NOTICE OF FILING

Details of Filing

Document Lodged:	Outline of Submissions
Court of Filing	FEDERAL COURT OF AUSTRALIA (FCA)
Date of Lodgment:	20/02/2026 4:17:01 PM AEDT
Date Accepted for Filing:	20/02/2026 4:16:59 PM AEDT
File Number:	NSD1288/2025
File Title:	CPC PATENT TECHNOLOGIES PTY LTD (ACN 615 736 028) v APPLE PTY LIMITED & ANOR
Registry:	NEW SOUTH WALES REGISTRY - FEDERAL COURT OF AUSTRALIA

Registrar

Important Information

This Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date of the filing of the document is determined pursuant to the Court's Rules.

No. NSD 1288 of 2025

Federal Court of Australia
District Registry: Victoria
Division: General

On appeal from the Federal Court

CPC PATENT TECHNOLOGIES PTY LTD (ACN 615 736 028)
Appellant

APPLE PTY LIMITED (ACN 002 510 054) and another
Respondents

Apple's outline of submissions - appeal and notice of contention

A. OVERVIEW

1. The Appellant (**CPC**), in its notice of appeal (**NOA**) and written submissions dated 2 February 2026 (**AS**), fails to identify any error by the primary judge (**PJ**) in *CPC Patent Technologies Pty Ltd v Apple Pty Ltd* [2025] FCA 489 (**Reasons**). Instead, CPC seeks merely to reargue that the **Apple Devices**[1] infringe the **Asserted Claims**.[2] The PJ, after enjoying the advantage of a three-week hearing, and receiving detailed technical engineering fact and expert evidence over nine days,[3] correctly construed the Asserted Claims, and held the Apple Devices fell outside them. The appeal should be dismissed, with costs.[4]

B. CONSTRUCTION and INFRINGEMENT

B.1 Controlled item (NOA grounds 1 & 6(a)-(b))

2. Claim 1 of the 168 Patent[5] requires that the "*receiver sub-system*" (**RSS**) must be able to provide "*secure access*" to the "*controlled item*", dependent upon an "*accessibility attribute*" (**AA**) provided by the "*transmitter subsystem*" (**TSS**): Reasons [104]. Logically, the controlled item must be a thing to which the RSS can provide access, defined by the AA. The body of the specification identifies, as examples of the controlled item, a "*door lock mechanism*" on a secured door (i.e. not the room/building) or "*an electronic key circuit*" in a computer (i.e. not the computer itself).[6] The PJ correctly construed the controlled item as a "*single discrete item*" to which the claimed system defined by the other integers "*may (or may not) grant access*"; it cannot comprise "*multiple sub-items which may require additional authentication*": Reasons [106], [111] (cf. NOA [1], AS [9]).

3. At **AS [7]**, CPC contends that the "*controlled item … is not a 'single locking mechanism'*" and "*access is not granted to a locking mechanism, this serves no purpose*". However, the 168 Patent at 10:18-23 states: "*The controlled item 111 can be a door locking mechanism on a secure door",* and granting access to a locking mechanism has the evident purpose of operating the mechanism.

4. At **AS [8]**, CPC relies upon aspects of the specification that do not support its contentions. 15:1-4 does not describe the "*one of a number of secure doors"* as the "*controlled item*", but in any event, it only describes access to a particular door (not the room/building) by operation of the system. 12.18-21 concerns access to the controlled item *in* a PC, namely the "*electronic key circuit*", after which the user will access the functionality of the PC. 28.14ff describes the

---

[1] As identified and defined in Reasons [7].
[2] Claims 1,2, 3, 5 and 6 of Australian Patent No. 2004301168 (**168 Patent**) and claims 1, 27, 29, 37, 39 and 41 of Australian Patent No. 2009201293 (**293 Patent**) (collectively, the **Patents**).
[3] *Globaltech Corp Pty Ltd v Australian Mud Company Pty Ltd* [2015] FCAFC 162; (2019) 145 IPR 39, [106].
[4] Including by reason of the matters raised by the Notice of Contention (**NOC**), addressed below.
[5] Neither party suggested that "*controlled item*" had a different meaning in other Asserted Claims: Reasons [99].
[6] 168 Patent 10:18-23 (Appeal Book Part C (**Pt C**) Tab 28 AB-1014); as identified at Reasons [107].

possibility of the "*system*" providing access to different items; however, this does not suggest that the controlled item may be anything to which the RSS is unable to grant access. Contrary to AS [9], the claims require the provision of secure access to the "*controlled item*", not a *part* of that item. The specification is entirely consistent with that.

5. The proper construction of "*controlled item*" is dispositive of appeal grounds 6(a)-(b) concerning infringement: Reasons [372], [375], [376]. In any scenario, the "*controlled item*" is not the Apple Devices, but the particular item (such as the home screen: Reasons [374]-[375]) to which a user seeks, and the FaceID or TouchID biometric security system is able to grant, access.[7]

B.2 Accessibility attribute (AA) (NOA grounds 2, 6(d)-(e), 7(c); NOC ground 3)

6. **Construction:** It was not in dispute below that the AA must establish "*whether and under which conditions*" access to a controlled item is granted to a user: Reasons [112]. However, CPC contends that the AA: *(i)* may be mere "*confirmation*" of a biometric match; *(ii)* need not contain conditions of access; and *(iii)* may be satisfied by user selected conditions.[8] Each of those contentions are wrong: Reasons [121]-[122].

7. *First*, the claim language provides that the AA is only provided (or output) "*if*" a "*legitimate*"[9] or "*matching*"[10] biometric signal is received (or that "*matching is authenticated*"[11]). Accordingly, the receipt of a matching biometric signal is a *precondition* to the provision of an AA (cf. AS [12],[13]). The PJ correctly held that this precondition "*equated to a biometric match*": Reasons [121]. The experts agreed.[12]

8. *Second*, the claim language makes clear that the AA is then provided in response to the biometric match; *ergo*, it is not mere confirmation of the match: Reasons [122]. CPC's criticism at AS[11] of the PJ's use of the word "*conveys*" is misplaced. The PJ held that the AA must "*establish*" whether and under which conditions access is granted, and the claims require that the AA is provided or output, which is synonymous with "*conveyed*": Reasons [122], [429].

9. *Third*, consistently with the above, the specification explains that "***authentication** of the biometric signature matching **produces** an accessibility attribute*".[13] AS[14] contends that this phrase does not require the biometric match and production of the AA to be "*entirely separate*"

[7] E.g., the process of obtaining access to Apple Wallet is independent of the process of obtaining access to the home screen of the Apple Device, using different hardware and software components: Reasons [255],[256], Exhibit 9 Tab 2 (unlocking an Apple Device), Tab 3 (Apps and Protected Operations) & Tab 4 (Apple Wallet) (Pt C Tab 63 AB-1769-1771), Dunstone T811.23-29 (Pt C Tab 91 AB-3425).
[8] NOA [2(a)-(d)].
[9] 168 Patent, claims 1 & 2
[10] 168 Patent, claims 3, 5 & 6.
[11] 293 Patent, claims 1, 27, 29, 37, 39 and 41.
[12] Boztas at T542.36-37, T542.43-45 (Pt C Tab 89 AB-3156), T672.17-22 (Pt C Tab 90 AB-3286); Dunstone at T434.22-24; T512.42-43; T517.11-15 (Pt C Tab 88 AB-3048, 3126, 3131); T529.27-31 (Pt C Tab 89 AB-3143).
[13] See, for example: 168 Patent 14:18-19 and 20:19-21.3 (Pt C Tab 28 AB-1018, 1024) explaining Figure 7; Reasons [124].

– but does not explain why. The experts agreed that it is "*successful* ***biometric authentication*** [that] ***produces*** *an Accessibility Attribute*".[14]

10. *Fourth*, a user selected "*control option*" is not an AA: Reasons [134]-[138]. CPC's contention to the contrary (NOA [2(c)] and AS [14]) is incompatible with: *(i)* the claim language, which *requires* the TSS to provide (or output) an AA in response to a biometric match; it is not open to a user to "*select*" one (or not); *(ii)* the specification, which expressly distinguishes between a "*control option*" (which a user can "*select*")[15] and an AA (which is produced by "*authentication of biometric signature matching*"[16]); and *(iii)* the evidence of the experts.[17]

11. **As to infringement**: *First,* if the PJ was correct to have rejected CPC's argument that the "*controlled item*" is the Apple Device as a whole, then CPC's argument as to the presence of an AA in the Apple Devices must fail: Reasons [439]-[440]. This answers NOA [6(e)].

12. *Second*, and in any event, there is no AA in the Apple Devices which determines whether "***and under which conditions***" access is granted to any controlled item, whether it be an Apple Device or lock screen.[18] The outcome of biometric authentication using FaceID or TouchID is always the same and is binary – access is either granted or denied.[19] Any requirement for a *separate* authentication process to obtain access to apps or Apple Wallet is established independently by pre-existing security policies, it is *not* imposed in response to, or affected by, biometric authentication.[20]

13. *Third,* to the extent that CPC contends that the AA is the unlock token or credentials provided in **steps 20, A20 and W20** (NOA [6(e)]; Reasons [431]) these are transmitted *between* components (e.g. SBIO to SKS) which CPC alleges to comprise the TSS,[21] and are therefore not "*provided*" or "*output*" by, or "*received from*", the alleged TSS, as required (see NOC [3(a)]). To the extent that CPC contends, alternatively, that the AA should be deemed as **"*continuing*" until steps 28**

---

[14] JER 1 at [10] (Pt C Tab 72 AB-2042). See also: Boztas at T668.12-38; T671.19-25 (Pt C Tab 90 AB-3282, 3285).
[15] 168 Patent 15:1-4 (Pt C Tab 28 AB-1019).
[16] 168 Patent 14:16-18 (Pt C Tab 28 AB-1018).
[17] Boztas at T672.1-5 (Pt C Tab 90 AB-3286); Dunstone 2 [202] (Pt C Tab 43 AB-1385). Boztas 1 [63], [111] (Pt C Tab 35 AB-1210, 1214).
[18] Cf. NOA[6(c)-(d)]. In the Apple Devices, the outcome of any biometric authentication "*will only determine whether access is to be granted to the item to which the user seeks access*", but will **not** determine any conditions: Reasons [442]. Furthermore, the particular item to which access is sought is determined by a selection made by the user *before* the presentation of a biometric, that is, by a precondition: NOC [3(d)]; Boztas at T835.9-15; T831.24-T832.40 (Pt C Tab 91 AB-3449, 3445-3446).
[19] Boztas at T817.37-818.32; T821.25-822.4; T824.45-T825.1; T835.10-15; T825.24-826.4 (Pt C Tab 91 AB-3431-3232, 3435-3436, 3438-3440, 3449). As to NOC [3(e)], this is also true in respect of exemplar category 4 (Apple Devices in combination with Apple Watch) – once "auto unlock" is enabled, unlocking an Apple Device will always cause an Apple Watch to unlock, without conditions: Benson 1 [83] (Pt C Tab 50 AB-1657); Dunstone 5, Annexure ESD-62 [integer 1.4] (Pt C Tab 49 AB-1613).
[20] Boztas at T819-33-41; T822.6-39; T823.35-42; T825.3-22; T826.6-12 (Pt C Tab 91 AB-3433, 3436-3437, 3439-3440); Benson 2 [6], [12]-[15], [22] (Pt C Tab 61 AB-1743, 1745, 1748); Dunstone at T822.47 (Pt C Tab 91 AB-3436).
[21] NOA [6(g)]; Reasons [383].

(home screen), A26 (apps) and W24 / W25 (Apple Wallet) (NOA [6(e)] and Reasons [432]). that has the consequence that (hardware and software) components that CPC has sought to exclude from the alleged TSS, but include in the alleged RSS (such as AppleSEPManager, AKS and SpringBoard/LoginWindow), are all involved in the "*provision*" or "*output*" of the AA, contrary to the Asserted Claims (see NOC [3(b)]). Finally, to the extent that CPC contends, alternatively, that the AA should somehow be **"*limited to*" steps 28, A26 and W24 / W25**, for the purpose of certain claims (NOA [6(e)]; Reasons [433]) those steps would require the AA to be output by a component (SKS) which the PJ correctly held cannot logically be excluded from the alleged RSS: Reasons [416]. Further, CPC's second and third (inconsistent) alternatives also wrongly conflate the alleged AA with the alleged "*secure access signal*" (see NOC [3(b)-(c)]).[22]

B.3 TSS / RSS (NOA 3, 6(f)-(g) & 7(a)-(b); NOC grounds 1 & 2)

14. **Construction:** The PJ correctly construed the Asserted Claims as requiring that the TSS and RSS be "*separate and distinct*" subsystems comprising "*separately identifiable*" components: Reasons [161]-[163].

15. CPC advances two, separate, contentions as to the TSS and RSS. *First*, the **Overlapping Contention**: that the TSS and RSS may include "*common or overlapping components*" and should be defined in purely "*functional terms*".[23] *Second*, the **Quintessential Components Contention**: that a TSS and RSS may be identified by the "*key or quintessential"* components responsible for achieving their functionalities (and may exclude ancillary or incidental components).[24] Both contentions should be rejected.[25]

16. As to the **Overlapping Contention**: *First,* while CPC at AS [16] correctly sets out the CGK as to what features a "subsystem" *may* have, that has no relevance to the specifically defined TSS and RSS of the Asserted Claims. (Similarly, how Apple defines its own sub-systems is irrelevant to the construction of the Patents, cf. AS [20]). *Second*, there would be no need for the Asserted Claims to identify the TSS and RSS as separate subsystems, "*if the functions of the two could be merged*": Reasons [161]. *Third*, the language of the Asserted Claims[26] requires "*a functional relationship*" between the TSS (which must transmit) and the RSS (which must receive).[27] This

[22] See: CPC's integer breakdown with cross-references to the Workings Documents (**CPC-AIB**) at [23] (Pt C Tab 75 AB-2181); cf. claims 5 and 6 of the 168 Patent and claims 1, 27, 29, 37, 39 and 41 of the 293 Patent.
[23] NOA [3(a), (c), and (d)(i) and (ii)] and AS[16]-[18].
[24] NOA [3(b) and (d)(iii)] and AS[16]-[18].
[25] As the PJ held, CPC has construed the Asserted Claims with "*an eye to infringement*": Reasons [410].
[26] Consistent with authority (*Australian Mud Co Pty Ltd v Coretell Pty Ltd* (2011) 93 IPR 188 at [77]), the PJ sought to give the terms TSS and RSS a consistent meaning throughout the Asserted Claims and Patents (whilst recognising that the specific requirements applicable to the TSS and RSS varied).
[27] The evidence of Boztas was that: "*the phrase "a transmitter subsystem comprising" refers to a subsystem within the overall system* ***which includes a transmitter***" and "*the phrase "a receiver sub-system comprising" refers to a subsystem*

would be incoherent if the subsystems could be overlapping in functionality: Reasons [157], [161]. *Fourth*, many of the Asserted Claims require "*a flow of information*" from the TSS to the RSS, which requires that the TSS and RSS be "*discernible as identifiably separate components*": Reasons [163]. The Asserted Claims consistently distinguish between the required functionality of the TSS and RSS.[28] CPC is correct at AS [17] to note that the "*ordinary meaning of 'transmitter' and 'receiver' is something that sends and something that receives, with a path between the two … and 'transmit' includes transmitting data along a cable in a PC or other logical system"*, but that is the antithesis of "*no physical separation at all"*. *Fifth*, the specifications consistently: *(i)* teach that the secure access system involves the use of two separate and distinct subsystems, the TSS (116)[29] and the RSS (117),[30] which perform **different** functions; and *(ii)* describe the TSS and RSS by reference to physically separate and distinct items of hardware (cf. AS [18]).[31] Without exception, the TSS is described as transmitting a signal over a distance (whether wirelessly or otherwise), and the RSS is described as receiving that signal and granting access to the controlled item.[32]

17. As to **AS [18(a)]**, the TSS being "*preferably*" fabricated from a single integrated circuit does not suggest that its componentry or functionality can be shared with the RSS. As to **AS[18(b)]**, CPC refers to a passage commencing "*In the event that the sub-system 116 is implemented as a remote fob…"* at 12:22. If CPC is submitting that the phrase contemplates something other than a "*remote fob*" being used, that may be accepted (i.e. 12.2-4 discloses the TSS being mounted in a protected enclosure). However, that does not suggest the TSS and RSS are not functionally, physically and logically discrete. As to **AS [18(c)]**, no reference to the specification is given. In any event, a recognition that the biometric signature database can be part of "*either*" the RSS or TSS is not a disclosure that it can be part of both at the same time. As to **AS [18(d)-(e)]**, the disclosure in Figure 10 again separates the TSS (116) and the RSS (117) - each is defined by dotted lines drawn around hardware components,[33] which communicate using "*a*

---

within the overall system which ***includes a receiver***" Boztas 1 [119], [130] (Pt C Tab 35 AB-1215, 1217). See also: Dunstone 2 [205], [208] (Pt C Tab 43 AB-1388-1390).

[28] Thus, taking the 168 Patent, the **TSS** must: *(i)* enrol biometric signatures (claims 1 & 5); *(ii)* provide or output an AA (claims 1 & 5); *(iii)* comprise a biometric sensor and means for matching a biometric signal against members of a database (claim 5); (*iv)* emit a secure access signal (claim 5); and *(v)* comprise a means for storing a biometric signal in the database (claim 6). In contrast, the **RSS** must: *(i)* provide access to the controlled item dependent upon the AA (claims 1 and 5); and *(ii)* comprise a means for receiving the transmitted secure access signal (claim 5).

[29] 168 Patent 11:4-6, 13-14; 13:2-8, 15-17; 14:1-7, 11-13; 15:8-10, 16-20; 17:9-12, 21-24; 27:2-9; 27:19-28:7 (Pt C Tab 28 AB-1015, 1017-1019, 1021, 1031-1032).

[30] 168 Patent 12:18-21; 15:21-16:17; 21:5-14; 22:1-3, 8-12, 17-25; 27:2-9 (Pt C Tab 28 AB-1016, 1019-1020, 1025-1026, 1031).

[31] Boztas conceded, when cross-examined, that there is not *any* disclosure that indicates that the TSS and RSS involve the same pieces of hardware: T459.34-T460.1 (Pt C Tab 88 AB-3073-3074). As the PJ observed, there is not a single example, anywhere in the Patents, which supports CPC's submission that the TSS and RSS may overlap: Reasons [165].

[32] 168 Patent 10:9-22; 11:4-8, 14-23; 12:3-12; 14:1-4; 15:21-16:7; 16:18-17:2; 21:5-7; 22:1-4, 17-24; 27:2-9 (Pt C Tab 28 AB-1014-1016, 1018-1021, 1025-1027).

[33] Boztas at T468.25-28; T467.19-24 (Pt C Tab 88 AB-3082, 3081).

communications network".[34] In both Figures 2 and 10, the TSS and RSS are identified as separate and distinct subsystems, comprising hardware components.[35] Thus, the specification states that software is to be "***loaded into*** *the transmitter and receiver sub-systems*", and executed using "*respective processor modules 107 and 109*", which are separate pieces of hardware.[36] The PJ correctly held that Figure 10 depicts TSS and RSS as separate and distinct: Reasons [166].

18. As to the **Quintessential Components Contention**, and contrary to AS [19]: *First*, this was not advanced until closing submissions, was not put to any expert, and did not find expression in any of CPC's written evidence: Reasons [168]. Indeed, it was contrary to the evidence of CPC's own expert.[37] *Second,* there is "*no support*", in the Asserted Claims (or Patents more generally), for such an approach.[38] As the PJ observed, "*the patentee did not choose*", when describing the embodiments in the Patents "*to separate out quintessential components*" of the TSS and RSS: Reasons [420]. *Third,* CPC's approach gives the TSS and RSS of the Asserted Claims "*an amorphous and arbitrary character*" that does not meet the requirements of the claim: Reasons [399]. *Fourth*, there is no rational basis to exclude "*components that are ancillary or incidental*" to, but still necessary for, the TSS and RSS to function. This would have the nonsensical consequence that an alleged TSS and RSS could not function. *Finally,* this contention directly contradicts the Overlapping Contention; if the TSS and RSS are defined in purely functional terms, then the TSS and RSS must, at a minimum, include **all components** necessary for them to perform their requisite functions.

19. Thus, it is apparent that the RSS and TSS must be physically separate and distinct items of hardware, with the PJ correctly rejecting the opposing contention: Reasons [388], [164]. If the PJ did not do so, he ought to have (NOC [1]; see also: Apple's submissions on validity at [21]-[22] & [43]-[46]).

20. **As to infringement**, if the PJ's construction of TSS and RSS is correct, NOA [6(g)], [7(a)-(b)] fall away and there can be no infringement. Further, and contrary to AS [29], there are myriad difficulties with CPC's identification of the alleged "*quintessential components*" constituting a TSS and RSS in the Apple Devices. *First*, the expert evidence did not support the identification of such components as quintessential; to the contrary, all components are important: Reasons

[34] 168 Patent 26:25-27:2 (Pt C Tab 28 AB-1030-1031).
[35] Boztas at T451.44-T452.5; T456.7-11; T467.19-24; T468.25-28 (Pt C Tab 88 AB-3065, 3070, 3081-3082).
[36] 168 Patent 26:9; 15-17 (Pt C Tab 28 AB-1030).
[37] In the context of infringement, Boztas consistently identified the alleged TSS and RSS by reference to **all components** involved in performing the relevant functionalities: see e.g. Boztas 1 SB-6 integer 1.3-1.5(Pt C Tab 36 AB-1224-1229); Boztas 3 at [21] (Pt C Tab 40 AB-1309); Boztas at T699.13-713.12 (Pt C Tab 90 AB-3313-3327). See also: Reasons [168].
[38] Reasons [419]-[420]. See, by contrast, the components identified as forming part of the TSS and RSS in Figures 2 and 10 of the 168 Patent (Pt C Tab 28 AB-1041, 1049).

[393]-[394].[39] Second, PJ found that CPC's alleged TSS and RSS *"is **not functional**"*, omitting components ***"significant***" and "***necessary** for the performance*" of both biometric enrolment and matching in the Apple Devices: Reasons [421]-[424].[40] Third, as the PJ held, "*no logically probative explanation has been advanced"* for the exclusion of various components from the alleged TSS and RSS, even if defined by reference to quintessential components, except that this suited CPC's case: Reasons [414]-[416], [422]-[424].

21. As to **NOC[2(a)-(b)]**, the components which CPC asserts constitute the TSS and RSS in the Apple Devices all reside on a single physical device, which grants access to itself. Those components are not physically separate and distinct, and are, even on CPC's case, involved in both transmission and reception functions.[41] There is no rational basis to label some of those components a TSS and others an RSS. As to **NOC[2(c)]**, the PJ ought also have found that the Apple Devices do not have a TSS or RSS because the hardware and software components involved in unlocking an Apple Device, accessing apps, and accessing Apple Wallet, are, in each case, different.[42] There is no subsystem in the Apple Devices responsible for "*enrolment*" and "*matching*", nor any separate and distinct subsystem responsible for "*providing access*". Rather, different hardware and software components are involved, depending on the particular item to which a user seeks access. As to **NOC[2(d)]**, if CPC still pursues any allegation in respect of the Apple Watch (it is not addressed in AS), there is no logical basis to identify an RSS as spanning hardware and software on both an Apple Device *and* a physically remote Apple Watch.

B.4 Administrator signature (NOA grounds 4 & 6(h)-(i))

22. **Construction:** The PJ correctly held that for a "*biometric signature*" (being a mathematical representation of information obtained from a biometric signal[43]) to be stored in a database as *"an administrator signature*",[44] the system "*must recognise*" it as such: Reasons [190], [192]. CPC's contention that it is sufficient for a signature to be identified with "*a person who has [the] access privileges needed to perform administrative functions*" is wrong (AS [23]). The claims expressly require the "***storing***" of a biometric signal in a database "***as an***" administrator signature (i.e. a signature with "*administrator privileges*").[45] Further, the Patents disclose that: *(i)* a "*user*"

---

[39] See also T595.46-596.36 (Pt C Tab 89 AB-3209-3210); T699-21-T704.4; T759.40-46 (Pt C Tab 90 AB-3313-3318, 3373); T773.3-44; T776.21-27; T830.37-831.9 (Pt C Tab 91 AB-3387, 3390, 3444-3445).
[40] See also: Annexure A to Apple's closing submissions on infringement.
[41] See, for example, steps 10 to 18(f) in the context of biometric enrolment (Ex 9, T6) and steps 15 to 28 in the context of access to the home screen (Ex 9, T6) (Pt C Tab 63 AB-1773).
[42] Exhibit 9, Tabs 2 (unlocking an Apple Device), Tab 3 (Apps and Protected Operations) & Tab 4 (Apple Wallet) (Pt C Tab 63 AB-1769-1771).
[43] Primer at [25] (Pt C Tab 70 AB-1982).
[44] This phrase is used in claims 3 and 6 of the 168 Patent and claim 41 of the 293 Patent.
[45] Reasons [192]. Administrator will "*have the ability to amend data stored…in the database*": 168 Patent 18.19-20 (Pt C Tab 28 AB-1022).

(or "*administrator*") is a fingerprint, not a person (the system distinguishes between biometric inputs, *not* persons); and *(ii)* a single person might, therefore, enrol multiple fingers "*as separate administrators or (ordinary) users*".[46] Thus, the experts agreed that "*administrative privileges*" must be "*attached to the biometric signature which is enrolled*", not merely "*the person*".[47]

23. The proper construction of "*administrator signature*" disposes of CPC's **infringement** allegations. *First,* iOS Apple Devices do not have different classes of users.[48] A signature cannot be stored as an administrator signature.[49] *Second*, in all Apple Devices, users can only exercise administrative privileges after entering a password, not by presenting a biometric.[50] Thus, whilst a user of a macOS Apple Device may be identified as an "*administrator*" or "*standard user*", there is still no "*administrator signature*" as the claims require: Reasons [459]-[462]

B.5 The series feature (NOA grounds 5 & 6(j)-(k))

24. **Construction:** The claims of the 293 Patent require a "*means for enrolling relevant signatures into the database*", comprising a means for: *(i)* receiving a "***series** of **entries***" of the biometric signal, with that series "***characterised***" according to at least one of the "***number** of said entries*" and a "***duration** of each said entry*"; *(ii)* **mapping** said series of entries "*into an **instruction***"; and *(iii)* **enrolling** relevant signatures into the database "***according** to the **instruction***". The PJ was correct to construe the series feature[51] as "*a mechanism for communicating to a secure access system that there is a need to enrol a signature*"; Reasons [211]. That is apparent from the structure of the claims, as well as the specification.[52]

25. CPC's contention that the series feature is "*directed to obtaining a quality biometric signature*" (AS [24]) is untenable. *First*, as the PJ observed, there is "*[n]othing in the language of the claim*" which supports this: Reasons [201]. *Second*, the claim language expressly requires that the series of entries be "*characterised*", not by the quality of the scan, but by the number or duration of entries (or both): Reasons [211]. *Third*, CPC fails to identify (and there is not) any passage in the specification which supports its construction. *Fourth*, CPC does not engage with the

---

[46] 168 Patent 19:1-6 (Pt C Tab 28 AB-1023); Boztas at T580.5-10 (Pt C Tab 89 AB-3194).
[47] Reasons [194]. Boztas and Dunstone at T580.40-T581.1 (Pt C Tab 89 AB-3194-3195). Otherwise, CPC has failed to offer any explanation of how claim 29 of the 293 Patent (which requires the database to "*comprise signatures in at least one of a system administrator class, a system user class, and a duress class*") is compatible with its construction. A signature in a "*duress class*" is not who a person who happens to be in duress, but a signal identified as falling within a duress class. See for example: 168 Patent 19.6-7; 20.23-21.4 (Pt C Tab 28 AB-1023-1025).
[48] Dunstone 5 [149(d)] (Pt C Tab 48 AB-1607).
[49] Reasons [458] & [460]; Boztas at T866.15-18 (Pt C Tab 91 AB-3480).
[50] Reasons [458]; Kostka 1 [37] (Pt C Tab 51 AB-1675); Boztas at T866.24-27 (Pt C Tab 91 AB-3480).
[51] Integers 5, 6, 7 and 8 of claim 1 of the 293 Patent (and a feature of all claims of the 293 Patent).
[52] The 293 Patent at 19.9-24 (Pt C Tab 29 AB-1074) describes how an administrator can provide control information to "*enrol an ordinary user*", which involves "*a succession of finger presses*" which is encoded by either or both *(i)* the "*number of finger presses*" and *(ii)* the "*relative duration of the finger presses*" and is checked against a "*stored set of legal control signals*" to determine whether the presses are "*control information*" or merely "*presses intended to provide access*".

requirement that the series of entries be mapped "*into an instruction*", which "*necessarily pre-exists the entry of the series*", and that relevant signatures will, only then, be enrolled "*according to the instruction*": Reasons [210]. *Finally*, there was no evidentiary support for CPC's construction - it was rejected by Dunstone[53] and evidence of Boztas was "*incoherent*" and "*difficult to understand*".[54] Contrary to AS [27], the PJ lucidly explained how, properly construed, the series feature requires the mapping of the characterised series of entries into an instruction, as well as how signatures are enrolled according to that instruction: Reasons [207]-[210].

26. **Infringement:** The PJ was correct to find that the Apple Devices do not satisfy the series feature: Reasons [453]; NOC [4(a)-(c)]. There is "*no fixed number of times or period of time*" that a user of an Apple Device is required to present a biometric in the context of enrolment and there is no means for receiving a "*series of entries*" of a biometric signal which is "***characterised***" (i.e. marked or distinguished) according to the number or duration of such entries: Reasons [450]. The only reason multiple entries may be input is to generate a template of "*sufficient quality*".[55]

27. Further, the Apple Devices do not map any characterised series of entries of a biometric signal "***into an instruction***" (i.e. "*a direction or command*").[56] There are only two ways that a user can instruct an Apple Device to enter enrolment mode, and neither involves the presentation of a biometric.[57] The images captured during enrolment on an Apple Device are not mapped into an "*instruction*" of any sort.[58] Nor is there any enrolment of relevant signatures "***according to***" such an instruction. To the extent that the Apple Devices ever receive a series of entries of a biometric signal, they do so *as part of* the enrolment process, *not* for the purpose of instructing the enrolment of relevant signatures.

C. VALIDITY

C.1 Deferred priority date (NOA ground 8; NOC ground 5)[59]

28. The PJ correctly held that the Provisional contained no real and reasonably clear disclosure of: *(i)* an AA; *(ii)* an administrator signature; or *(iii)* the series feature. That is unsurprising, as the text describing those features was only subsequently introduced. In the case of the administrator

[53] Reasons [210]-[211]; Dunstone at T601.27-38 (Pt C Tab 89 AB-3215).
[54] Boztas at T880.24-36 (Pt C Tab 91 AB-3494). Reasons [212].
[55] Reasons [453]; Touch ID: Kostka 1 [30] (Pt C Tab 51 AB-1672). Face ID: Wells [29] (Pt C Tab 53 AB-1700). NOC [4(a)].
[56] Reasons [450]; Boztas at T587.34-38 (Pt C Tab 89 AB-3201); Boztas 1 [115] (Pt C Tab 35 AB-1215); Dunstone 5 [104(i)] (Pt C Tab 48 AB-1591-1592).
[57] Boztas at T874.5-25 (Pt C Tab 91 AB-3488). A password is required for this purpose: Reasons [249]-[250]
[58] The evidence of Boztas as to what might constitute an "*instruction*" was remarkably inconsistent (Boztas 1 [125] (Pt C Tab 35 AB-1216); T589.6-29; T590.41-44; T591.9-10 (Pt C Tab 89 AB-3203-3205)) and, ultimately "*incoherent*" (T880.24-36 (Pt C Tab 91 AB-3494)).
[59] The effect of a deferred priority date is that Mathiasen becomes prior art for novelty purposes: Reasons [12(3)].

signature and series feature, AS [34] points to no disclosure in the Provisional at all. In the case of the AA, AS [33] seeks to rely on disclosure concerning "*access privileges*". However, AAs and access privileges are different concepts. Access privilege checking is a check of preconditions to access, resulting in a determination of *whether* to grant access. An AA must establish the *conditions* under which access is granted. Indeed, the Patents disclose that the *prior art* systems as described and depicted in Figure 1 involved the checking of access privileges. If that constitutes the provision of an AA, and the TSS and RSS may overlap (see: AS [15]-[18]) then, nonsensically, claim 1 of the 168 Patent would claim the prior art system of Figure 1.[60]

29. Further, the PJ should also have held that the priority date of the Patents is deferred because the disclosure of the invention of the Provisional is expressly limited to the use of a wireless pathway between the TSS and RSS, whereas the claims of the Patents are not so limited. The PJ correctly held at Reasons [502] that this meant that the path identified as 108 in Figure 2 was required to be wireless, but then took a wrong turn at Reasons [503]-[504]. That reasoning: *(i)* wrongly identifies the relevant path as "*connection 408*"; *(ii)* mischaracterises the passage referred to therein as describing a "*later embodiment*" when it is in fact summarising all embodiments; and *(iii)* fails to take account of the experts' agreement as to why, as a technical matter, the specification mandated that the pathway between the TSS and RSS be wireless.[61]

C.2 Novelty (NOA grounds 9 & 10)

30. The PJ correctly held that Wuidart disclosed an AA. Contrary to AS [35], the PJ was correct to find no difference in principle between the AAs described in the specification and the disclosure in Wuidart of a grant of access coupled with the response of adjusting vehicle conditions specific to the user seeking access: Reasons [641], [643]. Further AS [36] is wrong to state that the relevant signal is "*a purely binary lock/unlock signal*": it also includes the "*impersonal code*" providing additional commands to which the receiver responds: Reasons [630], [641].

31. The PJ was correct to conclude that, on CPC's construction, each of Scott, Hamid and Mathiassen disclosed an AA. The distinction which AS [38] seeks to draw is that "*determination*" of access in the TSS, rather than the RSS, is not disclosed in that prior art, but Reasons [139]-[144]; [554]; [580]-[582]; [619] correctly addressed this, and no error has been identified. (Notably, CPC's argument is inconsistent with the proposition it advances on infringement that the TSS and RSS may be an overlapping set of components which achieve the functionalities required by the claims). Additionally, the suggestion that Mathiassen discloses "*multiple signals being broadcast to separate receivers*" is wrong: Reasons [611].

[60] Boztas at T656.6-662.26 (Pt C Tab 90 AB-3270-3276).
[61] Dunstone T630.24-632.11 (Pt C Tab 89 AB-3244-3246); Boztas T656.6-660.46 (Pt C Tab 90 AB-3270-3274).

32. The PJ also rightly found that each of Scott, Hamid and Mathiassen disclosed an administrator signature on CPC's construction. On CPC's approach (which pays little heed to the claim language or the specification), there will be an administrator signature if a first user of a system is permitted to enrol their own biometric signature (say a fingerprint), and then enrol somebody else's. That is true of Scott, Hamid and Mathiassen: Reasons [557], [558], [587], [615]. CPC, in AS [39], ignores this.

9 February 2026

Tom Cordiner, Angus Lang, Peter Creighton-Selvay