonment, fines and other penalties.

The English court's powers when granting a freezing injunction are wide indeed: it may be given worldwide effect, apply to persons unknown, and cover cryptocurrencies and other digital assets. This is described as the other "nuclear weapon" of the English court. It will be unsurprising that there are several key – and often hard-to-meet – criteria one must meet to obtain such a draconian remedy.

Obtaining proper advice as to whether a freezing injunction is appropriate is therefore critical. It is a powerful tool that can be used to stop assets disappearing where they are the subject of further litigation, therefore making the litigation worthwhile. This can be an important step in an overall case strategy where enforcement is a goal.

Mastering the metagame:
Things to keep in mind when pursuing emergency measures

These are the big guns of the English court; asking for them to be used has many complexities which need to be considered. They also require resources, both in terms of legal spend and also the financial wherewithal to provide a "cross-undertaking in damages", which means the applicant is liable for any damages if it turns out they shouldn't have gotten the interim remedy in the first place.

> **Receiving robust legal advice early – about your options, but also your prospects – is important to arm you with the information you need to make the best decision, often in urgent situations with the need to move fast.**

Finally, many of the emergency measures described here may have extraterritorial effect and using such orders across several jurisdictions should be managed centrally to ensure steps are sequenced optimally to best achieve your overall strategic goals.

TL:DR

The English courts offer a range of powerful legal tools to respond urgently to protect gaming assets against threats such as theft of digital assets or intellectual property and breaches of confidentiality. These tools include search orders, freezing injunctions, and information orders.

The court has wide discretion to grant injunctive relief where traditional damages would not be an adequate remedy, which can be used to stop ongoing infringements and can even be granted against unknown persons, particularly useful in cases involving cyber breaches.

Freezing injunctions prevent bad actors from dissipating assets, and the court has wide ranging power to grant them worldwide ensuring that valuable assets remain available to enforce against.

Information orders, such as Norwich Pharmacal orders, compel third parties to disclose information necessary to identify wrongdoers or find the "missing piece of the jigsaw" before bringing a claim.

> **These measures, while effective, require careful consideration and robust legal advice due to their complexity and the financial implications of getting it wrong. The evolving legal landscape, particularly with the increasing value of digital assets, underscores the importance of these tools in safeguarding gaming assets.**

AUTHORS

Roman Hryshyn-Hryshchuk
Profile ›

Eoin O'Shea
Profile ›

Nadia Latti
Profile ›

Extra life

Sanctions compliance in the gaming world

In March 2022, one of the world's most popular blockchain games, Axie Infinity, became the centre of an international sanctions saga. Hackers later identified as North Korea's state-sponsored Lazarus Group infiltrated the game's blockchain system (the Ronin Network) and drained approximately $620 million worth of cryptocurrency. It was the largest virtual currency heist to date – a staggering sum stolen from a video game ecosystem.

The motive behind such audacious cybercrime soon became clear: under the chokehold of global sanctions, North Korea had turned to illicit digital activities to bankroll its regime. The U.S. Treasury confirmed that the DPRK, under pressure of sanctions, used the stolen crypto to support its weapons programme, laundering a portion through a virtual currency "mixer" service to cover their tracks (the U.S. Treasury later sanctioned the group and the mixer).

The Axie Infinity incident is but one example of the escalating risks posed by sanctions to the games industry. Beyond high-profile hacks, there are more insidious threats that can be equally consequential. Businesses that fail to spot hidden sanctions exposure can unwittingly become part of unlawful activity, exposing themselves to severe penalties. In a world where the games industry straddles multiple jurisdictions and involves multibillion deals, the stakes are higher than ever.

> **Sanctions are legal restrictions imposed by governments or international bodies to prohibit dealings with certain designated persons, entities, or countries.**

These designated targets might include terrorist organisations, oligarchs, or regimes such as Russia and North Korea under various sanctions programmes. In practice, if someone is on a sanctions list – for example, on the UK's consolidated sanctions list – it is generally illegal for UK persons to deal with their funds or provide certain services to them or persons owned or controlled by them. This prohibition applies not only within the territory of the UK, but also to UK persons overseas. Penalties for sanctions breaches can include hefty civil fines on a strict liability basis (meaning lack of knowledge about the sanctions breaches is not a legal excuse) and imprisonment.

At first glance, gaming might seem far removed from geopolitics and financial crime. Video games are about entertainment and community, and the rogue states and criminals are meant to be part of a story narrative only! Yet the industry's global, interconnected nature is exactly what makes it exposed to sanctions risks. Online games and esports platforms bring together millions of users from around the world – including regions or persons that may be subject to sanctions. This risk is then compounded by the often anonymous or pseudonymous way in which players interact in the game ecosystem. Without careful compliance policies and controls, a game company could easily find itself providing a service to a sanctioned market or individual or processing tainted funds.

Consider some real-world examples:

In 2019, U.S. trade sanctions forced a major American game publisher, Riot Games, to block players in Iran and Syria from accessing League of Legends. Practically overnight, gamers in those countries trying to log in were met with a message: "Due to US laws and regulations, players in your country cannot access League of Legends at this time."

More recently, the war in Ukraine and the resulting sanctions on Russia have put gaming firms in the crosshairs of compliance. Several games publishers have ceased all sales within the Russian market while streaming platform Twitch ceased payments to Russian streamers to align with sanctions regulations.

Esports tournaments and gaming events are not immune. Tournament organisers must be mindful if teams or players hail from sanctioned countries, or if sponsors and partners might be on sanctions lists. There have been instances of esports teams having to change sponsors because an owner was added to a sanctions list amid geopolitical tensions. For example, in 2022, a major esports organiser ESL banned teams like Virtus.pro and Gambit from its tournaments because of alleged ownership ties to sanctioned Russian entities.

Publishers, platform operators, payment providers, and investors in the interactive entertainment community are increasingly recognising that sanctions compliance has become a fundamental part of doing business internationally.

You cannot rest with enemies nearby

Not all sanctions risks are created equal. Some are explicit – clear-cut situations where a gaming company might knowingly or unknowingly violate sanctions law. Others are hidden – subtle, camouflaged threats that are easy to overlook without a proactive mindset.

Explicit risks are the straightforward ones.

For example, a game publisher might directly contract with a distributor in a sanctioned country, or an esports league might attempt to pay prize money to a team that happens to be owned by a person on a sanctions list.

Similar to the above examples, these are the scenarios most likely to raise red flags in legal departments, and usually avoided due to basic compliance checks. The key with explicit risks is awareness and having robust processes – knowing who and where your customers and counterparties are and having systems in place to identify and verify that information. If you fail to notice an obvious sanctioned party in your dealings, authorities will have little sympathy.

The hidden risks pose the trickiest challenges.

These involve dealings that on the surface look innocuous, but which may involve sanctioned persons or tainted funds underneath.

— **One major concern is the use of aliases and fake accounts.** When gaming, users routinely go by pseudonyms; a sanctioned individual can exploit this anonymity by creating an account under a false name and continuing to spend or receive money in-game. Without strong know-your-customer procedures, a company might not discover that "Player123" is actually a banned arms dealer.

— **Indirect ownership is another hidden risk area.** A gaming studio might take investment from a venture capital fund, only to later learn that half of that fund's money comes from a sanctioned oligarch. Or a tournament organiser might sign a sponsorship deal with a brand, not realising the brand is a front for a designated entity. UK sanctions laws account for this through the ownership and control test – if a sanctioned person owns more than 50% of an entity or directly or indirectly controls it, that entity is treated as sanctioned by law as well.

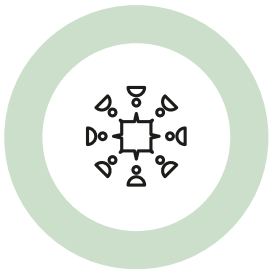
However, discovering these links goes beyond simple checks. Shell companies and complex corporate structures are common ways to mask true ownership, underscoring the need for enhanced due diligence and local legal advice as sanctions law varies between countries, requiring specific and informed consideration in each jurisdiction.

— **Then there are hidden financial flows through microtransactions or player-to-player trades.** Online games often involve thousands of small transactions – buying skins, weapons, loot boxes, and so on. A savvy launderer could intentionally make dozens of small purchases with illicit funds (staying under automated radar thresholds), then have another account sell items earned with those purchases to cash out clean money. Because each transaction is small, it might not trigger alerts the way a single large bank transfer would. Over time, though, the cumulative effect could be to wash a significant amount of dirty money through the game's marketplace. This risk is harder to detect, but it's very real – criminal enterprises have shown patience in exploiting systems through volume rather than single high-value moves.

Managing your quest log

Given the myriad risks outlined, what can gaming and esports companies actually do to protect themselves? The answer lies in treating sanctions risks as a strategic priority – building a compliance programme that is robust yet tailored to the unique contours of the gaming industry.

Here are some brief practical steps from business and legal perspectives:



1. Know your players and partners

Due diligence is your first line of defence. For players who transact on your platform – whether it's cashing out tournament winnings, trading high-value items, or buying lots of in-game currency – implement identity verification and sanctions screening. This can often be done using third-party compliance software that checks user details against updated sanctions databases. Likewise, vet your business partners: publishers, payment processors, sponsors, and suppliers. Before signing a contract, conduct background checks to ensure none of the entities or key principals are sanctioned or based in high-risk jurisdictions that can assist sanctioned persons in sanctions circumvention schemes.

2. Establish sanctions policies and training

A written sanctions policy tailored to the gaming context is essential. It should outline procedures for sanctions screening, how to handle a match with players from different countries, what to do if a user is found to be on a sanctions list (typically: freeze any funds and report to the relevant authorities, however some transactions can be still processed after obtaining a sanctions licence), and how to review any new features (like introducing an in-game cryptocurrency) for financial crime risks. Every relevant team should receive training on these policies, including marketing, finance, and development teams. Regular training ensures that employees remain alert to red flags; retaining records is also essential in case of future investigations.

3. Plan for the worst – incident response

Despite best efforts, mistakes or breaches can happen. What matters then is how you respond. Gaming companies should have an incident response plan for sanctions issues, similar to a data breach response plan. This includes steps like: immediate investigation of the issue, legal consultation, and having a communication strategy. Being prepared can turn a potential catastrophe into a manageable compliance incident. Regulators are often more lenient when a company can show it acted swiftly and responsibly upon discovering a violation.

Beyond legal advantage, implementing these measures may also create a competitive business advantage. It builds trust with payment providers, advertisers, and users. For example, banks and payment processors – which themselves must comply with sanctions – prefer to do business with a gaming company that they know has proper checks in place. A potential acquirer, in turn, will pay a premium for a gaming business that does not carry hidden liabilities like sanctions exposure. And in terms of brand integrity, avoiding scandals is obviously good for customer loyalty and broader market positioning.

Upgrading your base defences

The fast-paced world of gaming and esports might feel a million miles away from the sombre realm of international sanctions, but as we've seen, the two have increasingly intersected in surprising and consequential ways.

A blockchain game breach ends up financing a rogue state's weapons programme; global conflicts force studios to pull beloved games from entire countries; virtual currencies meant for fun become conduits for dirty money.

In this landscape, proactive compliance is not just about staying on the right side of the law – it's about the long-term sustainability and integrity of the gaming business itself.

By playing by the rules of the real world, the games sector can continue to thrive, innovate, and bring people together, all while keeping the bad actors off the high score lists. In a sector built on imagination and progression, a strong compliance foundation is not a limitation – it is the extra life that will help the industry continue to grow safely and sustainably.

TL:DR

In 2022, the Lazarus Group, a North Korean hacker organisation, stole $620 million from Axie Infinity's blockchain, using the funds to support the country's weapons program. This incident highlights the increasing risk of sanctions violations in the gaming industry, which operates across multiple jurisdictions and deals with virtual currencies that can be exploited for illegal activities like money laundering.

Gaming companies should proactively address sanctions risks by implementing strong compliance measures, such as appropriate due diligence on players and partners, sanctions screening and have clear internal policies and response plans.

Effective compliance not only prevents financial and legal repercussions but also builds trust with payment providers, advertisers, and users, safeguarding the industry's long-term reputation and growth. The "extra life" that comes from having strong compliance strategies in place ahead of any incident occurring may prove to be vital!

AUTHOR

Ed Arnold
Profile ›

Game workers of the world, unite

Growing popularity of union membership in the UK games industry, accompanied by the Government's proposals for far-reaching reforms to trade union law and workers' collective bargaining rights, present a challenge, and an opportunity, for the games sector.

Union membership has generally been in decline in the UK since its peak in the 1970s and has until recently still primarily within more traditionally unionised professions, particularly within the public sector. However, in more recent years there has been an increasing trend for unionisation in newer, private sector, industries.

Events such as the Covid pandemic and the cost of living crisis may well be a factor in this trend, but interest in union membership is also particularly pronounced where there are issues which are specific to and affect workers in a particular industry.

The highly publicised cultural concerns within the global games industry, followed more recently by significant redundancies within the sector, have led games workers to look to union membership and collective action as a way of having their voices heard and seeking to effect change. This trend, which started in the US, has picked up pace in the UK, with unions recognising the demand and focusing their recruitment efforts.

The Government's legislative changes to trade union laws, announced in October last year as part of the Employment Rights Bill and which are intended to increase union membership and enhance rights for members, mean that for employers in the games sector, understanding and engaging with union membership will be crucial to navigating the changing landscape of labour relations.

Level Up: Rising union membership

The rise in interest in union membership within the games sector follows a challenging period for labour relations within the industry. High profile reports around cultural concerns at US studios in the early 2020s led to workers in those companies turning to unionisation. Concerns around working conditions and culture within the industry more broadly, in what is often a high-pressure working environment, saw union membership grow internationally, including in the UK. More recently, significant layoffs through 2023 and 2024, with more already being announced in the first few months of 2025 have led to a growing interest among workers in the benefit of collective bargaining to secure better job security and working conditions.

> **This increase in interest is evidenced by unions such as BECTU and the Independent Workers Union of Great Britain (IWGB) both establishing specific games worker branches.**

The IWGB Game Workers Branch reportedly saw its membership exceed 1,500 at the end of last year, and with this published a manifesto declaring its plans to transform the games sector by tackling job insecurity, unpaid overtime, and inadequate pay. It highlights perceived issues such as the need for a more equitable distribution of studio profits through worker ownership models, policies to end the gender pay gap, and increases in salaries.

Whilst acknowledging that the games industry is an exciting and dynamic industry to work in, BECTU's Games Workers Branch highlights precarious employment conditions, long hours and a lack of transparency as some of the key issues raised by its members, suggesting that being unionised can result in employers treating their workers with respect and lead to more sustainable and equitable working environments.

Game changing reform?

The proposed changes in the Employment Rights Bill are set to further influence the landscape of union membership and collective bargaining in the UK. The Bill introduces several key reforms aimed at enhancing worker protections and simplifying the recognition process for trade unions, reflecting the Labour Government's manifesto aim of reversing the "anti-union" policies introduced by the previous government, as well as strengthening protections for trade unions and their members.

Information

The Bill will introduce a new obligation on all employers to provide workers with a statement of trade union rights. This will require an employer to give a worker a written statement that they have the right to join a trade union and may also include information on the protections workers have related to union membership or activities. At the same time, the Bill will strengthen and expand upon those protections, including protections against detriment and dismissal for taking industrial action, and protection against blacklisting.

These changes will increase awareness and potentially "normalise" union membership. On-the-ground impacts will include employers needing to update contractual documentation and be ready to engage with questions around their approach to worker representation that they may be unused to dealing with.

Topic to watch for the future: **Employment Rights Bill 2026**

Access

The Bill will introduce a new right of trade unions to access workplaces, with the aim of providing unions with the opportunity to recruit and organise within a workplace in order to gain recognition. The right will be contingent on the trade union and employer entering into an "access agreement" which sets out the terms on which a union will have access and may be varied by the parties at any time. The process for entering into an access agreement will involve a union presenting an "access request" to the employer, who may give the union a "response notice" agreeing or disagreeing with the request (in whole or in part). Where the employer chooses to respond, the parties will then have a "negotiation period" in which to agree the terms of access.

This new right is likely to be more impactful where:

- there is limited existing union recognition, such as the games industry, and where employers will be less experienced in dealing with trade unions. There may well be a requirement for upskilling management and HR to engage with these new rights.
- Unions have an incentive to commit time and resources to access workplaces where their recruitment activities are most likely to pay off, so larger employers may well be a focus.
- Union membership is more likely to gain traction, such as among a disaffected workforce where employee representation is less developed.

Proactive steps by employers to increase staff representation in the workplace, such as through the use of employee forums, may well make them less of a target for unions looking to exercise their new right.

Recognition

A trade union can currently apply to the Central Arbitration Committee ("**CAC**") for statutory recognition if they have at least 10% union membership within the proposed bargaining unit (which may for example be the workers within a particular company or a particular category of workers within that company). They must also have evidence that the majority of the workforce is in favour of recognition and satisfy certain other conditions.

The Bill will replace the current 10% membership requirement with a lower figure, of potentially as little as 2%. It will also remove altogether the requirement for the union seeking recognition to demonstrate that the application is likely to have majority support of those in the bargaining unit.

These changes are seen by some as raising questions as to workplace democracy, with the potential for non-members having unionisation forced on them by a very small minority of employees and being overlooked in union-employer negotiations.

Once an application is accepted, currently the union is required to secure at least 40% support in the bargaining unit in a recognition ballot to have recognition approved by the CAC. This will also be abolished under the Bill, with unions only needing to secure a simple majority of those who vote. It will therefore be important that those who do not want recognition vote, to avoid the request getting carried due to a high number of employees abstaining.

A game of strategy:
Implications of unionisation for employers

Whilst not due to come into force before 2026, the changes under the Employment Rights Bill will further raise awareness of union membership amongst workers and give trade unions a stronger voice in the workplace. Employers will need to be ready to engage with trade union rights, often having had no involvement with them previously.

However, unionisation is not likely to be an end in itself for games workers, but a means to an end.

Employers who proactively review their employment practices and workplace culture, and actively seek and listen to the concerns of their workforce, may well find that union membership is of less interest to their workers.

> **Alternatively, a positive approach to engaging with unions where membership increases is likely to make the process much less challenging. More importantly, considering the concerns of workers, unionised or otherwise, will foster a positive and supportive work environment, with all the benefits that follow, both for the employer, its workers and the sector as a whole.**

TL:DR

The UK games industry is experiencing a significant rise in union membership, driven by cultural concerns, an increase in redundancies, and proposed legislative changes aimed at enhancing workers' rights.

The Employment Rights Bill seeks to increase union membership and strengthen protections for union members. The Bill's key reforms include a new obligation for employers to provide workers with a statement of trade union rights, a new right for trade unions to access workplaces, and a reduction in the membership threshold (possibly as low as 2% union membership within the proposed bargaining unit) required for union recognition.

These changes are expected to increase awareness and normalise union membership, particularly in industries like the games sector where unionisation has been less prevalent.

> **Employers in the games industry will need to adapt to these changes by updating contractual documentation, engaging with union membership, and addressing worker concerns to foster a positive work environment.**

For further analysis on this subject and other aspects of the Employment Rights Bill, see our dedicated Employment Rights Bill web page.

AUTHORS

David Zeffman
Profile ›

Emily Sheard
Profile ›

Charlotte Sanderson

Betting on a billion-dollar industry

Balancing the risks and rewards of gambling sponsorship in esports

The global esports market was valued at USD $1.6 billion in 2022 according to Statista and is expected to grow to USD $2.9 billion by 2025. By 2032, the market is projected to be valued at over USD $10 billion – a fivefold increase within 10 years. Sponsorship provides a significant proportion of this revenue, contributing $837 million (52%) in 2022.

Despite the opportunities that sponsorship partnerships present, publishers have historically restricted the promotion of industries such as alcohol, gambling and cryptocurrency. But, the tide does appear to be turning for better or for worse...

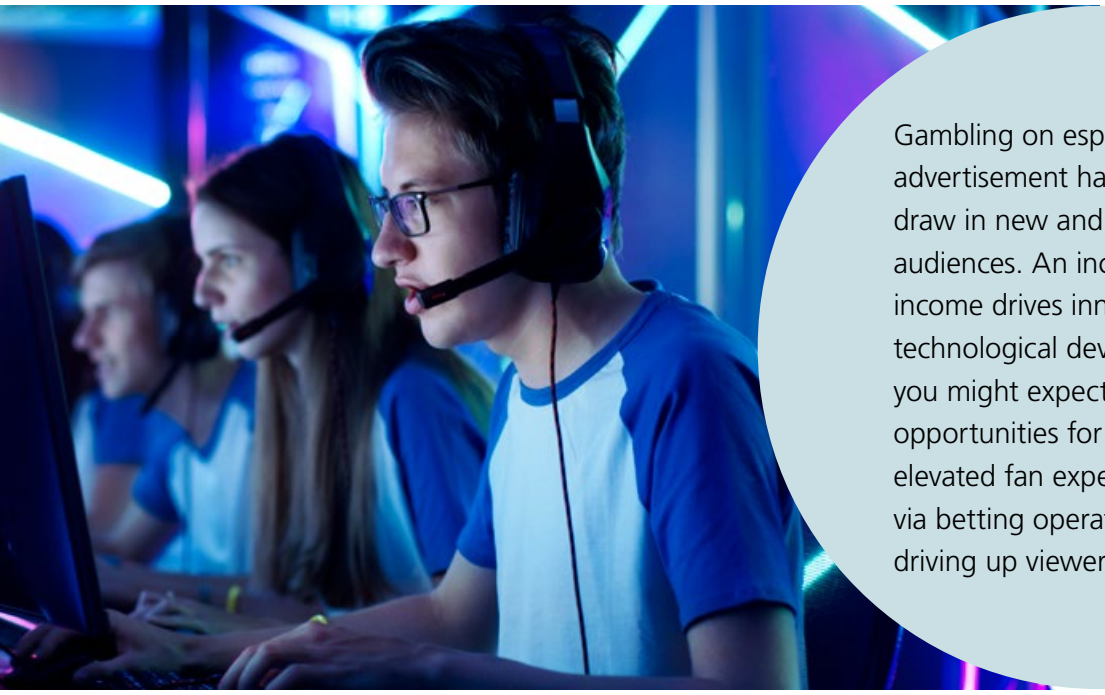
Valve, the developer of Counter Strike and DOTA 2, has allowed gambling sponsors for some events and permits teams to partner with betting brands. A number of high-profile Counter Strike teams including Natus Vincere and Astralis, have secured sponsorship from gambling operators and continue to be some of the most successful teams in the industry.

Riot Games is the most recent tournament organiser to change its position on betting partnerships. The COO of Riot Games esports, Whalen Rozelle, confirmed late last year that League of Legends and VALORANT teams would be allowed to explore partnerships with Riot Games approved betting platforms.

Gambling and esports: A high-stakes partnership

Previously off limits, partnerships with betting operators are a new category of sponsorship for esports and present a potentially highly lucrative opportunity for the industry. These partnerships might include having a gambling operator's logo on player jerseys or promotions through streams or on social media.

The industry relies heavily on sponsorship income, which made up 52% of income in 2022, and publishers who leverage these new partnerships could see substantial financial gains.



Gambling on esports and its advertisement has the potential to draw in new and more mainstream audiences. An increase in interest and income drives innovation and fuels technological development. With this, you might expect to see new opportunities for engagement and elevated fan experiences, including via betting operators, further driving up viewership and income.

The move towards allowing gambling operators to sponsor esports and the prospect of financial gain does not come without risk though. A lack of regulation presents potential safeguarding and responsible gambling issues for young esports players and fans, as well as risks to the integrity of esports and challenges in managing regulatory compliance.

Riot Games appears live to the risks that come with gambling sponsorship, perhaps after the backlash that came from its cryptocurrency partnership with FTX. In a recent statement, Rozelle emphasised that the decision to allow such partnerships was not taken lightly and that the aim was to "*unlock new revenue opportunities for teams while also protecting competitive integrity and the overall fan experience*".

Despite the relaxation of the rules for teams, Riot Games' channels will remain betting-free for the foreseeable future, and no betting brands will appear on broadcasts, socials or uniforms (for teams, that means that they might be able to obtain sponsorship from a betting operator but will not be able to have their logo featured on their jerseys – which will likely impact the sponsorship revenues on offer). All potential partners will also be vetted to ensure that they meet Riot Games' standards for integrity, transparency and fan engagement, which will include checks to ensure that they meet local regulatory and licensing requirements and comply with requirements around content and promotions.

Rozelle also made clear that Riot Games will learn along the way and will continue to evaluate opportunities to expand or refine its approach to gambling partnerships.

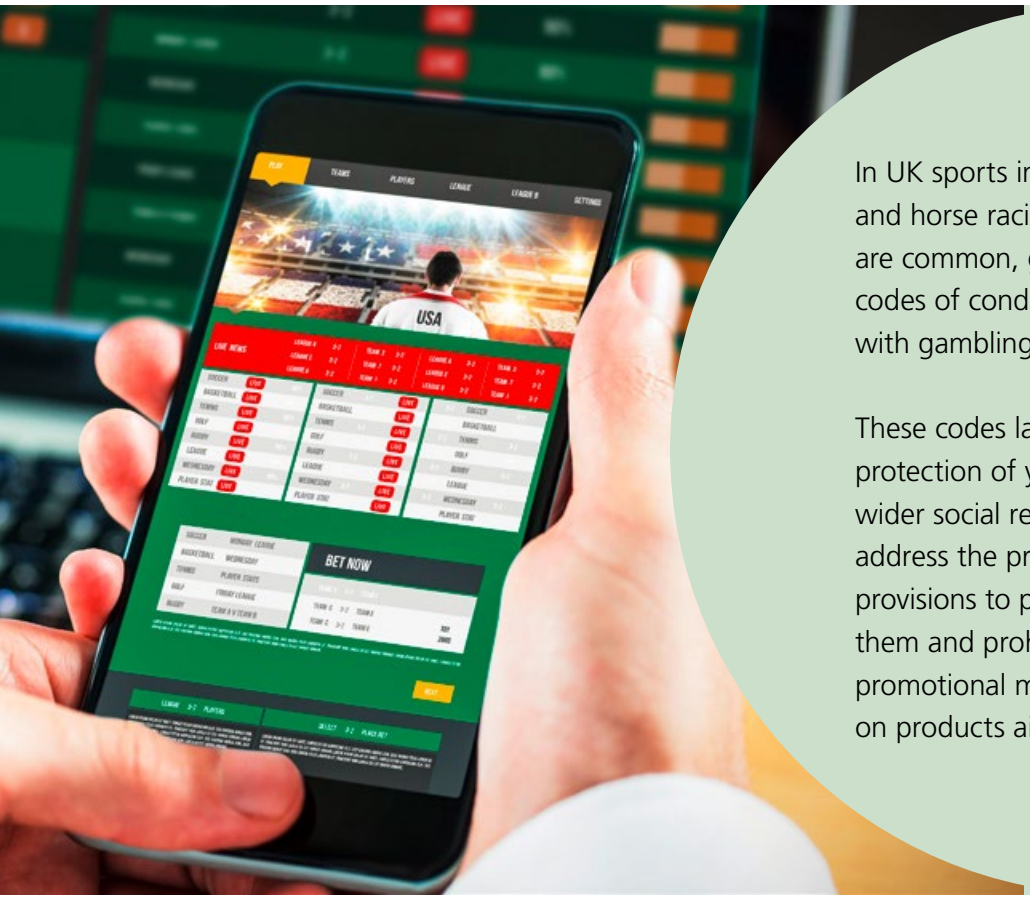
> **But, is this enough? We await the views of many industry players, though it is clear not all publishers and teams will be welcoming betting sponsorship just yet.**

Adam Adamou, the CEO of OverActive Media, has confirmed that Movistar KOI will not be pursuing betting partnerships, and there might be good reason for that…

Risky play:
The impact of betting partnerships on young gamers

In Europe alone, up to 26% of esports fans are thought to be between 16 and 24 years old and so naturally betting partnerships are likely to fuel concerns around exposing younger audiences to gambling and the risk that gambling partnerships will promote unhealthy gambling habits.

Responsible and safe gambling for 18 to 25 year olds has long been a concern for the Gambling Commission of Great Britain and following the publication of the UK's Online Safety Act and the implementation of the EU's Digital Services Act, the safety of young users and fans in the online world has been put into particular focus.



In UK sports industries, such as football and horse racing, where betting partnerships are common, governing bodies have adopted codes of conduct for sponsorship agreements with gambling companies.

These codes largely cover topics such as integrity, protection of young people, reinvestment and wider social responsibility. The codes specifically address the protection of under-18s, with provisions to prevent sponsors from targeting them and prohibit gambling logos or promotional material from being displayed on products aimed at children.

> **This raises the question of whether, before opening its doors to gambling sponsorship, the esports industry should have established a code of conduct to put safety and responsible gambling measures in place.**

Organisations, such as the International Esports Federation and the Global Esports Federation, have attempted to standardise rules and policy through initiatives focused on esports betting and the protection of young people across the industry, but they do not have industry wide buy in.

This is likely down to the piecemeal and localised nature of regulation in esports and the differing approaches to and dependency on sponsorship.

Esports tournament organisers will need to carefully manage partnerships with betting operators to ensure that they do not breach restrictions on targeting under 18 year olds and to ensure appropriate safeguarding measures for the younger audiences that make up a significant percentage of the esports demographic.

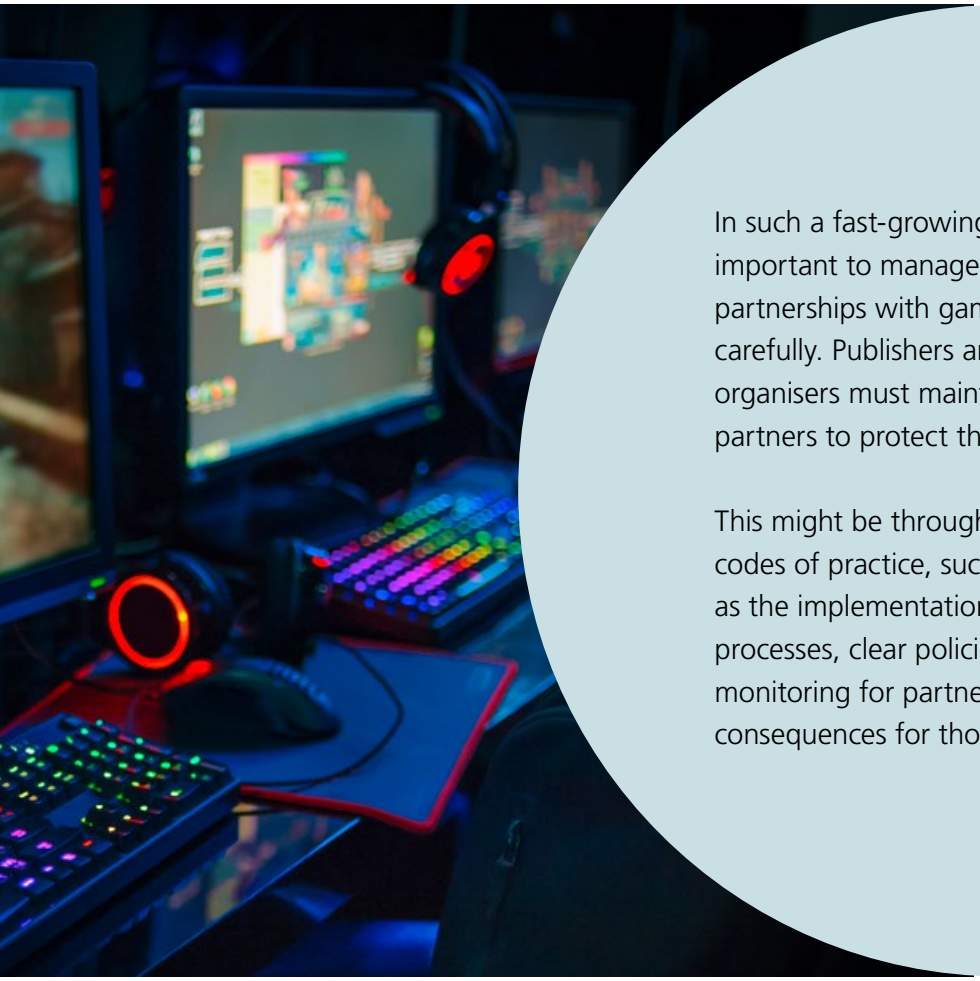
Betting on trouble?
The risk betting partnerships pose to the integrity of esports

Match fixing, even in the esports industry, is not a new phenomenon.

Much like in traditional sports, the introduction of betting partnerships into esports may increase the risk of match fixing and corruption. These risks are, of course, already present as a result of the availability of betting on esports, but bookmaker partnerships may well expose a wider audience to betting on esports and increase players' involvement with gambling. Players may be incentivised to influence game outcomes for reward and this risk will be exacerbated without proper safeguards in place.

This type of behaviour risks undermining the integrity of the competition, potentially damaging the reputation of the entire esports ecosystem.

The Esports Integrity Commission (ESIC) has a code that prohibits gambling on esports matches by certain individuals, including players, and imposes sanctions for match fixing offences. The code is supported by select member organisations, including certain publishers and tournament organisers, and is intended to prevent corruption and protect the integrity of esports.



In such a fast-growing industry, it will be important to manage the introduction of partnerships with gambling operators carefully. Publishers and tournament organisers must maintain high standards for partners to protect the integrity of esports.

This might be through a wider commitment to codes of practice, such as ESIC's code, as well as the implementation of proper vetting processes, clear policies and ongoing monitoring for partnerships, with consequences for those who fail to adhere.

Rolling the dice:
Regulatory challenges across jurisdictions

The online nature of esports competitions poses unique regulatory challenges, with some tournaments being held exclusively online, featuring players, publishers and sponsors from across different parts of the world.

Laws on gambling and the regulation of gambling operators vary widely from jurisdiction to jurisdiction, and esports organisations and players are likely to find themselves trying to navigate a complex legal and regulatory landscape. Players, publishers and gambling operators will be subject to different obligations and restrictions depending on the circumstances, meaning compliance will involve assessing a matrix of often overlapping legal and regulatory requirements across a web of jurisdictions.

By way of example, in the UK, gambling operators must comply not only with the UK Gambling Act 2005 and the rules and regulations laid down by the Gambling Commission of Great Britain, but also with marketing and sponsorship rules within the CAP Code and the guidance issued by the Advertising Standards Agency.

It will be important for esports organisations, publishers and players to have an understanding of the different legal and regulatory frameworks applicable to be able to take advantage of the opportunities, and mitigate the risk, that betting partnerships present.

If the industry fails to take this seriously enough, the likely result will be legal and regulatory crack down. That could come from two directions, with the introduction of additional regulation for the gambling industry, which could put limitations on the potential revenues available from betting sponsorship, or a more wholesale change in the regulation of esports.

Unlike traditional sports, esports are largely decentralised, with game developers devising tournaments without oversight of a governing or regulatory body. Without that oversight, they are free to set their own rules on sponsors. This does have benefits for a new and innovative industry. But, publishers must be mindful of longer term regulatory and reputational risk if they move too fast without properly assessing existing legal and regulatory requirements, or the need for additional protective measures.

Game on:
Are esports and betting partners ready for the next challenge?

As the industry continues to grow, the relaxation of rules on betting partnerships could offer the esports industry lucrative revenue opportunities.

> **However, publishers will need to navigate the complex ethical, legal and regulatory issues, as well as safeguarding challenges to leverage these opportunities without compromising the core values that have made esports a global phenomenon.**

A more unified approach to betting sponsorships across the industry may help navigate these challenges, particularly, in providing an opportunity for publishers to come together and agree policies or codes of practice for such partnerships to mitigate the risks that they present.

As part of this, but also on a wider scale, maintaining the integrity of esports competitions and fostering a positive relationship with the fans will be key to sustaining long-term growth and success in this billion-dollar industry.

TL;DR

The value of gambling sponsorships in the esports industry is projected to grow significantly over the next decade. Major game developers like Valve and Riot Games have begun to relax their restrictions on gambling partnerships, allowing teams to explore lucrative sponsorship opportunities.

However, this shift brings substantial risks, particularly concerning the exposure of young audiences to gambling and the potential for match-fixing and corruption. Esports organisations will need to ensure that they implement responsible gambling measures, regulatory compliance, and safeguarding to protect the integrity of esports. They will also need to navigate a complex legal landscape, due to the variation in gambling laws across jurisdictions.

> **A unified approach to betting sponsorships, including the establishment of industry-wide codes of conduct, is a potential way to mitigate these risks and ensure sustainable growth.**

AUTHORS

Kenny Henderson
Profile ›

Alex Danchenko
Profile ›

Looking for group

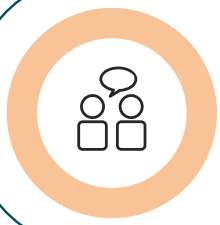
Class action litigation risk in the gaming space

Game ecosystems and the communities built within them are some of the most important assets to any gaming company and significant resources can be dedicated to engaging with them. But what if it goes wrong? We need to be alive to the risk that relationships with the community and end consumers could turn hostile – at a moment's notice – particularly where there is a perception of some wrong or injustice taking place. In the modern world, those consumers' choice of weapon to combat perceived wrongs includes group litigation.

Attack its weak point for massive damage!

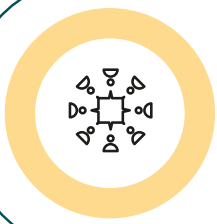
The gaming and interactive entertainment industry occupies a unique – if not uniquely vulnerable – position vis-à-vis group litigation. Consider the following:

An average gamer in the traditional sense is tech-savvy, with considerable spending power, often opinionated and driven. There is also now a lot more of them, with gaming becoming the new generations' equivalent of television.



Though increased market penetration has brought along greater profit, it may have reduced customer loyalty and sense of community. Hard-core communities still exist, but other groups of consumers will engage with more products in a shallower way, and may take more aggressive steps to get redress for perceived grievances.

Claimant law firms and litigation funders have also been paying attention to the catchy multi-billion dollar industry size figures, to the point that specialist outlets focussed on the industry are now starting to emerge.



Most game distribution happens through platforms that are conduits to the ultimate end-user on one end and for publishers and developers on the other. The nature of this role – combined with the perception of large platforms having "deep pockets" – are obvious magnets for claimant firms looking to employ novel competition / consumer law litigation.

The mass and diverse nature of consumer / platform / storefront interactions means that many things of different nature can go wrong, starting with personal data leaks and breaches – to leaks / misuse of payment data – to minor errors in a patch making a game (or even the whole platform) unavailable to swathes of its angry paying customers.

It is not surprising that we have been seeing more and more high-profile group litigation in the space not only in its traditional hotbed in California / the US, but also in the UK. This is a risk that now needs to be priced in regardless of where your organisation is based – or your customer base is located.

The dark age of CATelot

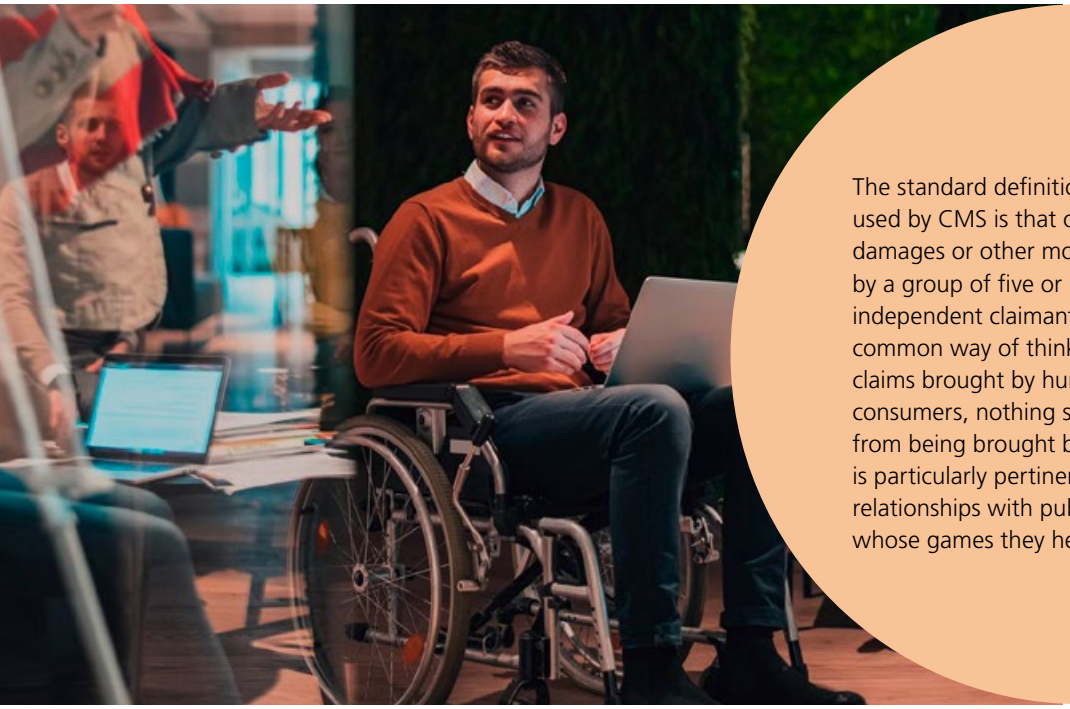
While the overall share of new class actions filed in the UK has been falling relative to other European countries, now roughly at 30% of the total number, the cumulative value of group claims brought in the country still sat at a staggering EUR145 billion as at the end of 2023*.

> **Given the UK is also one of the largest (if not the largest) markets for video games in Europe, it follows that it is *the* group litigation risk hotspot to be aware of.**

*For more key data on the growth of group litigation risks in Europe, check out CMS's 2024 edition of the **European Class Actions Report** – and do keep an eye out for the new edition this summer!

This status is facilitated by the UK's sophisticated judicial framework for group litigation. Most pertinently, the UK Competition Appeals Tribunal ("**CAT**") can issue Collective Proceedings Orders, certifying claims on an "opt-out" basis – meaning that every *member* of the described class affected by the alleged wrongdoing is *automatically* entitled to redress if the claim succeeds, without having to do anything. The threshold for certification of claims is also rather low, following the appeal certification decision in *Merricks v Mastercard* [2021] CAT 28, to the point that some defendants even choose not to contest it. And once a claim is certified, it is on a direct pathway to trial.

While CAT's jurisdiction is limited to breaches of competition law, it has nevertheless resulted in astronomical damages being sought even where any redress due to an individual consumer was less than £100. The total value of opt-out CAT claims as at the end of 2023 was around EUR 66.3bn. Many claimants are seeking to characterise issues of consumer law as issues of competition law instead, to be able to litigate in the CAT and take advantage of its lenient certification framework. This means that even platforms which consider themselves to be in the clear from competition law perspective are not always protected from a potential opt-out CAT claim.



The standard definition of a "class action" used by CMS is that of an action for damages or other monetary award brought by a group of five or more economically independent claimants. While the most common way of thinking of these is as mass claims brought by hundreds of individual consumers, nothing stops a group claim from being brought by corporates – which is particularly pertinent to platforms' relationships with publishers and developers whose games they help distribute.

The way these claims may be characterised is as unfair pricing / abuse of dominant position claims, particularly in relation to platform commissions and forcing digital distribution restrictions / creating "walled gardens". There are currently two such cases making their way through the CAT (see opposite).

Similarly framed arguments had previously been made in high profile industry litigation in the US – e.g., *Epic Games v Google* which ultimately resulted, in October 2024, in the permanent injunction to force Google to allow third party app stores within its Android ecosystem. This goes to show that many of the trends we see States-side are often replicated in the UK few years later.

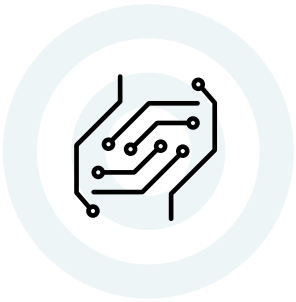
> **To illustrate, the legs of the Valve claim in the CAT may be said to grow from *Wolfire Games v Valve*, pursued on similar grounds, but on behalf of publishers and developers using Steam to distribute their games.**

- ***Alex Neill v Sony Interactive Entertainment*** (Case No. 1527/7/7/22): currently scheduled to go to trial in March 2026, allegedly for £5 billion; and
- ***Vicki Shotbolt v Valve Corporation*** (Case No. 1640/7/7/24): filed in 2024 and not yet granted certification, allegedly for c. £656 million.

Notably, both of the claims are against platforms / storefronts, and are being pursued by the same claimant law firm, Milberg London LLP.

Prepare for unforeseen consequences

Armed with the theory that UK litigation trends tend to follow those in the States, it is worth considering what other group litigation theories we may (or likely may not) end up seeing developing over the course of the next few years.

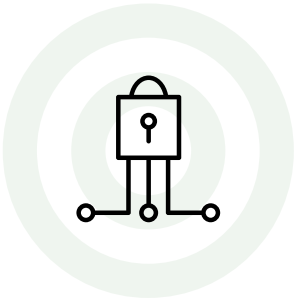


Virtual assets

A hot topic in and of itself, this is of particular interest for the industry given the vast array of different kind of assets that percolate within it – from TF2 hats, to EVE Online PLEX, to WoW gold-selling, to what remains of the recent NFT / Web3.0 games craze. While the 2023 Law Commission report on digital assets concluded, on a provisional non-binding basis, that in-game assets will not generally attract traditional common law property rights, there have been precedents abroad of digital assets being treated similarly to traditional property: with reported prosecution in the Netherlands for theft of in-game items, and more significantly, a California case of *Jane Doe v Roblox Corporation* (ultimately settled) pursuing remedies for content moderation policy resulting in deletion, without compensation, of in-game items.

Dark patterns and gaming addiction

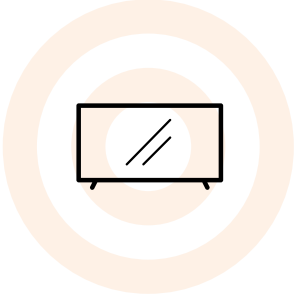
This relates to what the US FTC defined as "*design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm*". Much noise has been made about this issue by enforcement agencies and lawmakers on both sides of the Atlantic, with for example, US$245 million settlement entered with the FTC by Epic Games and the publication of UK ICO's Age Appropriate Design Code intended to deal with things like "nudge" techniques. That being said, there have also been signs of the reversal of the trend.



Data privacy

While there has been evidence of data protection / privacy claims filed against large gaming companies, bringing large data privacy group claims in the UK has become less attractive following the seminal Supreme Court decision in *Lloyd v Google LLC*, and related decision in *Prismall v Google UK Limited and DeepMind Technologies**. Absent a major development, we would expect the trend to continue.

(*See our coverage of *Lloyd* and *Prismall*.)



False advertising

This is a good illustration of how more traditional theories can be adapted for use in the gaming industry context. These have ranged from a rather straightforward 2023 claim for alleged promise of discounts on in-game reward packs (the *King of Avalon* litigation against KingsGroup and FunPlus), to, reportedly, more arcane "bait and switch" scenarios where an item description for an in-game purchased gem in *Diablo Immortal* was allegedly changed (or clarified) to give a smaller damage buff than advertised. In our view, this is one to watch, particularly given that at least one of the claims in this category (*Cassell and Liu v Ubisoft, Inc.*) related to the shut-down of a live service game The Crew, in circumstances where there has recently been a string of *very* high-profile live service game failures…

You must construct additional pylons

Which is all not to say that it is easy to bring a class action in the UK, even against an attractive defendant and armed with a viable litigation theory. The principal challenge lies in attracting litigation funding and managing the network of relationships between the funders and other stakeholders. A number of developments in recent years made this even harder.

What is known as the PACCAR decision of the Supreme Court threw a spanner in how litigation funding agreements are allowed to be structured, significantly setting back a number of high-profile claims.

At the same time, the funders' degree of control over group litigation and class representatives and members has been coming under increased scrutiny.

There is an ongoing and highly publicised conflict between the class representative and funder in the *Merricks v Mastercard* litigation due to the former agreeing to a settlement sum significantly below the advertised £10 billion claim value. In his witness evidence accompanying the settlement proposal, the class representative made a number of statements which prima facie suggest there may exist a conflict of interests on his part.

Even more strikingly, January this year saw the first ever outright refusal to certify a class action in the CAT due to, among other things, the alleged degree of control exercised upon the class representative by the funder.

This goes to show that there are avenues successfully to challenge UK group litigation, albeit it requires a considerable degree of finesse, preparedness, and understanding of the intricate psychological and power dynamics within the funder – claimant firm – representative Unholy Trinity.

TL;DR

The gaming industry faces an increasing risk of class action litigation due to its large, tech-savvy, and often opinionated consumer base.

Factors such as the growing market, high-profile cases, and the rise of claimant law firms have led to more group litigation in both the US and UK.

In the UK, class actions in the CAT can be certified on an "opt-out" basis, with current claims including billion-dollar disputes over platform commissions and digital distribution practices.

Other potential litigation risks include loss of virtual assets, gaming addiction (through "dark patterns"), data privacy, and false advertising.

However, class actions remain difficult to run successfully, with real difficulties lying in attracting litigation funding and managing the network of relationships between funders and other stakeholders. In particular, recent case law indicates that the UK courts are taking a dim view where funders exert excessive control over the class representatives.

> **UK group litigation can therefore be challenged, but this requires finesse, preparation, and understanding of the power dynamics between the funder, claimant firm, and representative. Gaming companies should be aware of these risks and prepare accordingly.**

Who we are

Preparing for tomorrow's challenges starts today. That's why CMS adopts a Future Facing approach, ensuring our clients stay ahead in an ever-evolving landscape. Global expertise, local insights, always with your commercial goals in mind.

Industries can rapidly change, business models can be disrupted, and regulation can force organisations to change course almost overnight. By continually scanning the horizon, CMS helps its clients to anticipate both the challenges and the opportunities headed this way. This is Future Facing Law.

In a world where innovation is business as usual, our mission is to deliver practical, business-focused advice that helps clients of every size to face the future with confidence.

Our lawyers immerse themselves in our clients' worlds, and as genuine experts in their fields, offer a grasp of detail that is second to none. We combine this with a next-generation mindset that means we can deliver innovative processes and solutions at speed, and at scale.

If you have any questions or would like to discuss any of the topics in more detail, please don't hesitate to reach out to our team.

cms.law

1,300+ Partners	6,800+ Lawyers	10,000+ Staff
21 Member firms	45+ Countries	80+ Offices

Our global coverage

The Americas

Bogotá
Lima
Mexico City
Rio de Janeiro
Santiago de Chile
São Paulo
Silicon Valley*

Europe

Aberdeen
Amsterdam
Antwerp
Barcelona
Belgrade
Bergen
Berlin
Bratislava
Bristol
Brussels
Bucharest
Budapest
Cologne
Dublin
Duesseldorf
Edinburgh
Frankfurt
Funchal
Geneva
Glasgow
Gothenburg
Hamburg
Istanbul
Kyiv
Leipzig
Lisbon
Liverpool
Ljubljana
London
Luxembourg
Lyon
Madrid
Manchester
Milan
Monaco
Munich
Oslo
Paris
Podgorica
Poznan
Prague
Reading
Rome
Sarajevo
Sheffield
Skopje
Sofia
Stavanger
Stockholm
Strasbourg
Stuttgart
Tirana
Vienna
Warsaw
Zagreb
Zurich

Africa

Casablanca
Ebene
Johannesburg
Luanda
Maputo
Mombasa
Nairobi

Middle East

Abu Dhabi
Dubai
Muscat
Riyadh
Tel Aviv

Asia-Pacific

Beijing
Brisbane
Hong Kong
Shanghai
Singapore
Sydney

*Representative Office

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Abu Dhabi, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bergen, Berlin, Bogotá, Bratislava, Brisbane, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Cúcuta, Dubai, Dublin, Duesseldorf, Ebene, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Gothenburg, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Maputo, Mexico City, Milan, Mombasa, Monaco, Munich, Muscat, Nairobi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, São Paulo, Sarajevo, Shanghai, Sheffield, Silicon Valley, Singapore, Skopje, Sofia, Stavanger, Stockholm, Strasbourg, Stuttgart, Sydney, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.

Further information can be found at **cms.law**