16 November 2026

Comments of

TRUSTED FUTURE

To the

United Kingdom's Competition and Markets Authority (CMA)

regarding its

Consultation Response
on the Proposed NFC Access Conduct Requirement
for 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 enhance trust throughout today's digital ecosystem, we welcome this opportunity to provide input to the proposed Conduct Requirement (CR) for Near-Field-Communication (NFC) access on 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 any measure that CMA considers 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.

Trust has emerged as the single currency underpinning the entire mobile payment and digital identification world. The entire ecosystem functions only when every participant—consumers, merchants, and banks—has absolute confidence that transactions are secure, data is private, and unauthorized access is practically impossible. To make this possible, Apple has developed its NFC plus Secure Element infrastructure which relies upon a deeply integrated, hardened hardware and FaceID system which operates like a hardware "vault" to make it immune to external attacks. This tight coupling is what convinces banks to tokenize and authorize card issuance on consumer devices in the first place. But the CR wants to upend this trusted system, and enable a less secure Host-Card Emulation ("HCE") based system which relies on cloud-based credentials and software-level OS processing, making it fundamentally vulnerable to operating system compromises. Requiring Apple to support an HCE solution in the UK - particularly where the right of the CMA to force to Apple to provide and maintain a second alternative technology is not granted by statutory authority - would undermine Apple's ability to ensure robust privacy, security, and performance for contactless transactions, by forcing it to adopt a solution that does not support hardware-based security.

When well-intentioned but misguided regulations intervene into this secure system, they risk unraveling the trusted foundation that underpins the success of the system in two primary ways – 1) it fragments and

weakens the security perimeter, and 2) artificial price controls can freeze the continuous investment necessary to fight an endless arms race against increasingly sophisticated fraud syndicates.

A digital wallet is only as strong as its least secure mandated standard and its most underfunded defense. By forcing technical compromises and strangling reinvestment, unnecessary regulation risks breaking the invisible contract of trust that makes cashless commerce viable.

After a careful review of the proposal, we find the CR's technical mandates create severe security and privacy risks to UK consumers, its price controls will stifle the reinvestment necessary to protect consumers against increasingly sophisticated fraudsters, that this regulatory intervention is unnecessary in a rapidly changing marketplace, and we therefore strongly urge the CMA to reconsider its proposed interventions. Further, the CMA is attempting to exceed its statutory authority by over-reading the authority for 'preventing' an action to mean the authority to force the building and maintenance of technology and subsystems not offered in the UK market. The proposed CR goes well beyond what is needed to achieve the CMA's stated aims, and the evidence the CMA relies on does not support measures of this scope.

Below, we outline our primary arguments against the implementation of the proposed CRs.

1. Regulatory Intervention is Unnecessary in an Actively Evolving Market

The assumption that Apple's platform restricts developer entry is contradicted by current market realities. The Proposed CR is seeking to 'open up' NFC access where such access already exists.

Apple's NFC & SE Platform is already open to interested third-party developers in the UK. It is fully capable of supporting a wide array of use cases, including contactless card payments, account-to-account (A2A) payments, stablecoins, and digital ID. This platform supports a variety of payment methods (like credit and debit cards) as well as everyday non-payment uses—such as digital keys for cars, homes, and hotels, corporate badges, student IDs, loyalty cards, event tickets, and government IDs—meeting all the use cases highlighted in the CR. Dozens of UK-based and international developers have already been authorized or applied to use the platform. Developers are able to offer NFC solutions separate from Apple Pay and Apple Wallet, and to have access to specific functionalities utilised by Apple Pay, including Foreground NFC Access, Field Detect, Double-click, and authentication tools such as Touch ID and Face ID.

There is no concrete evidence that the NFC & SE Platform's technical solutions or fee structures inherently inhibit innovation or investment. The limited uptake of Apple's platform to date may be attributable to a variety of facts. For example, sluggish user adoption can be driven by user satisfaction with available trustworthy solutions, and developer adoption may lag because of satisfaction with existing contactless methods like QR codes, and macroeconomic trends causing firms to deprioritize new NFC solutions. The CR seems to assume that this lack of uptake stems from technical impediments or fee structures. However, both Barclays and PayPal launched proprietary HCE wallets on Android to bypass supposed platform restrictions, but then withdrew them from the market because of weak customer demand. It suggests that the problem is that there just isn't strong consumer demand for such a solution, and a mandate to enable it, as proposed in the CR, is unlikely to substantially increase adoption or guarantee success.

Market-driven ecosystem solutions are solving integration friction. The broader market is already stepping in to ease technical integration. For example, both Mastercard and Visa launched iOS SE Software Development Kits (SDKs) to streamline integration and licensing for banks, fintechs, and merchants, significantly lowering the technical hurdles of developing SE-based wallets without regulatory intervention. The CMA should allow this momentum to develop and grow, rather than prematurely forcing a different technical model now that could leave UK developers stranded.

2. "Utility-Style" Price Controls Will Stifle UK Innovation and Undermine Needed Investments

Imposing rigid, utility-style price controls on dynamic digital platforms threatens ecosystem quality, disincentivizes innovation, and restricts the ongoing investment required to protect users against evolving fraud threats.

The NFC and Secure Element (SE) platform relies on a predictable, value-based commercial structure that provides developers with long-term investment certainty. Forcing a strict, cost-recovery pricing model introduces unnecessary market volatility and disrupts forward planning for digital platform builders.

Traditional cost-based price regulation was originally designed for static natural utilities (like water or electricity networks). Applying these static models to fast-moving, IP-intensive, and security-critical technology platforms misaligns regulatory policy with the realities of modern software ecosystem engineering.

Although the CMA's overarching principles recognize that companies need to monetize IP, recoup R&D investments, and maintain pricing flexibility, the proposed Conduct Requirement in practice effectively bars Apple from charging for its proprietary NFC hardware and software infrastructure. Barring fee models under the logic that they "reduce developer incentives" severely penalizes platform operators and restricts the continuous reinvestment needed to upgrade platform defenses.

Mandating access to Host-Card Emulation (HCE) alongside the hardware Secure Element (SE) prevents platform developers from recovering the substantial capital sunk into building integrated hardware-software security. This dual-track mandate disadvantages developers currently building on high-security hardware and deters future UK-specific platform investment.

Under existing frameworks, third-party developers retain complete control over their end-to-end user experience and retain full freedom to monetize their applications directly through subscriptions, service fees, and value-added features without intrusive regulatory price caps.

3. Mandated Technical Access Creates Severe Security and Privacy Risks

Mandating HCE access introduces critical security and privacy vulnerabilities for UK consumers.

Apple’s NFC and Secure Element (SE) architecture combines hardened hardware and Face ID in a tightly integrated manner to operate as an isolated "vault" immune to external OS compromises. Banks rely on this tight coupling to authorize card issuance. In contrast, HCE processes transactions in software at the OS level and relies on cloud credentials, making it vulnerable to system-level attacks.

Storing credentials centrally in the cloud expands the attack surface, increasing susceptibility to credential theft and fraudulent transactions via infected devices.

Security research has identified hundreds of malicious apps using HCE to impersonate payment terminals and intercept victim data. Zimperiam, for example, found bad actors misusing NFC/HCE solution in a "Tap-And-Steel" scheme to illegally obtain payment data and conduct fraudulent transactions. Their research found more than 760 malicious apps observed in the wild—demonstrating that NFC/HCE relay abuse is not a minor issue, but continues to accelerate.

Likewise, ESET Research found attackers were able to clone NFC data from a victims' physical payment cards using Android HCE malware, and relay this data to an attacker's device, which was then able to emulate the original card, and withdraw money from an ATM. In another example, researchers at Cleafy, Identified SuperCard X malware that used a novel NFC-relay technique, enabling threat actors to fraudulently authorize payments and ATM withdrawals by intercepting and relaying NFC communications from compromised devices.

Bad actors haven't stopped. In just the last few weeks fake Android Apps that in some cases are designed as payment apps like PayPal, Amazon and Zelle, are putting thousands of UK mobile users at risk. McAfee's Mobile Research Team has reportedly identified more than 1,900 malicious applications associated with the malware campaigns targeting more than 90,000 devices in the UK.

Because HCE wallets lack hardware-enforced isolation, they are more vulnerable to these relay attacks. By contrast, Apple's platform isolates payment data from the main OS and lacks reader-mode capability, preventing unauthorized data extraction. The measures proposed in the CR would likely extend potential new NFC relay vulnerabilities to the entirety of the UK's iPhone owning population that have to date been protected from these types of NFC attacks.

Allowing developers to opt for cheaper, lower-security HCE solutions shifts the security and privacy risks onto end users.

4. Severe Degradation of the Consumer User Experience

The CR proposes removing vital control mechanisms, directly threatening the usability of mobile devices.

Granting developers unfettered access to a Default Status API will incentivize them to relentlessly prompt users to meet target conversion rates. This could result in severe over-prompting and user fatigue, leading consumers to blindly accept prompts just to stop the harassment, or to dismiss them without proper consideration. Such access could even lead to aggressive developer behavior, such as blocking users from accessing a third-party app entirely until they agree to set it as the default.

Apple's current presentation and cooldown windows (via the Suppression API) are critical to ensure that a third-party wallet cannot suppress the user's preferred default wallet indefinitely. Diluting these cooldown protections also threatens core device performance, as it forces the smartphone's NFC radio to constantly monitor for nearby readers, leading to rapid battery drain.

5. The CR's Solution Represents a Disproportionate Remedy.

The CMA has a statutory duty to show that the measures are proportionate to meet its stated aims. However, in this case, the CMA is attempting to dictate a UK specific technical architecture by mandating Apple build and support an entirely new parallel HCE solution that Apple does not utilize for its own services. This regulatory demand fails standard legal proportionality tests, as it forces an unprecedented, disproportionate technical burden on the company. The proportionality failure is highlighted, and exacerbated, by the lack of statutory authority to force the use of a second technology, engineer third-party access to technology, and force maintenance of the same - where the technology is not even offered in the UK market – under a stretched beyond reason interpretation that the authority of 'preventing' something (pursuant to Section 20 (3)) means forcing the creation, use, and maintenance of technology that is not offered in the product or service in the UK.

6. Trust has emerged as an essential infrastructure upon which UK digital opportunity is built.

Trustworthy technologies, including the integrated payment and transaction systems built into these devices are a critical foundation upon which the UK's digital ecosystem is built. As mobile devices have become a trustworthy companion, they have become almost ubiquitous throughout our lives, and a cornerstone of the British digital economy. They are now the number one way UK citizens access the Internet. As a result, UK consumers and businesses now rely on the integrity of their mobile devices to protect some of their most sensitive and mission critical aspects of their lives, transactions and businesses.

This trustworthy foundation has been built by the smartphone manufacturers who have made the important investment decisions necessary to build privacy, safety and security into their technologies by design. 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

Conclusion

Trusted Future urges the CMA to recognize that the current NFC & SE Platform already provides a viable, secure, and market-appropriate pathway for developers. The proposed interventions risk destabilizing a highly secure ecosystem and punishing the very innovations that have made mobile payments trusted by UK consumers without any clear or compelling authority to do so.