Virtual Currencies, Real Harms: Why Legal Certainty Demands Regulatory Clarity

Setting the Tone

As a legal interpreter, my role is not to champion or condemn the industry's business model but to dissect the legal reality through established frameworks like the UCPD, CRD, and evolving EU jurisprudence. Let me be apparent from the outset: not all innovation is progress, and not all virtual currencies are games. Some are obfuscation systems, engineered uncertainty, and extraction, designed to obscure costs and drive excessive spending in digital environments. This debate isn't a simplistic clash of innovation versus regulation; it's a critical tension between legal certainty and consumer harm. Virtual currencies in gaming often blur the line between entertainment and exploitation, raising urgent questions about transparency, fairness, and the protection of vulnerable players in an increasingly complex digital marketplace.

"Let me be clear from the outset: not all innovation is progress, and not all virtual currencies are games. Some are systems of obfuscation, engineered uncertainty, and extraction."

Part I: Legal Certainty and the ACM's Authority

The Netherlands ACM operates within a robust EU consumer protection framework, with its recent enforcement actions reflecting a decade of evolving jurisprudence and guidance. The ACM's "Protection of Online Consumers" policy framework (2019) targets information asymmetry, transactional manipulation, and unfair commercial practices in the digital economy, aligning seamlessly with the Unfair Commercial Practices Directive (UCPD). Specifically, Articles 5–7 UCPD address misleading omissions and aggressive practices, empowering the ACM to tackle opaque pricing, manipulative countdown timers, and exploitative designs in online gaming and beyond. This approach is bolstered by CJEU case law, such as Case C-628/17 Orange Polska, emphasising the necessity of informed decision-making in complex digital environments, ensuring unclear or coercive tactics do not mislead consumers. *The ACM is not operating in a vacuum. Its recent enforcement aligns directly with the evolution of EU consumer protection jurisprudence and regulatory guidance over the past decade.*"

Further reinforcing the ACM's authority, the European Data Protection Board's Guidelines 05/2020 on valid consent underscore that "confusion is not compliance," demanding transparency in digital interactions. The ACM's actions thus bridge consumer and data protection principles, addressing practices that obscure costs or pressure vulnerable users. At the core lies the principle of legal certainty: in a functioning internal market, economic actors—gaming companies included—require clear rules to operate, but so do consumers, particularly children, who face heightened risks from exploitative designs. By grounding its enforcement in UCPD, CJEU rulings, and EDPB guidance, the ACM delivers predictable, principled oversight, safeguarding consumers while fostering fair digital markets.

Part II: Virtual Currencies as Legal Fictions and Consumer Traps

Virtual currencies are not currencies in the legal or economic sense. Instead, they are *digital representations of value*, often constructed as loyalty schemes engineered with the opacity of financial instruments and the behavioural pull of gambling. While this characterisation is analytically functional for legal purposes, it is crucial to acknowledge how these mechanisms function in practice: they are designed to obscure actual monetary cost, fragment user spending, and manipulate consumer decision-making.

Most virtual currencies are only available through *forced bundling*, meaning users can only purchase them in fixed denominations (e.g., 500 or 1,200 coins), regardless of actual need. This invariably creates *breakage*—unused leftover value that cannot be easily redeemed, trapping residual funds in the platform and incentivising further spending to "make use" of the remainder. Worse, these currencies are *non-convertible*: they cannot be refunded, exchanged, or used outside the specific game ecosystem, immobilising the consumer's purchasing power and eroding autonomy.

These structural elements are not accidental but hallmarks of *manipulative choice architecture*. As detailed by several academics (including myself and the OECD, and the European Commission and and and) and reinforced by the ACM, the Norwegian Consumer Council, and UNCTAD's work on digital consumer protection, these designs exploit behavioural biases—*default bias*, *the sunk cost fallacy*, and artificially induced urgency via countdown timers or limited-time offers—to encourage overspending and deepen user entrenchment in the platform economy.

Such practices fail to meet the *average consumer benchmark* set out in Recital 18 of the Unfair Commercial Practices Directive (UCPD), which requires that commercial communications be transparent, fair, and comprehensible to the average consumer acting with reasonable diligence. When children are involved, the standard tightens. Their age, credulity, and limited understanding significantly lower the threshold of acceptable practice. As recognised by European consumer authorities, targeting or affecting minors with such opaque pricing schemes and manipulative mechanics is not merely unfair—it is unconscionable.

Importantly, there is **no justifiable legal or ethical basis** for treating consumers differently when they spend money *within* a game as opposed to spending it *elsewhere*. The industry's argument that in-game purchases merely constitute the execution of a licensing right, rather than a "purchase", is disingenuous. These transactions are consistently presented to consumers in the language and framing of real-world purchases. Platforms employ purchase confirmations, shopping cart interfaces, and marketing cues indistinguishable from standard e-commerce. It should be regulated as one if it walks and talks like a purchase.

Part III: Harms to Children and the Doctrine of Vulnerability

"Children do not negotiate with platforms. They shape them."

In EU law, children are not treated as miniature consumers. They are recognised as a specially protected class, entitled to elevated safeguards in digital environments where asymmetries of power, information, and autonomy are most acute. This doctrinal foundation is well-established:

- Recital 38 of the GDPR explicitly states that children merit specific data protection, particularly in the context of marketing and behavioural profiling.
- Article 5(3) of the ePrivacy Directive prohibits storing or accessing information on a user's device without informed consent—an obligation that takes on special force where children are involved.
- Across Europe, regulators have issued coordinated guidelines on online manipulation, recognising the exploitative targeting of children as a distinct category of harm.

Virtual currencies in gaming environments systematically bypass the protective logic of EU consumer law. They decouple spending from recognisable monetary value, using opaque conversion rates and abstract token systems that blur the boundary between play and payment. These systems exploit cognitive and behavioural vulnerabilities, especially acute in children, by embedding intermittent reinforcement loops, variable rewards, and perceived scarcity, thereby encouraging compulsive spending.

The legal issue is not whether children can be taught to be "savvy" users. These mechanics are structurally designed to erode defences, not test them. This is not incidental. It is engineered by design, not by accident.

Such systems breach the average consumer benchmark under the Unfair Commercial Practices Directive and collapse entirely when assessed against the elevated standard applicable to minors. As EU guidance has repeatedly affirmed, the law must reflect children's credulity, inexperience, and developmental vulnerability. Regulatory scrutiny must be most exacting in domains like gaming, where children spend time, form habits, and experience emotional reward.

"When design becomes deception, the law does not stand still. Nor should we."

In this context, regulatory inertia is not neutrality—it is complicity. Where monetisation strategies are intentionally constructed to circumvent children's cognitive limits, legal systems must act not merely to prohibit but to dismantle such architectures.

Part IV: Procedural Injustice or Regulatory Maturity?

"The industry has claimed 'procedural injustice'. But enforcement is not injustice — it is evidence of a maturing regulatory system responding to maturing harms."

Assertions that the Netherlands Authority for Consumers and Markets (ACM) acted arbitrarily or without due notice are not only **factually incorrect**, but legally misdirected. Regulatory action is not injustice; it is the **culmination of a transparent and foreseeable trajectory** of oversight rooted in public law mandates and evolving consumer protection jurisprudence.

Since 2019, the ACM has consistently and publicly articulated its enforcement priorities concerning **manipulative digital design and opaque monetisation practices**. Its seminal framework *"Bescherming van de online consument"* (2019) flagged these very issues—dark patterns, transactional opacity, and asymmetric information—as enforcement targets. Subsequent policy publications, coordinated market studies, and participation in multilateral initiatives (e.g. with the CPC Network and the European Commission) reinforced these commitments. The industry was not blindsided. It was **systematically forewarned**.

Moreover, the ACM's actions align with an international regulatory arc: from UNCTAD's digital manipulation assessments to the Norwegian Consumer Council's exposés, and from UK and Belgian scrutiny of loot boxes to the EU's own legislative clarifications under the Digital Services Act. ACM's approach is not exceptional. It is **jurisdictionally consistent and procedurally foreseeable**.

What is frequently labelled "procedural injustice" in these contexts is, more accurately, **resistance to substantive accountability**. When enforcement finally interrupts longstanding practices that have evaded legal scrutiny, it is not the process that is unjust—it is the discomfort of facing long-deferred compliance.

"Clarity of rules may be painful, but it is not unfair."

Legal certainty is not the same as legal convenience. The gaming industry cannot credibly demand predictability while ignoring published warnings, side-stepping regulatory dialogue, or refusing to meaningfully reform monetisation structures targeting children and vulnerable users. When regulators finally act, it is not retaliation—it is the **rule of law catching up to an industry long overdue for oversight**.

Part V: Regulatory Timeline for Virtual Currencies in Gaming

Regulatory scrutiny of virtual currencies and randomised virtual goods in gaming environments began in earnest before 2015, with the UK Gambling Commission probing unlicensed gambling sites using in-game items as early as 2014, followed by the European Central Bank's 2012 report flagging risks. Initial discussions gained traction with the UKGC's 2015 "Social Gaming" paper, which found no urgent need for new rules, and evolved through 2016-2017 with EU resolutions, anti-money laundering directives, and UKGC position papers demanding licenses for gambling with convertible in-game items. By 2017, Japan defined virtual currencies and enforced oversight. China mandated odds disclosure for loot boxes and banned virtual currencies, signalling a shift to concrete action to protect consumers, especially children, from exploitation.

From 2018, enforcement intensified: Belgium and the Netherlands classified certain loot boxes as gambling, forcing companies like Rocket League to adapt by 2019. Meanwhile, 15 European regulators and one U.S. body declared risks in blurring gaming and gambling lines. The UK's 2019 DCMS inquiry pushed for tighter rules under the Gambling Act, and the Netherlands' ACM fined Epic Games in 2020 for unfair practices in Fortnite. By March 2025, the Consumer Protection Cooperation Network, with the Netherlands' ACM, targeted Star Stable Entertainment AB, demanding compliance within a month under EU consumer laws. This timeline reflects a clear arc—early investigation, debate, and guidance for targeted regulations and enforcement, underscoring a global resolve to safeguard players from financial and psychological harm in gaming ecosystems.

Part VI: The Illusion of Soft Commitments – Why Structural Regulation is Non-Negotiable

Voluntary industry codes and aspirational pledges to "do better" are not safeguards. They are reputational shields—mechanisms for deflection, not accountability. In the context of virtual currencies and their behavioural exploitation within gaming environments, soft law measures—absent robust enforcement structures—do not meaningfully constrain commercial behaviour. They offer a mirage of responsibility, while leaving underlying manipulative architectures intact.

Legal scrutiny of self-regulation reveals three core deficits: first, the absence of **independent enforcement** capable of compelling compliance; second, the lack of **clear metrics or benchmarks** to determine success or failure; and third, the evasion of **binding timelines** that ensure time-sensitive reforms. These are not peripheral omissions—they are structural deficiencies that render such frameworks inadequate from a legal and consumer protection standpoint.

While space must remain for cooperative and co-regulatory approaches—especially those involving technical expertise or dynamic risk modelling—such schemes are only defensible when **nested within an enforceable statutory regime**. As with the **Digital Services Act's** risk-based obligations or the **Unfair Commercial Practices Directive's** binding minimum standards, the legitimacy of any hybrid regulatory arrangement hinges on its subordination to public law oversight. Without this, self-regulation becomes a vector for delay, dilution, and reputational laundering.

"Self-regulation only works where there is trust. And trust is earned through accountability, not declarations."

In light of the **persistent violations** of the UCPD and CRD in virtual currencies, ranging from obfuscated pricing to aggressive commercial practices, regulatory patience for rhetorical compliance must end. Structural exploitation demands a structural remedy. The legal imperative is clear: **the law becomes complicit in harm without enforceable obligations**.

Epilogue: UCPD and CRD Violations by Virtual Currencies in Gaming

Using virtual currencies in gaming environments raises significant concerns under the Unfair Commercial Practices Directive (UCPD) and Consumer Rights Directive (CRD) outlined by the Consumer Protection Cooperation Network. Key violations include obscuring actual costs through complex virtual currency exchange rates and bundled purchases, violating UCPD's misleading actions and omissions principles (Articles 6-7) and CRD's pre-contractual information requirements (Article 6). Aggressive practices, such as countdown timers and designs forcing excess spending, exploit cognitive biases and contravene UCPD's rules on undue pressure (Articles 8-9) and professional diligence (Article 5). Additionally, denying the 14-day withdrawal right for unused virtual currency or digital content purchases breaches CRD provisions (Articles 9-16), while unfair terms—e.g., unilateral value changes or account bans without recourse—clash with consumer protections, potentially implicating the Unfair Contract Terms Directive.

When targeting children, these practices face heightened scrutiny due to their vulnerability, amplifying the impact of violations. Direct exhortations to buy in-game items, banned under UCPD's Annexe I, exploit children's credulity and inexperience, distorting economic behaviour in harmful ways. The lack of robust payment controls, such as password-protected purchases or age-appropriate default settings turning off spending, fails to shield children, contravening UCPD's emphasis on protecting vulnerable groups (Articles 5-8). Regulatory bodies prioritise enforcement here, demanding transparency, pressure-free environments, and stringent parental controls to align with stricter fairness thresholds. This underscores the elevated risk of harm and the urgent need for traders to adapt practices to safeguard young players.

VCs in gaming environments pose significant risks, clashing with the UCPD and CRD by obscuring actual costs and eroding transparency. Complex exchange rates, multiple VC types, and failure to display real-world prices mislead players, violating UCPD's principles against misleading actions and omissions (Articles 6-7) and CRD's pre-contractual clarity rules (Article 6). Psychologically, VCs disconnect spending from tangible money, boosting expenditure by reducing the 'pain of paying,' while practices like forced bundling, countdown timers, and designs exploiting biases—sunk cost fallacy, urgency cues—pressure players into overspending, breaching UCPD's aggressive practices rules (Articles 8-9) and professional diligence (Article 5).

Additional harms compound the issue: denying the 14-day withdrawal right for unused VCs or digital content flouts CRD provisions (Articles 9-16), unfair terms—unilateral VC value changes, unchallengeable account bans—undermine consumer rights. Gambling-like risks from loot boxes, especially when VCs or items hold tradable value, fuel excessive spending and problem gambling, particularly without licenses, raising concerns of fraud and loss-chasing. Real money trading (RMT) erodes trust, fosters regret, and disrupts gameplay. At the same time, immersive game designs paired with VC inaccessibility can trigger anxiety, exploiting vulnerable players like "whales" in violation of UCPD's fairness standards (Article 5).

Harms intensify when children are involved, as their vulnerability—lack of experience, credulity—amplifies susceptibility to obscured costs, direct exhortations to buy, and pressure tactics, all banned or scrutinised under UCPD (Annexe I, Articles 5-8). Gambling-like loot boxes pose acute risks, with young players four times more likely to face adverse effects, prompting regulatory focus on blurred gaming-gambling lines. Inadequate payment controls, unadapted information, and failure to default-disable spending without parental oversight exploit children, violating stricter UCPD fairness thresholds and demanding urgent trader accountability to protect this vulnerable group.