27 July 2026

Comments of

TRUSTED FUTURE

To the

United Kingdom's Competition and Markets Authority (CMA)

regarding its

Consultation regarding

Steering Conduct Requirement

Apple's Mobile Platform

On behalf of **Trusted Future,** a non-profit organization dedicated to the belief that we need smart well-informed policies to drive trust throughout today's digital ecosystem, we welcome this opportunity to provide input to the Competition & Markets Authority (CMA) on its Consultation regarding Steering Conduct Requirement: Apple's Mobile Platform.

At a time of such dynamic change, when trust in digital ecosystems is being challenged nearly every day, and trust has emerged as a central enabler for digital adoption, a non-pretextual pro-competition differentiator, and a basis for consumer gains, we believe it's vital that CMA's efforts in this domain be reviewed through a lens of trust. This will help ensure that UK users are able to take full advantage of a vibrant mobile digital ecosystem that is innovative, safe and secure, competitive and trustworthy — an ecosystem where people are able to improve their lives because they have access to trustworthy technologies that protect their privacy, safety and security.

We are thankful for this opportunity to respond, and have divided our response into four main sections: 1) How trust has emerged as essential infrastructure upon which UK digital opportunity is built. 2) How the CMA can address potential inconsistencies with consumers and the UK Government's trust priorities. 3) How the CMA can incentivize a competitive, innovative and trustworthy mobile ecosystem in the UK; and 4) The technical requirements necessary for achieving a trustworthy link-out framework.

1. How Trust Has Emerged as an Essential Infrastructure Upon Which UK Digital Opportunity is Built.

In October 2023, after taking input from CMA and Ofcom, the UK Government published an updated version of its voluntary Code of Practice setting out the baseline security and privacy requirements for app store operators and app developers — helping to advance and ensure baseline levels of trust in the app store ecosystem. As a result of these and other efforts by smartphone manufacturers to integrate privacy, safety and security into their technologies by design, the mobile ecosystem has become a cornerstone of the British digital economy. UK mobile data consumption has surged, up 495% between 2018 and 2025, driven by more powerful devices, advances in connectivity, and a trusted app economy. In fact, the UK mobile app market has exploded into a £28.3 billion economic powerhouse in 2025, growing at 12.9% annually, and benefitting the 95% of the population that now owns smartphones. This level of adoption and integration into the UK economy has only been possible because of the trust that users and businesses place in their mobile phones.

As mobile devices have become a trustworthy companion, they have become almost ubiquitous throughout our lives. They are now the number one way UK citizens access the Internet. Because they now enable us to do almost anything and everything, UK consumers and businesses now rely on the integrity of their mobile devices and the app ecosystem to protect some of their most sensitive and mission critical aspects of their lives and businesses. Surveys now show that more than half of consumer mobile phones contain sensitive work information. To protect their data, users rely on built-in privacy and security safeguards so they can trust their information will be protected, as will their transactions when they bank, buy, communicate, learn, date, play, and travel. And they rely on these safeguards to protect the extremely sensitive and private information they contain like health data, banking credentials, private photos and communications.

The changes in the way people use this technology have been enabled by massive investments to integrate trust into the core of mobile technologies and into the vibrant app ecosystem built. Increasingly, this trusted mobile ecosystem has proven vital for almost every sector of the UK's economy.

Trustworthy transactions are at the heart of this economic ecosystem, and trustworthy transactions are at the heart of this proceeding. Mobile commerce now accounts for roughly 73% of all retail transactions in the UK, and it is the primary interface for the UK's modern service economy. This major shift in adoption and capability has forced traditional industries (like banking, energy, and retail) to invest heavily in a mobile-first infrastructure which is rooted in trust. Trustworthy technologies, including the integrated

payment and transaction systems built into the app ecosystem — have proven to be the foundation upon which global e-commerce, app marketplaces, and UK's digital enterprises are all built.

According to the UK Department for Science, Innovation and Technology (DSIT) Consumer Survey on App Stores, respondents generally have a high-level of trust in and usage of app stores. At this critical moment in time, when AI superhacking models have the potential to put the vital trust that UK users need in their mobile devices on the line, now is not the time to weaken the incentives for a trustworthy mobile ecosystem.

We appreciate that the CMA explicitly outlines how it has considered user trust safety, security and privacy factors in its CR, and appreciate its stated goal: "[o]ur aim seeks to ensure that there are appropriate safeguards to protect legitimate platform interests, including to mitigate genuine risks to Apple's Mobile Platform such as in respect of security and privacy." This is a laudable goal and the CR has taken steps in this direction, but the CR shows significant room for improvements to ensure the outcome leads to a more vibrant, competitive, and trustworthy mobile ecosystem that UK economic prosperity and opportunity now depends on.

2. How CMA Can Address Potential Inconsistencies with Consumer and the UK Government's Trust Priorities.

There are several critical efforts being undertaken that are important to consumers and the UK government to further advance a trustworthy digital ecosystem – efforts that could be impacted or even undermined by the CMA's proposed CR unless clarified and remedied.

At a high level, we have concerns that the CMA's CR is out of sync with critical trust enabling goals in four key areas:

A. **NCSC's efforts to tackle increasingly sophisticated mobile security threats – and the market incentives necessary for its secure by design approach.** The UK is facing increasingly sophisticated, frequent, and expensive cyberattacks aimed at mobile devices that cost the UK economy billions annually. These mobile threats include state-sponsored hackers targeting a range of UK organizations through mobile phone app managers, mobile malware phishing campaigns targeted to breach UK company networks, and a mobile-first attack strategy that has been adopted by bad actors. The need for robust mobile device security has become so critical and intertwined with competition policy that it led the Royal United Services Institute (RUSI) to "[A]dvise competition policy and consumer rights

regulators to account for cybersecurity when making judgements on mobile ecosystems." As these cyber threats have multiplied, the UK's National Cyber Security Center (NCSC) has adopted "secure-by design" guidance for mobile devices. Because of NCSC's concerns that "the market does not currently support and reward those companies that make the investments in and build secure products," it is championing the importance of market incentives as a foundation for enabling a more secure digital ecosystem.

> **Yet, we have concerns that the CMA's CR narrow approach to cost recovery, which disincentivizes critical investments in platformwide integrity, is fundamentally out of sync with NCSC's approach to improve the market incentives necessary for advancing a more dynamic and secure UK digital marketplace.**

B. **CMA's efforts to target subscription traps, and make it easier for people to unsubscribe.** The CMA has adopted new measures aimed at making it easier for consumers to manage and cancel their digital subscriptions. A recent survey by The Harris Poll UK reveals that 89% of UK consumers hold low trust in subscription services, feeling that companies deliberately make cancellation harder than signing up.

> **Yet, rather than address the consumer trust gap, we have concerns that CMA's CR approach would deprive mobile users of a centralized one-stop, one-click subscription tracking management and refund system by excluding certain mobile transactions and subscriptions from the tool's reach. CMA may in fact be making it easier for unscrupulous companies to avoid subscription management features – making subscription cancellation harder without full disclosure to the consumers of the loss of functionality and safeguards, and thus preventing CMA from achieving its goal of enabling trust, transparency, and well-informed consumer choices. This trust gap can be more effectively accomplished in partnership with platform operators like Apple.**

C. **UK Government's efforts to better protect children.** Ofcom research reveals that UK children face financial harm from in-game purchases, highlighted by high rates of overspending, confusion, and buyer's remorse. Over half of UK children (58%) spend money online via gaming or social media, significant numbers of children still overspend or encounter financial harms, a third (32%) of children regret in-game purchases, and 43% regret spending on social media platforms. It's no wonder that more than half of UK parents express worry over their children's online spending behavior and benefit from robust smartphone parental

control tools aimed at online purchasing. Fortunately mobile platforms have created tools and protections that enable parents to manage and limit their children's online activity.

> **While we are heartened to see a carve out for "content harmful to children" in the CR, we are unclear whether it includes parental controls, and have concerns that CMA's CR only "strictly necessary" language does not allow appropriate safeguards, and are concerned that without specific clarification that parent controls and child protection features are allowed, that UK's parents and children could be worse off than those under, for example, Japan's digital markets regime. It also veers into the territory of CMA dictating design choices, which is overreach, and better left to companies who both have the experience to do so, and are closer to consumer feedback.**

D. **UK's national campaign against fraud and scams and Stop! Think Fraud campaign.** The UK has become a hotbed for online consumer scams and frauds – often of mobile phishing campaigns targeting UK consumers with scams that impersonate well-known retail brands and service providers. A recent UK Consumer Security Survey on mobile app security finds:

    a. 62% of UK consumers declared mobile fraud their number one concern,

    b. 80% favour pre-emptive anti-fraud measures

    c. 27% report first-hand experience or second-hand awareness of social engineering scams

    d. 56% of people in the UK now prefer using mobile apps over other channels to buy goods and services

These untrustworthy links are aimed at mobile users (70% of UK consumers have received scam messages appearing to come from trusted sources such as delivery firms, banks or government bodies) and the UK government has invested heavily in a public campaign to better inform consumers to think twice before clicking on risky links. Mobile platforms have invested heavily to prevent and deter fraud, and protect users from scammy and malicious links that take users outside of the trusted app marketplace in order to direct transactions to legitimate looking websites, encourage fraudulent transactions, or to steal personal information or financial credentials.

A time when the UK government this month (July 2026) is attempting explore targeted interventions to better address fraud and the fact that "[t]he UK faces a rapidly evolving fraud threat that causes profound harm to individuals, businesses, and the wider economy," the CMA should not undermine efforts aimed at fraud protection.

> **While the CR includes a carve out for steering restrictions for "preventing malware, fraud, unlawful content" we have concerns that it is too limited by a "strictly necessary" standard rather than "justifiable reasons" standard as Japan has adopted. We have concerns that it doesn't include a broader range of carve out like those in Japan for cybersecurity, privacy, device safety, system integrity, and other illegal content like Japan's, and we are concerned that overall steering options and a limited cost recovery could exacerbate these risks by increasing exposure to untrusted transactions, scams and fraud.**

Because of potential conflict with each of these important UK government objectives, the CMA should take special efforts to align its efforts with these other important trust enabling objectives.

3. How the CMA Can Incentivize a Competitive, Innovative and Trustworthy Mobile Ecosystem in the UK.

Given the CMA's important prior work, its legal mandate, and the significant digital challenges that the UK is currently facing, we were expecting the CR would take a different approach. We were surprised in some key areas that it was either vague, or specifically undermined efforts to advance a more dynamic, competitive and trustworthy digital ecosystem in the UK.

The CMA's limited approach to cost recovery disincentivizes critical investments in platform privacy, safety and security and the foundations of trust.

Under paragraph 12(a)(iv) of the proposed CR, the CMA limits the recovery of costs and a reasonable rate of return strictly to infrastructure and services supporting Native App Distribution that are "to a material and direct extent, causally attributable to providing Native App Distribution" to steering developers. This completely discounts the integrated reality of modern mobile operating systems, and the core privacy, safety and security investments necessary for supporting a trustworthy marketplace. Platform security and privacy features are not siloed; they form an integrated package of complementary services across the entire ecosystem. By legally excluding the general platform investments necessary for enabling a trustworthy platform from fee calculations, the CMA essentially penalizes the platform for maintaining and investing in

broad, system-wide trust enabling privacy, safety and security protections. It's conceptually problematic to be thinking about the marginal cost for enabling steering in a platform defined by the CMA as an integrated ecosystem. There are important investments in trust that should be recoverable regardless of whether an app steers.

The CR's proposed framework would essentially allow multi-billion-dollar third parties (such as Spotify or Epic) to free-ride on a trustworthy ecosystem infrastructure without supporting the investments in trust that makes the market viable and attractive. This kind of free riding, in turn, can starve the platform of the critical investment necessary to fund continuous security engineering, advance new privacy safeguards, and to continuously improve the software development tools and APIs that enable all developers to take advantage of continuously advancing features. It effectively lets developers use these tools, technologies, and distribution systems for free, without paying for them at all.

It also can lead to user confusion and harm where users think they are transacting with the safer Apple environment, while in fact the payment component is separated and less secure. Such an approach does not align with the CMA's stated goal to "ii) support end-users' ability to make informed and effective decisions between purchasing options" (¶2.1)

A long-term reduction in platform feature investment would ultimately degrade the overall breadth and quality of app protections available to UK consumers and businesses, and disincentivize critical new investments in platform privacy, safety and security. A company like Apple that competes in the market based on its trustworthiness is entitled to be compensated for its investments in value, integrity and trust upon which the ecosystem depends, and upon which all app developers are able to build their business and monetize their work.

The approach is also inconsistent with CMA's prior statements, advice and decisions. For example, the CR's approach is inconsistent with the CMA's Final Designation Decision (¶1.15) which found that the "component digital activities of Apple's Mobile Platform" together allow users to access, view and engage with digital content, and that these components "form **an integrated package of complementary services**." … "Accordingly, it is appropriate, for the purposes of arriving at an assessment of SMS under the Act, to consider them together, reflecting their interlinkages."

Likewise, the CMA, through its in-depth studies on Digital Comparison Tools (DCTs) found that non-price factors like platform trustworthiness are critical to how consumers choose services. Its DCT Market Study Final Report argued that "trust" and "quality" are core drivers of competition. CMA, for example, found that "**consumers need sufficient**

trust and confidence to use" the technology in the first place. CMA indicated it would "approach future complaints in the sector in a similar way, prioritising our work to reflect the importance of the sector and of ensuring effective competition and consumer trust."

Likewise, in DMCCA Explanatory Notes, ¶180, "When considering the imposition of conduct requirements the CMA will assess the information and factors that it considers relevant in each case. This could include […] burdens on designated undertakings and third parties, freedom of contract and property rights**, the safety and privacy of users**, and innovation in digital markets" (emphasis added) But it appears that the CMA has not adequately considered the safety and privacy of users.

Even prior to the DMCCA, in November 2021, the CMA and Ofcom provided advice to the government on the application of a code of conduct on what would be fair and reasonable compensation between platforms and content providers. As a part of that advice to government, the CMA did not see there was some notion that the platform's compensation should be constrained to the cost of the provision of incremental service, rather Ofcom and the CMA embraced a joint value approach – an approach that would reflect the value of both participants on the platform. The advice found, "[W]hen platforms and content providers collaborate, value is created for both the platform and the content provider through their relationship." This approach, they suggested, would result in nondiscriminatory outcomes between all platform participants.

The Fallacy of Separating a Platform from its Network Effects.

The CMA's CR directly mirrors the core economic framework and definitions proposed in the 2025 paper by Jorge Padilla and Kadambari Prasad – who note in their paper that they work "on behalf of Spotify." The alignment between the regulatory text and the Spotify-backed paper is striking, particularly in how the CMA defines a "fair and reasonable" steering fee.

In their paper, Padilla argues that network effects are fundamentally a "property of the market" rather than an intrinsic value created by the platform itself. From this premise, he asserts that platform operators should not be permitted to monetize or bake the value of these network effects into their access fees under digital market regulatory frameworks – as the CR has reflected.

However, the argument that network effects belong solely to the market is inconsistent with standard platform economics in several ways. In basic two-sided market literature, network effects do not spontaneously exist in a vacuum; they must be actively catalyzed, orchestrated, and maintained by the platform.

A core flaw in this argument is the attempt to value an app store while ignoring its user base. In a two-sided market, the primary product being sold to developers is access to the aggregated user base. Stating that a platform can only charge for its idiosyncratic technical functionality while treating the user network as an unpriceable externality is economically artificial. Without the curated, secure user base, the underlying app-distribution software has virtually zero economic utility to a developer. The CR intends to exclude a broad range of legitimate costs that the platform would be able to recover in any market economy, without considering whether its app developers (who already retain the vast majority of value jointly created on the platform) are already fairly remunerated and incentivized.

It creates tension with the widely accepted economic principle that the *expectation* of capitalizing on network effects is precisely what drives companies to invest billions to create digital marketplaces in the first place.

While third-party apps certainly make an ecosystem attractive, those apps are simultaneously leveraging billions of dollars in sunk platform R&D, security updates, APIs, and global payment compliance provided by the platform operator. By forcing the platform to net out the aggregate value of *all* developers against a fee charged to an *individual* developer, the framework allows highly profitable apps to free-ride on the ecosystem's collective value while paying utility-rate, cost-plus fees.

The arguments Padilla now makes on Spotify's behalf, and that appear to be mirrored in the CR, are also wholly inconsistent with Padilla's prior advocacy and analysis. For example, in a 2022 paper co-authored by Padilla (Vertical Control Change and Platform Organization under Network Externalities), the authors recognize that network externalities are a variable that the platform actively shapes, signals, and builds through its own corporate strategy and organization.

Furthermore, the CR doesn't establish a sufficient basis for the intervention, as required by the DMCCA. Under s19(5) of the DMCCA, the CMA may only impose a conduct requirement where it can establish that a potential intervention would be proportionate for achieving one or more of three specific objectives: 1) trust and transparency, 2) fair dealing, 3) and open choices. This constitutes a rigorous legal test that the record does not support.. In establishing that it is proportionate, the CMA must weigh the positive and negative effects of any potential intervention, including the potential negative harms and unintended consequences.

To the extent that the CMA were to fully weigh the benefits, it would find that there are very few apps that are in-line to potentially benefit. The debates around payment steering relate to a very small portion of total billings and sales — just 3% — that Apple

earns on digital goods and services transactions — with 97% accruing to developers without any commission owed to Apple. By contrast, the potential negative effects impact the entire ecosystem – by undermining core elements of trust upon which the entire mobile ecosystem depends. These changes are unnecessary for enabling new entrants, are not supported by the evidence, and as we have described can create new consumer harms that undermine trust.

And while the CR supposed purpose is to enhance competition in mobile app distribution, it's impossible that enabling steering link-outs would increase app distribution price regulating the commission rate for a small percentage of hugely profitable apps doesn't increase the competition between those apps either – but it could help these large apps further consolidate an already entrenched music streaming and gaming markets.

In debates between and about trillion-dollar companies and billion-dollar companies, it's often the needs of small start ups and scale ups that get left behind. They are the majority of businesses in the app marketplace and they are the players that 1) ~95% of the time make their apps available for free (making money in other ways) and therefore pay zero commissions at all (and so are not impacted by CMA's steering cost concessions), but 2) are wholly dependent on having a trustworthy marketplace where they can utilize SDKs, coding tools, APIs and overall platform integrity to avoid having to make huge investment in basic security and privacy safeguards. They would be negatively impacted by a scheme that disincentivizes platform-wide integrity and trust.

The CR undermines the core market incentives that the UK's National Cyber Security Center (NCSC) says are essential for the UK's economy and security.

In the NCSC's annual review for 2024, emphasized the importance of market incentives as a foundation for enabling a more secure digital ecosystem – outlining why price alone is not enough to incentivize security. It says, "Put simply, if the majority of customers prioritise price and features over 'security', then vendors will concentrate on reducing time to market at the expense of designing products that improve the security and resilience of our digital world." … "We can improve the overall resilience of systems by encouraging investment in 'secure by design' practices. This is particularly true at the 'foundational layer' of our digital architecture, as any software or systems built on those foundations will benefit." These arguments ring especially true in this context, where investment in 'secure by design' practices is especially essential for enabling a trusted mobile marketplace.

NCSC goes on to argue that we need to create the right market incentives, but "the software and hardware market does not incentivise investment in *security*. The reasons for this are due to a wide set of market behaviours and incentives, including:… a belief by some that the risks of insecure technology and digital infrastructure should be borne by wider society, rather than by those making investment decisions."

"A series of discussion groups, expert panels and academic research led the NCSC to develop an understanding of four key drivers that we believe could shift the incentive structures that underpin technology markets and their attitude to security."

These drivers include "financial reward" which the NCSC argues are a critical market tool to incentivize 'secure by design' technology at the heart of the UK's strategy. They say:

> "Finally, we need to show a clear return on investment in those organisations that invest in foundational security. How can we help organisations measure and compare the costs incurred by vulnerabilities (either through patching, suffering incidents, or some other whole of life cost) with long-term investment in more resilient technologies?
>
> It says, "It is these market fundamentals that need to be addressed if we are to prevent software and hardware vulnerabilities being exploited. … to go further, faster, we need to harness the power of competitive innovation to improve resilience."

Yet it's these "financial rewards" that NCSC describes, that are exactly what the CMA approach will eliminate.

NCSC explains, "Leveraging these drivers to develop policy options would use network effects, the drive for profit and the desire to maintain reputation to incentivise enterprises to prioritise security. We believe that a *range* of incentives are required to encourage commercial enterprises to focus on security for their own benefit, which will mean better security outcomes for everyone." Yet the inability to fully capture these financial network effects, as the CR proposes, undermines the security incentives that the NCSC has argued are essential for the UK's economy.

NCSC's CTO, for example, has specifically raised concerns when technology markets do not reward those technology companies that invest in cyber security. He says, "The ecosystem has the expertise, it has the skills, but the market does not currently support and reward those companies that make that investment and build secure products" …. "When we need to build an ecosystem that's capable of meeting this modern threat, we have to find ways where we can incentivize those vendors to be rewarded for their hard

work, for those that go the extra mile, for those that build the secure technologies which our foundations are going to rely on in the future."

With cyber attacks costing UK businesses billions annually and high-profile incidents such as the Jaguar Land Rover breach exposing critical weaknesses, the Royal United Services Institute (RUSI) has argued that weak cyber security undermines UK economic growth and national security, and has led RUSI to "Advise competition policy and consumer rights regulators to account for cybersecurity when making judgements on mobile ecosystems." At a time when serious cyber incidents cost businesses an average of £195,000, with about half of small firms experiencing one in the past 12 months, officials argue a more interventionist and comprehensive market approach to cyber security is needed.

4. The Technical Requirements Necessary for Achieving a Trustworthy Link-Out Framework

While paying attention to some trustworthy factors, the CMA's lack of clarity could undermine necessary safeguards. Much of the CMA's focus is targeted at link-outs (actionable links that take users outside the app to complete a transaction) as a means for enabling competition by allowing more transactions outside of the integrated billing system. However, as we have seen elsewhere, such interventions create new consumer complexity, duplicative functionality, and introduce new privacy, safety and security issues without creating new competition, enabling consumer savings, or addressing any specific consumer harm. Link-outs to external websites are a well-known exploitable security vulnerability — especially when they link to unvetted, unverified websites that don't belong to the app developer itself.

We appreciate that in the CR, the CMA has outlined "How we have considered user trust, security and privacy factors." We appreciate that the CMA may be attempting to adopt an approach that is more aligned with Japan's MSCA approach, which is a step improvement over Europe's DMA approach that specifically prevented privacy and security safeguards from being implemented as a part of the alternative payment link-outs.

But the CMA's claim that its CR would "support improved customer experience, including in relation to billing, refunds and support" is not substantiated. Despite an attempt at some safeguards, consumers will nonetheless be faced with an increased risk of scams and fraud through alternative payment systems and be deprived of centralized refund management capabilities and subscription tracking features that are not available for transactions made outside of platform payment options. In fact, the

Steering Consultation recognizes that "steering users to third party websites or content introduces an additional party to the user journey, which can introduce additional risks to end-users," but the CMA has not sufficiently mitigated these additional risks.

Link-outs to external websites are a known exploitable vulnerability

Mandating unrestricted link-outs can enable threat actors to harness these links to distribute malicious apps, hijack accounts via fake login pages, expose users to fraudulent scams, or deploy spyware undetected. The open web is a well known hotbed for criminals, scammers and fraudsters. Regulators must always think about the reality of today's online ecosystem — that not everyone is a good actor, or has the consumer's welfare at heart.

The UK's National Cyber Security Centre, for example, has developed extensive resources to "watch out for suspicious links." They say, "Cyber criminals insert malicious links into SMS text messages, emails, and increasingly on social media posts." CMA shouldn't expand this list by also including apps to the list of places where criminals insert malicious links. Why does the NCSC warn about these harms? Because there is already a multibillion industry aimed at tricking people into clicking on things they shouldn't. According to the FBI's Cybercrime report, the number one reported cybercrime involved efforts to get people to click on a legitimate looking but malicious link or URL. Zimperium found that 82% of all phishing sites now target mobile devices. But under the DMA, platforms are being restricted from comprehensively protecting users from scammy and malicious link-outs under the guise of competition law.

According to the UK's Cyber Security Breaches Survey 2025, 85% of businesses experienced a breach or attack in the last 12 months with phishing attacks remaining the most prevalent and disruptive type of breach or attack — efforts to trick users into clicking onto a link that they shouldn't.

Within the UK alone, the government has helped block almost 1 billion attempts to access malicious websites. Given the breadth and prevalence of efforts to get UK consumers to click on untrusted links, the government should be equally concerned that bad actors would try to leverage untrustworthy links in apps too and give this appropriate weight when considering the harms a potential steering intervention.

A. Allowing Consumers to Choose the Most Trustworthy Payment Option. The CMA's proposed CR requires steered transactions to be presented side-by-side with Apple's trusted commerce system. While still creating new risks, this approach nonetheless helps give consumers a better ability to choose the approach that they feel they can

trust, and that best meets their needs. However, we are concerned that consumers can only be provided with a single disclosure screen that contains only "strictly necessary" information that a consumer is transacting outside the safeguards built into the platform.

Users not only need to be kept informed when they are not transacting with the platform's built-in payment system, but they need to know: 1) who they are transacting with, 2) be made aware that they could be faced with an increased risks of scams and fraud through alternative payment systems that introduce an additional party to the user journey, and 3) that they will be deprived of centralized refund management capabilities and subscription tracking features that are not available for transactions made outside of platform payment options. The CR severely limits the platform from objectively describing the security trade-offs of the transaction to the consumer -- including the loss of centralized refund systems and subscription management. Without full disclosure that enables users to understand what functionality applies to their transaction, and who they are transacting with, CMA will be unable to achieve its goal of enabling trust, transparency, and well-informed consumer choices.

It also can lead to user confusion and harm where users think they are transacting with the safer Apple environment, while in fact the payment component is separated and less secure. Such an approach does not align with the CMA's stated goal to "ii) support end-users' ability to make informed and effective decisions between purchasing options" (¶2.1)

B. Allowing for Additional Protection for Children and Tackling Fraud. Paragraph 3(b) of the CR indicates that Apple may only restrict steering if the restriction is strictly necessary for an "objectively justifiable purpose of preventing malware, fraud, unlawful content or content harmful to children." While a step forward, the "strictly necessary" construct will likely result in only the narrowest of consumer and parental protections. By contrast, Japan's MSCA allows companies to take steps "safeguarding youth who use smartphones" — including "measures to establish parental functions in the basic operation software." In practice, this enables parental control tools and means apps in the app store's children's category for users under 13, can't include external transaction link-outs. In addition, Japan importantly appears to include a broader array of exemptions that are also critical to enabling trust including for cybersecurity, privacy, protecting children, devices safety, device performance, and other illicit acts like gambling. This could mean that Japanese children and consumers are being better protected than UK users. We are unsure because there is a degree of ambiguity in the CMA's language. To the extent that these important features are accommodated, the CMA should explicitly confirm that they are in their final result.

Conclusion & Proposed Refinements

To protect the vital incentives that keep the digital ecosystem secure and innovative, the CMA at a minimum must revise its proposed pricing principles. Specifically:

1. **Revise the Cost-Based Approach:** A cost-based approach is unnecessary and inappropriate. By choking the revenue stream that funds this collective security architecture, the CMA inadvertently threatens the long-term safety of the entire UK mobile economy, directly contradicting its own "trust and transparency" statutory objective. At a minimum, paragraph 12(a)(iii) should explicitly recognize that general platform trust architecture, developer tools, and ecosystem governance are common costs *causally relevant* to the existence of all transactions, steered or otherwise, and should be proportionally recoverable.
2. **Recognize Integrated Platform Costs:** General security, app review processes, and developer software development kits (SDKs) are the very reasons consumers feel safe entering the digital marketplace in the first place. Labeling these foundational elements as "unrelated costs" under paragraph 12(b) ignores the reality that without these investments, there would be no traffic to steer. The CMA should strike or heavily modify paragraph 12(b)(ii) to ensure that investments in developer tooling and general platform capability—which directly benefit the developers utilizing steering—are not artificially zeroed out.