NFC Access *for Mobile Payments*

Submission to the Competition and Markets Authority (CMA)

Consultation on NFC Access Conduct Requirement: Apple's Mobile Platform

INTEROPERABILITY, SECURITY, AND COMPETITION IN DIGITAL MARKETS



Prepared by **Legal Wings Institute**

Bernardo Fico • João Navas • Thiago Poloni

Legal Wings *institute*

About Legal Wings Institute

Legal Wings Institute is a Brazil-based research and advocacy organization dedicated to the legal, regulatory, and institutional challenges raised by emerging technologies and the digital economy. Its work focuses particularly on the governance of artificial intelligence, data protection, platform regulation, digital rights, competition in digital markets, and the broader relationship between technological innovation and fundamental rights.

The Institute develops applied legal research, policy analysis, and strategic contributions to public and regulatory debates, with particular attention to the Brazilian and Global South perspectives. Its activities include the production of reports, studies, and recommendations, as well as engagement with academics, civil society, regulators, and market actors on questions involving responsible innovation, democratic governance, inclusion, and accountability in digital environments.

Legal Wings Institute seeks to contribute to the development of legal and policy frameworks that are both innovation-oriented and rights-respecting, helping ensure that technological progress is aligned with public interest, legal certainty, and the protection of vulnerable groups.

I. Scope of the submission

This submission examines the Competition and Markets Authority (CMA)'s proposal concerning the terms of access to Near Field Communication (NFC) technology on Apple's mobile platform, focusing on the relationship between interoperability, security and competition in digital markets. In assessing the scope of the proposed intervention, it considers the characteristics of Secure Element (SE) and Host Card Emulation (HCE) architectures, differentiation between technological ecosystems and the proportionality requirements applicable to regulatory obligations.

Section II first considers security as a dimension of competitive differentiation between digital ecosystems, focusing on the protection of credentials afforded by the SE, the different attributes of HCE and the importance of those attributes to service quality and consumer choice, while distinguishing their preservation from restrictions on alternative architectures.

Section III then examines developments in the European Union, Switzerland and Australia. Their different approaches show that access to NFC infrastructure may be promoted through a range of regulatory measures, without assuming that one technological solution is superior in every context.

Finally, Section IV assesses the proportionality of requiring HCE and SE simultaneously, considering the commercial and operational difficulties identified by the CMA, academic literature on interoperability remedies and the CMA's own guidance. It considers whether improvements to SE access and access to both architectures would achieve the intended competitive outcomes, taking account of their respective benefits and burdens.

II. Security as a dimension of competitive differentiation between digital ecosystems

In an earlier submission to the Competition and Markets Authority (CMA), concerning the consultation on app store rules, Legal Wings Institute observed that competition in mobile device markets takes place both within each ecosystem (*intra-ecosystem competition*), through rivalry between service providers and developers, and between distinct ecosystems (*inter-ecosystem competition*), whose value propositions may appeal to different groups of consumers. That submission noted that security, privacy, technological integration and freedom of choice are dimensions of *non-price competition* on which platforms compete. An assessment focused solely on increasing the options available within a particular ecosystem may therefore overlook important effects on competition between platforms.[1] Conversely, competition between ecosystems does not establish that restrictions on rivalry within an ecosystem are necessary to preserve those attributes. The assessment should distinguish benefits attributable to the architecture from restrictions on access that may not be needed to preserve them.

This distinction places non-price attributes at the centre of the competitive assessment of digital ecosystems, as security, privacy, integration and openness affect the user experience

[1] Legal Wings Institute, Competition in Digital Ecosystems of Mobile Devices: Competitive Trade-offs in Mobile Device Operating Systems (submission to the Competition and Markets Authority, May 2026) 7–9, especially 9.

and the relative attractiveness of services. Some consumers may value close integration between hardware and software, together with specific safeguards for credentials, while others may prefer environments offering greater flexibility in their choice of apps and features. The coexistence of different approaches to technological organisation is itself an expression of competition.

Quality differentiation also extends to the architectural choices underpinning each ecosystem, since the integration of hardware and software, the protection of credentials and the access terms offered to third parties influence incentives to invest and innovate. Apple adopts a model involving closer integration and greater control over certain components, whereas the Android ecosystem accommodates a wider range of solutions implemented by manufacturers and developers. Both, however, provide security and openness mechanisms whose scope depends on the application concerned.

The coexistence of these distinct strategies helps preserve diversity of supply, allowing platforms to compete on security, convenience and freedom of choice. This perspective is particularly relevant to contactless communication: although Secure Element (SE) and Host Card Emulation (HCE) architectures both enable NFC-based services, they have different properties and implementation requirements. Those differences should be considered when assessing the quality attributes on which ecosystems compete.

Although consumers do not choose a mobile device solely on the basis of the architecture used for contactless payments, decisions at this infrastructure layer contribute to the security and reliability offered by the platform. Credential protection, transaction integrity and the integration of authentication processes form part of consumers' perception of quality. The use of the SE should therefore be assessed as a technological choice with potential competitive implications, rather than merely as an internal mechanism through which apps operate.

NFC enables short-range wireless communication, while SE and HCE refer to different ways of organising certain operations that use it. The SE uses a protected hardware component to store credentials and perform sensitive operations in an environment isolated from the main operating system. HCE, by contrast, enables cards to be emulated by the host system, relying on complementary safeguards such as tokenisation, encryption and the protection of credentials in external infrastructure. These differences do not, in themselves, determine the overall security of an application, but they affect credential management, authentication controls and exposure to different categories of risk.[2]

At paragraph 5.68 of the consultation document, the CMA notes that the hardware-based protection afforded by the SE may be suitable for applications involving credentials subject to stringent security requirements. This is relevant because functional equivalence between payment solutions does not necessarily eliminate architectural differences that may matter for other use cases. The CMA draws on this distinction to support allowing developers to choose the technology best suited to their needs. It also provisionally considers that HCE-specific risks can be effectively mitigated and that residual additional security and privacy risks are likely to be low. A regulatory assessment should therefore address the safeguards proposed for iOS and

[2] Competition and Markets Authority, NFC Access Conduct Requirement: Apple's Mobile Platform (Consultation Document, 20 October 2026) paras 1.11–1.12; Android Developers, 'Host-based Card Emulation Overview' <https://developer.android.com/develop/connectivity/nfc/hce> accessed 13 November 2026.

the requirements of each application, rather than infer the case for restricting access from architectural differences alone.[3]

The risks associated with these architectures are also examined by the National Institute of Standards and Technology (NIST), the US federal agency responsible for developing technological standards and guidance. In its *Mobile Threat Catalogue*, NIST notes that HCE-based payment applications do not benefit directly from the protection provided by storing cryptographic keys in a Secure Element. They must therefore employ specific mechanisms to safeguard the confidentiality and integrity of sensitive information at application level. NIST also identifies greater exposure to compromise on rooted or jailbroken devices, that is, devices on which operating-system security restrictions have been bypassed to obtain privileged access to normally protected functions and information. These findings highlight the relevance of isolating credentials in protected hardware against certain threats, while recognising that modern HCE implementations may employ additional controls capable of mitigating the risks identified.[4] These threat descriptions identify risks and mitigation needs.

The U.S. Payments Forum likewise identifies this distinction, observing that HCE solutions do not offer the same physical tamper resistance as a dedicated Secure Element and therefore require additional safeguards. Among the measures it discusses specifically for HCE are transaction restrictions based on amounts, countries, merchants and payment channels, intended to reduce fraud risk; the report does not set out equivalent recommendations for the SE. Where applied, such restrictions may limit certain transactions available to consumers. Their practical significance depends on implementation and should be compared with the costs, controls and restrictions associated with SE-based services.[5]

The importance of isolating credentials in hardware is also apparent in initiatives undertaken by public financial institutions. A Bank of England report published in April 2025 on experiments with offline payments for a potential digital pound provides an example. All four solutions examined used Secure Elements to protect cryptographic keys or help prevent counterfeiting and double spending, demonstrating a use case in which the architectural choice responds to specific security requirements. Although these experiments do not establish the universal superiority of the SE, they indicate that hardware-based protection remains relevant to certain services and, in mobile devices, may form part of legitimate strategies for differentiation based on security and reliability.[6]

HCE may nonetheless offer benefits of a different kind. A white paper published by the Smart Card Alliance Mobile & NFC Council explains that, because credentials need not be stored in a Secure Element owned and controlled by another party, HCE removes the commercial, roadmap and brand dependencies. In its conclusions, however, the same paper

---

[3] Competition and Markets Authority (n 2) paras 5.67–5.72.

[4] National Institute of Standards and Technology, 'Host Card Emulation Application Attacks' (Mobile Threat Catalogue, PAY-5) <https://pages.nist.gov/mobile-threat-catalogue/payment-threats/PAY-5.html> accessed 13 November 2026.

[5] U.S. Payments Forum, Update: Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions (version 2.0, December 2025) 17–19, ss 4.1–4.1.2.

[6] Bank of England, Digital Pound Experiment Report: Offline Payments (10 April 2025) 'Project overview' and 'Risk management' <https://www.bankofengland.co.uk/report/2025/digital-pound-experiment-report-offline-payments> accessed 13 November 2026.

presents these advantages as trade-offs against the SE model, acknowledging that HCE may involve a less secure implementation and, in some cases, a degraded user experience.[7] Lower barriers for independent providers may therefore be obtained at some cost to security and service quality, the extent of which depends on the safeguards adopted and the security requirements of each use case.

The evidence examined shows that security is an important dimension of competitive differentiation between digital ecosystems, as technological architecture affects credential protection and service reliability. In this context, the Secure Element represents a differentiation strategy based on dedicated hardware protection, contributing to *non-price competition* both between ecosystems (*inter-ecosystem competition*) and among market participants. HCE, by contrast, reflects a different balance, favouring autonomy and openness for service providers at some cost to the level of protection and, in some cases, the user experience.

Neither architecture is therefore inherently superior, and any regulatory decision should weigh the distinct costs and benefits of each option across these dimensions, including security, reliability, user experience, openness and conditions of entry, having regard to the requirements of each use case.

III. Opening access to NFC infrastructure and international competition policy approaches

The importance of security and technological differentiation to competition between ecosystems calls for an assessment of regulatory approaches to widening access to NFC infrastructure. The choice of intervention may affect both opportunities for independent providers to enter the market and the attributes offered to consumers. Developments in the European Union, Switzerland and Australia reveal different approaches to access to HCE and SE, helping to assess whether opening a particular architecture is an appropriate way to address competitive barriers or whether other measures may achieve comparable results.

The European Union provides the principal example of opening NFC functionality through HCE on iOS. In July 2024, the European Commission made binding commitments offered by Apple to enable independent contactless payment services to operate without relying on Apple Pay or Apple Wallet. Intended to apply for ten years, the commitments provided for free access to the relevant functionality, objective and non-discriminatory eligibility criteria, authentication arrangements and mechanisms for selecting a default wallet, with the aim of reducing barriers faced by independent providers across the European Economic Area.[8]

In a response submitted to the Australian Parliament on 27 March 2026, Apple stated that six independent HCE-based wallet apps were available on the App Store in the European Economic Area, approximately twenty months after the European Commission's decision. These launches show that independent providers have entered following the opening of HCE

---

7 Smart Card Alliance Mobile & NFC Council, Host Card Emulation (HCE) 101 (MNFCC-14002, August 2014) 16–17, s 3.4, and 25, s 6 <https://www.securetechalliance.org/wp-content/uploads/HCE-101-WP-FINAL-081114-clean.pdf> accessed 16 November 2026.

8 European Commission, 'Commission Accepts Commitments by Apple Opening Access to "Tap and Go" Technology on iPhones' (Press Release IP/24/3706, 11 July 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3706> accessed 13 November 2026.

access. Assessing the scale and competitive impact of that entry would require evidence on adoption, usage and the services available to consumers.[9]

The European approach thus represents an enforceable commitments regime for technological access, through which the European Commission sought to foster competition by requiring HCE to be made available to independent developers. This approach, centred on introducing an alternative architecture for NFC access, offers a useful comparison with other jurisdictions which, faced with similar competition concerns, have focused on assessing the commercial and operational terms of access to existing infrastructure, without so far requiring a second architecture to be made available.

In Switzerland, competition enforcement has focused on the terms of access to Apple's NFC & SE infrastructure, which was opened to independent developers in late 2024. In December 2025, the Secretariat of the Swiss Competition Commission (COMCO) announced a preliminary investigation into whether Apple's terms might restrict competition between digital wallets. It acknowledged the European HCE commitments and, given its preliminary nature, has not imposed any remedy, whether concerning SE terms or HCE access. The investigation concerns the conditions for using SE-based infrastructure and their potential effects on competing providers, without prejudging what remedy, if any, may ultimately be necessary.[10]

The Swiss investigation identifies the commercial, contractual and operational terms of SE access as a subject for scrutiny. Its preliminary status does not establish that improvements to those terms would be sufficient, or that access to an additional architecture would be unnecessary.

The Australian debate also reflects an approach different from that adopted by the European Union. In its June 2026 report, *A Level Paying Field*, the parliamentary committee expressly considered the European opening of access through Host Card Emulation (HCE), including the competitive advantages identified by banks and developers. Its recommendations did not, however, require that architecture to be made available. Instead, they focused on reviewing the terms of access to Near Field Communication (NFC) and Secure Element (SE) technologies. The committee recommended that Australia's competition authority examine fees, contractual terms and restrictions on access, and that the government consider intervention allowing those technologies to be used without commercial agreements with Apple. These recommendations identify potential measures for improving access to existing infrastructure.[11]

The Australian regulatory debate also includes alternatives to mandated HCE access, as demonstrated by the Reserve Bank of Australia's (RBA) review of payments system regulation. In October 2026, the RBA published a summary of submissions received in its consultation,

---

[9] Apple Pty Limited, 'Follow Up Questions from Hearing of 24 February 2026' (response to the House of Representatives Standing Committee on Economics, 27 March 2026) 8, question 14.

[10] Swiss Competition Commission, 'The Secretariat of COMCO Launches Preliminary Investigation into NFC Access on Apple Devices' (11 December 2025) <https://www.weko.admin.ch/en/newnsb/egoLzxP2rT6G265nJvqnA> accessed 13 November 2026.

[11] House of Representatives Standing Committee on Economics, A Level Paying Field: Report on the Inquiry into Schemes, Digital Wallets and Innovation in the Payments Sector (June 2026) paras 4.81–4.86, recommendations 7–8.

bringing together proposals from banks, fintechs and other market participants concerning access to Apple's NFC infrastructure. Suggestions included fair, reasonable and non-discriminatory terms, revisions to fees and contractual requirements, phased intervention and, from some respondents, adoption of the European HCE access model. Although the RBA did not adopt a final position in that document, the range of proposals shows that improving access to existing infrastructure forms part of the Australian debate alongside proposals for HCE access and it does not establish a regulatory preference or the relative effectiveness of either approach.[12]

Taken together, these international experiences demonstrate that NFC interoperability may be promoted through different regulatory approaches, depending on market characteristics and the competitive barriers identified in each jurisdiction. While the European Union adopted commitments requiring HCE access, Switzerland and Australia have examined alternatives involving improvements to the commercial and operational terms of access to NFC & SE infrastructure. This diversity highlights the importance of tailoring intervention to the circumstances of each market, taking account of the effectiveness and proportionality of the available measures. These developments are at different procedural stages and identify options for comparison. It is therefore appropriate to assess how both SE reform and access to both architectures would address the barriers identified in the UK, using comparable criteria for effectiveness and proportionality.

IV. Proportionality and the comparative assessment of NFC access remedies

Determining an appropriate regulatory response to access to NFC technology requires, first and foremost, identifying the approach most likely to promote effective competition without overlooking the technological attributes that differentiate digital ecosystems. As discussed above, rivalry between platforms extends beyond the number of apps available in each environment to include security, reliability and service integration. International experience also shows that authorities may address similar barriers through different measures. The central question for the CMA's proposal is therefore whether simultaneous access to HCE and SE is necessary to meet the intended competition objectives, or whether improving the terms of access to existing infrastructure could achieve equally effective outcomes with lower overall burdens. Preserving differentiation should encompass the scope for independent providers, as well as others agents in the ecosystem, to innovate.

This choice must be assessed against the legal framework governing the CMA's own interventions. Section 19(5) of the Digital Markets, Competition and Consumers Act 2024 requires the imposition of one or more conduct requirements to be proportionate to the statutory objectives of fair dealing, open choices, and trust and transparency, while section 19(10) requires particular regard to be had to the likely benefits for consumers. It is therefore not enough that a measure might, in the abstract, widen third-party access. There must be a

[12] Reserve Bank of Australia, Review of Payments System Regulation: Summary of Submissions to the Issues Paper (October 2026) section 3.1.

justified relationship between the competition concern identified, the outcomes sought and the extent of regulatory intervention.[13]

These principles are developed in the CMA's *Digital Markets Competition Regime Guidance* (CMA194), which explains the application of the new digital markets regime and whose criteria are also reflected in Appendix A to the NFC consultation document. In paragraphs 3.33–3.35, specifically addressing conduct requirements, the CMA explains that obligations should be effective, should not impose burdens greater than necessary and should be the least onerous option where equally effective alternatives exist. They should also avoid disadvantages disproportionate to their purpose. The guidance further requires consideration of the effects on the designated undertaking, third parties and consumers, including adaptation costs, security, privacy and innovation.[14–15]

In *Antitrust Interoperability Remedies*, Herbert Hovenkamp examines both the benefits and the limits of compelled interoperability as a competition remedy, recognising its potential to facilitate entry and rivalry, while highlighting how excessively broad obligations may reduce product differentiation and undermine the diversity of solutions available in the market. He argues that intervention should focus on assets whose opening is necessary and capable of delivering competitive benefits, while preserving opportunities for rivalry in other respects. Applied to the CMA's proposal, this approach supports assessing which obstacles could be addressed by improving the commercial and operational terms governing the SE and what additional benefits HCE access could deliver.[16]

Apple's NFC & SE Platform, available in the United Kingdom since October 2024, provides a concrete basis for this comparison. It enables independent contactless payment services and other NFC use cases, subject to authorisation, contractual, integration and security requirements. The existence of the platform does not mean that current access is sufficient: the CMA identifies fees that may make commercial entry unviable for certain providers, insufficient transparency concerning contractual provisions, uncertainty over the time required for authorisation and substantial development and certification costs for SE-based applications. These issues show that effective competition depends not only on the technical availability of the technology but also on the economic and operational conditions under which third parties can use it.[17]

---

[13] Digital Markets, Competition and Consumers Act 2024, ss 19(5), 19(10) <https://www.legislation.gov.uk/ukpga/2024/13/section/19> accessed 14 November 2026.

[14] Competition and Markets Authority, Digital Markets Competition Regime Guidance (CMA194, 19 December 2024) paras 3.33–3.35 <https://assets.publishing.service.gov.uk/media/6762f4f6cdb5e64b69e307de/Digital_Markets_Competition_Regime_Guidance.pdf> accessed 14 November 2026.

[15] Competition and Markets Authority, NFC Access Conduct Requirement: Apple's Mobile Platform (Consultation Document, 20 October 2026) Appendix A, paras A.3–A.5.

[16] Herbert Hovenkamp, 'Antitrust Interoperability Remedies' (2023) 123 Columbia Law Review Forum, section VI.A, 'Product Differentiation and Excessive Interoperability' <https://columbialawreview.org/content/antitrust-interoperability-remedies/> accessed 14 November 2026.

[17] Competition and Markets Authority (n 3) paras 1.13–1.18, 4.22–4.29 and 4.214–4.229; Apple Developer, 'NFC & SE Platform for Secure Contactless Transactions' <https://developer.apple.com/support/nfc-se-platform> accessed 14 November 2026.

The difficulties identified in the CMA's consultation, particularly those concerning fees, contractual requirements, transparency and authorisation procedures, point to an important distinction in the design of a competition remedy. Several of these barriers arise from the terms on which third parties are permitted to access NFC technology. Transparent, reasonable and non-discriminatory requirements can address those barriers under either architecture. Other barriers, including development and certification costs, may vary by architecture and affect how quickly independent providers can enter.[18]

The European Union's experience illustrates this concern, since opening NFC access through HCE also required technical and operational improvements. Before the commitments were finally approved, changes were needed to functionality, eligibility criteria and access procedures. Even after July 2024, implementation remained subject to updates and monitoring, demonstrating that making a new architecture available does not, in itself, remove the challenges of providing effective market access. The terms and procedures for access should therefore form part of the assessment of both SE reform and dual access.[19]

International experience and the obstacles identified by the CMA therefore reinforce the need to assess how improvements to SE access and the availability of HCE would affect entry across different NFC use cases. Under the CMA's own proportionality criteria, intervention should seek effective competitive outcomes with no greater burden than necessary, preserving security, technological differentiation and incentives to innovate, without mandating HCE where less extensive measures could achieve the same objectives.

V. Conclusion

Promoting NFC interoperability requires recognition that competition in digital markets is not confined to the entry of new providers within a particular ecosystem; it also encompasses rivalry between platforms and their ability to offer technologically differentiated solutions. In this context, the security afforded by the Secure Element (SE) is a relevant dimension of quality-based competition, whose preservation contributes to the diversity of technological models available to consumers. Competition intervention should therefore remove unjustified barriers to access without unnecessarily undermining characteristics that differentiate ecosystems or incentives to innovate.

International experience shows that opening access to NFC infrastructure can involve different regulatory approaches and that mandating Host Card Emulation (HCE) is not a universal prerequisite for promoting competition. The Competition and Markets Authority's (CMA) consultation identifies commercial and operational barriers to accessing SE infrastructure several of which arise from the terms on which third parties may use that infrastructure. The difficulties identified support examining whether those restrictions can be addressed directly before requiring access through another architecture. The opening of HCE access in the European Union enabled some independent providers to enter the market. Entry alone does not establish the extent of the benefits for consumers, and work to improve the

[18] Competition and Markets Authority (n 3) paras 4.22–4.29 and 4.214–4.229.

[19] European Commission, 'Commission Accepts Commitments by Apple Opening Access to "Tap and Go" Technology on iPhones' (IP/24/3706, 11 July 2024); CMA (n 3) para 5.58(d).

technical and operational conditions of access continued after the opening. This concern is consistent with the CMA's own institutional guidance, which expressly recognises proportionality as a central consideration in its interventions in digital markets. In its*Digital Markets Competition Regime Guidance*, the CMA states that, where equally effective alternatives are available, the option imposing the least burden should be preferred. This reinforces the importance of comparing improvements to existing infrastructure with broader technological obligations, in order to identify which can achieve the intended competition objectives with the least burden.

Accordingly, improving the terms of access to SE infrastructure should be considered as a central regulatory alternative, through a review of fees, contractual requirements and authorisation procedures that hinder its use by independent developers. Under the principle of proportionality, requiring both architectures simultaneously would be justified where its additional competitive benefits outweigh the additional burdens of more extensive intervention. This would allow regulatory action to focus on the barriers actually identified, while preserving competition based on security, quality and innovation among market participants and across digital ecosystems.

References

Android Developers, 'Host-based Card Emulation Overview' (Android Developers).

Apple Developer, 'NFC & SE Platform for Secure Contactless Transactions' (Apple Developer).

Apple Pty Limited, 'Follow Up Questions from Hearing of 24 February 2026' (response to the House of Representatives Standing Committee on Economics, 27 March 2026).

Bank of England, *Digital Pound Experiment Report: Offline Payments* (10 April 2025).

Competition and Markets Authority, *Digital Markets Competition Regime Guidance* (CMA194, 19 December 2024).

Competition and Markets Authority, *NFC Access Conduct Requirement: Apple's Mobile Platform* (Consultation Document, 20 October 2026).

Digital Markets, Competition and Consumers Act 2024, c 13.

European Commission, *Case AT.40452, Apple Mobile Payments* (Commitments Decision, 11 July 2024).

European Commission, *Case M.10262, Meta/Kustomer* (Commission Decision, 27 January 2022).

European Commission, 'Commission Accepts Commitments by Apple Opening Access to "Tap and Go" Technology on iPhones' (Press Release IP/24/3706, 11 July 2024).

European Commission, *Report on Competition Policy 2024* (2025).

House of Representatives Standing Committee on Economics, *A Level Paying Field: Report on the Inquiry into Schemes, Digital Wallets and Innovation in the Payments Sector* (June 2026).

Hovenkamp H, '*Antitrust Interoperability Remedies*' (2023) 123 *Columbia Law Review Forum* 1.

Legal Wings Institute, *Competition in Digital Ecosystems of Mobile Devices: Competitive Trade-offs in Mobile Device Operating Systems* (submission to the Competition and Markets Authority, May 2026).

National Institute of Standards and Technology, 'Host Card Emulation Application Attacks' (*Mobile Threat Catalogue*, PAY-5).

Reserve Bank of Australia, *Review of Payments System Regulation: Summary of Submissions to the Issues Paper* (October 2026).

Smart Card Alliance Mobile & NFC Council, Host Card Emulation (HCE) 101 (MNFCC-14002, August 2014).

Swiss Competition Commission, 'The Secretariat of COMCO Launches Preliminary Investigation into NFC Access on Apple Devices' (11 December 2025).

U.S. Payments Forum, *Update: Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions* (version 2.0, December 2025).