

**UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE PATENT TRIAL AND APPEAL BOARD**

---

TOYOTA MOTOR CORP.

and

KIA CORPORATION,  
Petitioners,

v.

EMERGING AUTOMOTIVE LLC,  
Patent Owner.

---

Case IPR2026-00059  
U.S. Patent 11,104,245

---

**EMERGING AUTOMOTIVE LLC'S  
PATENT OWNER PRELIMINARY RESPONSE**

**TABLE OF CONTENTS**

I.	Introduction.....	1
II.	Background.....	4
	A. Innovations of U.S. Patent 11,104,245 .....	4
	B. Related and Parallel Litigation Proceedings .....	5
	C. Person of ordinary skill in the art.....	8
III.	Petitioners’ unexplained, inconsistent claim construction positions—Involving Alleged Disclaimer of the Petition’s Primary Reference, Zaid—warrant denial of institution. ....	8
IV.	All Grounds fail because Petitioners have failed to show that it is more likely than not that any reference, alone or in combination, teaches or suggests multiple limitations of independent claim 1.....	14
	A. Grounds 1 and 2 fail because neither Kleve nor Kleve in combination is shown to disclose independent claim limitations 1[f], 1[g], 1[h] and 1[i].....	16
	1. Petitioners have failed to show that any reference, alone or in combination, teaches or suggests the “the coded data from the mobile device including a unique access code received by the mobile device from the server,” as recited by independent claim 1[f].....	16
	2. Petitioners’ failure to show any reference, alone or in combination, that teaches or suggests “the unique access code functioning for the e-key,” as recited by independent claim 1[i], further highlights the Petition’s failure as to claim 1[f]. ....	23
	3. Petitioners have failed to show that any reference, alone or in combination, teaches or suggests the “privileges for the unique access code” or “the unique access code is associated with privileges set via the server,” as recited by independent claim	

1[g].	24
4. Petitioners have failed to show that any reference, alone or in combination, teaches or suggests “the privileges are set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle ... privileges are for the unique access code” as recited by independent claim 1[g].	25
5. The Petition fails to demonstrate why a POSITA would have been motivated to modify or combine Kleve in view of Mottla.	31
6. Petitioners have failed to show any reference, alone or in combination, teaches or suggests a “camera capturing video ... during a period of time in which the unique access code is to be active,” as recited by independent claim 1[h].	43
B. Petitioners’ Zaid-based Grounds 3 and 4 fail for at least the same failures of proof identified by the Board in IPR2024-00981.	44
1. The Zaid Reference (EX1008).	45
2. The Board already determined that the alleged “time period” of Zaid’s reservation is not set by the owner as the Petition contends, therefore Petitioners’ Zaid-based Grounds 3 and 4 both fail.	47
C. For Grounds 3 and 4, Petitioners’ reliance on the Examiner’s findings is of no avail, as the Examiner agreed Zaid does not teach or suggest the limitations of claim 1.	51
1. The Petition fails to identify any disclosure to satisfy claim 1[i]’s recited “the unique access code functioning for the e-key.”	51
2. The Petition fails to demonstrate why a POSITA would have been motivated to modify Zaid in view	

Mottla.....53

3. The Petition fails to show that Zaid, or Zaid in combination with Kleve, teaches or suggests the recited elements of claim 1[h].....55

V. Conclusion .....56

**TABLE OF AUTHORITIES**

**Cases**

*In re Kahn*,  
441 F.3d 977 (Fed. Cir. 2006) .....42

*Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*,  
821 F.3d 1359 (Fed. Cir. 2016) ..... 42, 55

*Kia Corp. and Toyota Motor Corp. v. Emerging Automotive LLC*,  
IPR2024-00785, Paper 16 (PTAB May, 27, 2025) .....7

*Kia Corp. and Toyota Motor Corp. v. Emerging Automotive LLC*,  
IPR2024-00981, Paper 37 (PTAB Jan. 8, 2026) .....8

*Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*,  
688 F.3d 1342 (Fed. Cir. 2012) ..... 42, 55

*KSR Int’l Co. v. Teleflex Inc.*,  
550 U.S. 398 (2007).....42

*Revvo Technologies, Inc. v. Cerebrum Sensor Technologies, Inc.*,  
IPR2025-00632, Paper 20 (Director Nov. 3, 2025).....9

*Tesla, Inc. v. Intellectual Ventures II LLC*,  
IPR2025-00340, Paper 18 (Director Nov. 5, 2025).....1, 9

*TikTok, Inc. v. ShopSee, Inc.*,  
IPR2025-01485, Paper 13 (Director, Jan. 16, 2026) .....9

**Regulations**

37 C.F.R. § 42.104(b) .....9, 14

**PATENT OWNER'S UPDATED EXHIBIT LIST**

Exhibit No.	Description
2001	Declaration of Sam Malek, Ph.D.
2002	Civil Docket Report for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:23-cv-0437-JRG (lead case)
2003	Google Patents search, U.S. Patent No. 11,104,245, available at <a href="https://patents.google.com/patent/US11104245B2/en?q=11%2c104245#citedBy">https://patents.google.com/patent/US11104245B2/en?q=11%2c104245#citedBy</a> (identifying assignees of patents and patent applications which cited to U.S. Patent No. 11,104,245)
2004	Final Written Decision, IPR2024-00981
2005	Discovery Order for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:25-cv-00782-JRG (lead case)
2006	Defendant's Claim Construction Brief, <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:23-cv-0437-JRG
2007	Civil Docket Report for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:23-cv-0434-JRG (member case)
2008	Civil Docket Report for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:25-cv-0782-JRG (lead case)
2009	Civil Docket Report for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:25-cv-0799-JRG (lead case)
2010	Order Denying Motion to Stay, <i>Digital Doors, Inc. v. Int'l Bus. Machines Corp.</i> , No. 2:22-cv-00457-JRG-RSP (E.D. Tex. July 24, 2023)
2011	<i>Curriculum Vitae</i> of Dr. Sam Malek
2012	"How are QR codes generated?", QRcodeKit, available at <a href="https://qrcodekit.com/guides/how-are-qr-codes-generated/">https://qrcodekit.com/guides/how-are-qr-codes-generated/</a>

## **I. Introduction**

Patent Owner Emerging Automotive LLC (“Patent Owner”) submits its Preliminary Response to the Petition for *Inter Partes* Review No. IPR2026-00059 (“Petition” or “Pet.”) filed on October 21, 2025, by Kia Corp. and Toyota Motor Corp. (collectively, “Petitioners”) challenging claims 1-18 of U.S. Patent 11,104,245 (“the ’245 Patent”). EX1001.

As detailed in its separately-filed Request for Discretionary Denial, Patent Owner respectfully submits that the Director should exercise discretion and deny institution under 35 U.S.C. § 314 for each of the reasons set forth in the Request for Discretionary Denial. To the extent the Petition is referred to reach the merits of Petitioners’ asserted Grounds, the Petition should be denied institution because:

(1) Petitioners’ inconsistent claim construction positions—particularly the broad construction presented in this forum contrasted against the narrow construction advanced in district court based on Patent Owner’s comments concerning the very same reference relied upon in this Petition—compromises the Board’s ability to assess the Petition’s merits and directly undermines Petitioners’ argument that either primary reference, Kleve or Zaid, actually discloses the “privileges” limitations of independent claim 1[g]. “[P]etitioner [wa]s required to explain why those different positions are warranted,” *Tesla, Inc. v. Intellectual Ventures II LLC*, IPR2025-00340, Paper 18, at 3 (Director Nov. 5, 2025)

(informative), but failed to even acknowledge, let alone justify the alternative positions presented in the Petition.

(2) Petitioners concede that for the Kleve-based Grounds, 1 and 2, there is no reference, alone or in combination, that discloses a “unique access code”—an element which is recited by no fewer than five different limitations in independent claim 1 (and by dependency, all challenged claims). Petitioners instead rely on expert testimony to contend that Kleve’s “matrix barcode,” like “QR codes,” by their very nature, “encode a unique access code” or “encode a unique value”—but this is flatly wrong. “A QR (Quick Response) code, also referred to as a matrix barcode, is not inherently unique; rather ‘[a] QR code becomes unique only when the data encoded within it is unique.’” EX2001, quoting EX2012. As anyone who has scanned a QR code for a restaurant menu can affirm, the QR codes at each table of a restaurant will reveal the same menu for each table, and therefore QR codes, like Kleve’s matrix barcode, do not inherently encode a “unique” value. As detailed further below, the Petition’s failure on this point alone is fatal to both Kleve-based Grounds.

(3) For Grounds 1 and 2, the Petition’s failure to demonstrate any reference that teaches or suggests a “unique access code” means that the Petition also cannot sustain its burden as to independent claim elements 1[g], 1[h], or 1[i]—each of which recite features or functions of the “unique access code.” And Grounds 1 and 2 fail

regardless, as the Petition suffers from additional failures of proof as to independent claims 1[g], 1[h] and 1[i].

(5) Grounds 1 and 2 also fail because the Petition fails to show that Kleve and Mottla are properly combined, and even if they were, the combination still fails to satisfy the limitations of claim 1[i].

(6) Similarly deficient are the Petition's Zaid-based challenges, Grounds 3 and 4, because the Board's decision in IPR2024-00981 already rejected Petitioners' allegation that Zaid's owner announcing or advertising "vehicle availability and vehicle location" is a "rental period restriction" for Zaid's vehicle reservation. The Board determined that for Zaid's vehicle reservation, the "vehicle renter uses his or her own account to make a reservation and to send a request that generates an electronic key," and Zaid offered neither "teaching or suggestion that such a user account would encompass the vehicle owner." The Petition's renewed reliance on Zaid is equally misplaced, as it is the vehicle *renter* that makes the vehicle reservation and its time period—*not the vehicle owner*, as Petitioners contend.

(7) For Grounds 3 and 4, the Petition suffers from additional failures of proof as to independent claims 1[g], 1[h] and 1[i].

(8) Finally, the Petition fails to demonstrate why a POSITA would have been motivated to modify Zaid in view of Mottla for alleged disclosure of independent claim 1[i]. This failure is fatal to both Grounds 3 and 4 of the Petition.

## II. Background

### A. Innovations of U.S. Patent 11,104,245

U.S. Patent 11,104,245 (“the ’245 Patent”) issued on August 31, 2021. EX1001, Face Page. The ’245 patent is titled “Vehicles and Cloud Systems for Sharing E-Keys to Access and Use Vehicles” and “relates to systems and methods for generating and sharing electronic keys (e-Keys) with users and cloud-based processing systems[.]” *Id.* at 1:1-3, 1:59-62. Companies like Apple, Ford, Samsung, Audi, General Motors, Volkswagen, and even Petitioner Toyota and Petitioner Kia’s parent, Hyundai, have all cited to the ’245 Patent in their own patent applications. EX2003, (identifying assignees of patents and patent application publications which cited to the ’245 Patent).

The ’245 Patent describes innovations that allow a vehicle owner to assign, refine, and control the generation of any number of e-keys to any number of users for a vehicle—each unique e-key having its own privileges. EX1001, 43:26-40. For example, the owner can set a restriction associated with a mode of allowed use of the vehicle, such as “valet mode,” in which “the vehicle will have restricted use parameters, and will also provide for reporting back to the user in case violations occur in accordance with the predefined privileges assigned to a valet.” *Id.*, 38:21-30.

The claims recite that the vehicle receives coded data from the mobile device

for unlocking and use of the vehicle, that the coded data includes a unique access code including a unique access code received from the server. EX1001, (independent claim 1). “The unique generation of access codes enables each electronic key[] to be different for each user and each e-key can be canceled at any time from a device having access to the Internet.” EX1001, 43:49-53. Accordingly, each e-key is unique, and “being unique, can be cancelled and eliminated without affecting other issued e-keys.” *Id.*, 48:53-59, 47:57-61. Additionally, the claims recite that “privileges are set via the server,” the “privileges are for the unique access code,” and the privileges are “responsive to a restriction set by an administrator of the vehicle” and that “the restriction is associated with a mode of allowed use of the vehicle.” *Id.*, claim 1.

### **B. Related and Parallel Litigation Proceedings**

In July 2025, Patent Owner asserted infringement of the '715 Patent against Petitioners in the Eastern District of Texas (“*Emerging Automotive v. Toyota/Kia, II*”). EX2008; EX2009. Patent Owner also asserted two other Emerging Automotive patents, U.S. Patents 12,337,715 and 12,337,716, against Petitioner Toyota, and asserted the 12,337,715 Patent against Petitioner Kia. *Id.*

Previously, in September 2023, Patent Owner filed two patent infringement lawsuits against Petitioner Toyota and Petitioner Kia, asserting infringement of U.S. Patent 10,407,026 (“the '026 Patent”), U.S. Patent 11,738,659 (“the '659 Patent”),

U.S. Patent 9,365,188 (“the ’188 Patent”) (collectively “related e-key patents”) and U.S. Patent 9,171,268 (against Petitioner Toyota only)<sup>1</sup>. EX2002; EX2007. These 2023 proceedings were consolidated (“*Emerging Automotive v. Toyota/Kia, I*”) and, on the eve of trial, *Emerging Automotive v. Toyota/Kia, I* was stayed, following the district court’s summary judgment order on a non-instituted asserted patent. EX2002. In *Emerging Automotive v. Toyota/Kia, I*, fact discovery, expert discovery, claim construction proceedings and the submission of a pretrial order had been completed and the parties participated in a Pretrial Conference.<sup>2</sup> *Id.*

The district court issued a Markman Order on May 14, 2025 for each of the ’026 Patent, the ’659 Patent, and the ’188 Patent—the related e-key patents. EX1015. Specifically, the district court construed the “electronic key” / “eKey” / “e-key” terms of those related e-key patents as “electronic data that enables one or more

---

<sup>1</sup> Emerging Automotive had originally asserted U.S. Patent 11,296,244 (“the ’244 Patent”) in its 2023 patent infringement action against Toyota, but subsequently amended the complaint to withdraw the ’244 Patent from the lawsuit. EX2002.

<sup>2</sup> For the *Emerging Automotive v. Toyota/Kia, II* district court proceedings, the parties have agreed to utilize the discovery completed in *Emerging Automotive v. Toyota/Kia, I*. EX2005, at ¶¶ 5, 12(g)-(h).

functions of the vehicle”:

Term	Disputed Term	The Court’s Construction
1	“electronic key”/ “eKey”/ “e-key” (’026 patent, Claims 1, 2, 6, 13, 15; ’659 Patent, Claims 1, 3, 4, 12, 13, 20; ’188 Patent, Claims 1, 11, 16, 17; ’268 Patent, Claims 10, 18)	“electronic data that enables one or more functions of the vehicle”

EX1015, at 32. Additionally, the district court ordered that the plain and ordinary meaning of “privileges,” as recited in the related e-key patents (*id.*, at 12-13), specifically excludes “unfettered access”:

*Id.* (internal citations omitted). Plaintiff then emphasized its prosecution remarks that Zaid did not disclose “a unique access code that includes privilege settings set for additionally limiting types of use of the vehicle.” *Id.* at 17. In other words, Plaintiff equated “unfettered access” with the absence, not presence, of “privileges.” Given that, the Court agrees with Defendants that “privileges for use of the vehicle” cannot simply be “unfettered access” to the vehicle, which is the “plain and ordinary meaning” of these phrases on this record.

*Id.*, at 13.

Regarding the IPR/EPR proceedings on related e-keys patents, the Board did not institute IPR2024-00785, which challenged claims of the ’026 Patent. *See Kia Corp. and Toyota Motor Corp. v. Emerging Automotive LLC*, IPR2024-00785, Paper 16 (PTAB May, 27, 2025). The Board instituted proceedings in IPR2024-00981 and issued a Final Written Decision finding that all challenged claims of the ’188 Patent were shown to be unpatentable. EX2004. A Request for Director Review of that Final Written Decision is currently pending. *See Kia Corp. and Toyota Motor Corp.*

*v. Emerging Automotive LLC*, IPR2024-00981, Paper 37 (PTAB Jan. 8, 2026). Regarding the '659 Patent, the Board instituted proceedings in IPR2024-01167, and that matter is pending (*Kia Corp. and Toyota Motor Corp. v. Emerging Automotive LLC*, IPR2024-01167, Paper 14 (PTAB Jan. 27, 2025)); additionally, the Office issued a final rejection in Reexamination 90/019,456, for which an appeal is pending. Pet. 1, 9.

**C. Person of ordinary skill in the art**

Petitioners' expert opines that "a person of ordinary skill in the art pertinent to the '245 patent would have had a four-year undergraduate degree in electrical engineering, automotive engineering, or a closely related field and at least two years of experience in the fields of access control systems, vehicle electronics, and/or cryptography. More education can supplement practical experience and vice versa." EX1004, ¶ 84.

For purposes of this Preliminary Response, Patent Owner and its expert apply this definition. *See* EX2001.

**III. Petitioners' unexplained, inconsistent claim construction positions— involving alleged disclaimer of the Petition's primary reference, Zaid— warrant denial of institution.**

Petitioners have taken inconsistent positions in district court and in the IPR Petition regarding the "privileges" terms recited in each of the challenged claims of the '245 Patent, which directly undermines the Petition's argument that Kleve, the

primary reference for Grounds 1 and 2, teaches or suggests said “privileges” and also directly undermines the Petition’s primary reference, Zaid, for Grounds 3 and 4.

The Petition should be denied because of Petitioners’ (1) failure to construe the “privileges” terms of the claims, in light of the district court order, as required by 37 C.F.R. § 42.104(b)(3) and (2) failure to explain Petitioners’ inconsistencies in the two forums, as required by *Revvo Technologies, Inc. v. Cerebrum Sensor Technologies, Inc.*, IPR2025-00632, Paper 20 (Director Nov. 3, 2025) (precedential (“*Revvo*”)), *Tesla*, Paper 18 at 3-4, and the Director’s recent decision set forth in *TikTok, Inc. v. ShopSee, Inc.*, IPR2025-01485, Paper 13 (Director, Jan. 16, 2026) (denying institution where petitioner failed to explain inconsistent claim construction positions).

As excerpted below, Petitioners advised the Board that apart from “e-key,” “no other terms need construction here.” Pet. 14:

**VI. Claim Construction**  
The District Court construed “electronic key”/“eKey”/“e-key” as “electronic data that enables one or more functions of the vehicle.” Ex. 1015. Claims only need to be construed to the extent necessary, and no other terms need construction here.

However, Petitioners’ position in this IPR proceeding is inconsistent and irreconcilable with their proposed construction of the “privileges” terms in district

court, terms which are found in each of the challenged claims of the '245 Patent— i.e., “privileges set by the server responsive to a restriction, the restriction is associated with a mode of allowed use of the vehicle” and “privileges are for the unique access code” (independent claim 1) and “privileges are defined for each sharing session of the vehicle” (dependent claim 8). EX1001, claims 1, 8.

In district court Petitioners advanced a narrower construction of “privileges” to specifically exclude “unfettered access”—and Petitioners’ narrower construction was in fact adopted by the district court. EX1015, at 12-13. Specifically, Petitioners’ proposed construction in district court was based on Patent Owner’s comments during prosecution when distinguishing Zaid—e.g., that Zaid could not disclose the recited privileges limitations in light of Zaid’s “unfettered access” to the vehicle, and Zaid did not disclose “a unique access code that includes privilege settings.” *Id.*

In Zaid, a user reserves a vehicle using a server. “[T]he vehicle reservation is communicated to a wireless communication device of the user, “and the wireless communication device receives and caches the reservation.”

After decrypting the reservation, the wireless communication device forwards the decrypted reservation to a “vehicle access kit” of the vehicle. Then, unfettered “vehicle access is provided based on the received reservation.”

*Id.* (internal citations omitted). Plaintiff then emphasized its prosecution remarks that Zaid did not disclose “a unique access code that includes privilege settings set for additionally limiting types of use of the vehicle.” *Id.* at 17. In other words, Plaintiff equated “unfettered access” with the absence, not presence, of “privileges.” Given that, the Court agrees with Defendants that “privileges for use of the vehicle” cannot simply be “unfettered access” to the vehicle, which is the “plain and ordinary meaning” of these phrases on this record.

EX1015, at 12-13; Defendants’ Claim Construction Brief, EX2006, at 6:

limits, geographic restrictions, amount of time, etc.” Ex. G (“’026 POPR”), 3–4. EA argued that cited prior art did not disclose the claimed “privileges” because it provided “unfettered” vehicle access. *Id.*, 10. Therefore, the claimed “privileges for use” and “conditions of use” do not define whether “unfettered” access to the vehicle is permitted. Instead, they define permitted uses that restrict *how* the vehicle can be used with the e-key, such as speed restrictions, geographic limits, or the like, and not merely *whether* the vehicle can be accessed.

Petitioners failed to disclose to the Board that the district court had construed the “privileges” terms to specifically exclude “unfettered access,” based on comments concerning Zaid, despite the Petition’s substantial reliance on Zaid to challenge each of the claims of the ’245 Patent, and the fact that each of the challenged claims requires both that “the unique access code is associated *with privileges* set by the server,” that those “*privileges* are for the unique access code,” and that those “privileges set by the server” are “*responsive to* a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle[.]” Pet. 14; EX1001, claim 1. And here Zaid is not merely the Petition’s primary reference for Grounds 3 and 4. As detailed below, the Petition purports to adopt many of the Examiner’s Zaid-based rejections in an attempt to fill in the Petition’s evidentiary gaps—a strategy which, in fact, dooms the Petition’s showing that any reference teaches or suggests claim 1[i]. *See* Section IV.C.1, *infra*.

Accordingly, this is not only a case in which Petitioners made inconsistent claim construction arguments in two different proceedings, but also one in which the

Board's ability to assess the Petition's merits is compromised by the Petition's lack of disclosure.

Because each of the challenged claims of the '245 Patent recites the "privileges" term, Petitioners should have advised the Board that this term had already been construed. EX1001, claim 1. They did not. Also, to allow the Board to properly review the merits of the Petition's challenge, the Petition should have provided a justification for the inconsistent positions and proposed invalidity arguments premised on the "privileges" construction. Petitioners did neither.

The Board's ability to assess the Petition's merits is compromised by the Petition's lack of disclosure. Here, the Petition has failed to inform the Board of the narrowed district court construction—a construction Petitioners sought—which not only has direct relevance to the "privileges" limitations at issue in each of the challenged claims of the Petition, but also relevance as to whether the Petition's primary references, Kleve (Grounds 1 and 2) and Zaid (Grounds 3 and 4), actually disclose those very "privileges" limitations.

Each of the Petition's Grounds fail, for multiple independent reasons, as detailed further below. For example, for claim 1[g]'s limitation reciting "privileges set via the server responsive to a restriction set by an administrator of the vehicle," the Petition argues that Zaid's owner's ability to "advertise or announce when the vehicle will be available for sharing" is the alleged "restriction" for which

“privileges set via the server” are “responsive.”

Of course, as Zaid explains, the owner advertising or announcing when the vehicle is available for sharing is just what Zaid says it is, an advertisement or announcement. And of course, that vehicle availability can a year (or more), or months within a year, or weeks within a month, or days within a week, etc. *Id.* As detailed further below, the Petition fails to show any “privileges set via the server responsive to” this announcement of “availability.”

However, had the Petition actually informed the Board of, and applied, the district court’s construction of “privileges,” this deficiency would be even more glaring. As is clearer with the proper construction, there can be no showing of privileges responsive to this announcement of vehicle availability, where “privileges” expressly excludes “unfettered access.” EX1015, at 12-13.

Accordingly, to weigh the merits of the Petition, the Board should have been informed of the district court’s construction of the “privileges” term, as well as why Petitioners advanced that construction—the comments based on Zaid during prosecution—and Petitioners should have explained the reason for their inconsistent positions across the two proceedings. Petitioners did neither.

The Petition provided no reason for advancing a different claim construction before the district court, and these unexplained inconsistent claim construction positions alone warrant denial of institution. But here Petitioners took this error

further, failing to inform the Board of their own narrowed district court construction of “privileges,” their reliance on the prosecution comments concerning Zaid, and then failing to apply the narrowed construction in their challenges. The Petition’s failure to comply with 37 C.F.R. § 42.104(b)(3), and failure to heed the Director’s express requirements set forth in *Revvo*, Paper 20, *Tesla*, Paper 18, and *TikTok*, Paper 13, not only increases the risk of inconsistent decisions across the two forums, but also renders the Board’s decision on the Petition’s challenges as merely advisory.

For these reasons alone, Institution should be denied.

**IV. All Grounds fail because Petitioners have failed to show that it is more likely than not that any reference, alone or in combination, teaches or suggests multiple limitations of independent claim 1.**

The Petition fails to meet the required threshold for any claim, as the Petition relies on conclusory expert opinions to try to fill the glaring evidentiary gaps for multiple limitations required of independent claim 1 (and therefore required by dependency for all challenged claims 1-18).

Independent claim 1 recites no fewer than four different limitations to specify the “unique access code”:

(1) how the vehicle receives the unique access code and where it comes from, e.g., “the coded data from the mobile device including a unique access code received by the mobile device from the server” (EX1001, claim 1[f]);

(2) what the unique access code does and how it is managed, e.g., “the unique

access code functioning for the e-key that is managed via one or more graphical user interface inputs rendered on a screen of the mobile device” (*id.*, claim 1[i]);

(3) specific features of the unique access code, e.g.:

(a) “privileges are for the unique access code” (*id.*, claim 1[g]);

(b) “the unique access code is associated with privileges set via the server responsive to a restriction set by an administrator of a vehicle, the restriction is associated with a mode of allowed use of the vehicle” (*id.*, claim 1[g]); and

(4) components and operations when “the unique access code is to be active,” e.g., “a camera of the vehicle is used for capturing video of an area that includes the vehicle during a period of time in which the unique access code is to be active, such that actions taken by a user using an electronic key (e-key) is recorded” (*id.*, claim 1[h]).

Notwithstanding its integral role in the challenged claims, the Petition’s primary reference for Grounds 1 and 2—Kleve—fails to teach or suggest any “unique access code.” The Petition would have the Board institute regardless, accepting Petitioners’ say-so that this claim term is meaningless and can be readily discarded, despite the multiple claim limitations specifying the features and the functionality of the unique access code.

While Petitioners point to Kleve’s matrix barcode as allegedly satisfying both the claims’ “coded data” and the “unique access code,” it does not. The facts, and

Kleve itself, show otherwise. And it is by this sleight of hand that the Petition seeks to evade its burden of proof as to *all the other independent claim limitations* which specify this “unique access code.” This sophistry cannot sustain Petitioners’ burden, and Petitioners’ mere assertion is insufficient to render superfluous the claims’ requirements of the “unique access code.” Grounds 1 and 2 both fail.

**A. Grounds 1 and 2 fail because neither Kleve nor Kleve in combination is shown to disclose independent claim limitations 1[f], 1[g], 1[h] and 1[i].**

- 1. Petitioners have failed to show that any reference, alone or in combination, teaches or suggests the “the coded data from the mobile device including a unique access code received by the mobile device from the server,” as recited by independent claim 1[f].**

For Grounds 1-2, the Petition points to Kleve’s “matrix barcode” as the independent claim’s recited “coded data ... for unlocking and use of the vehicle.” Pet. 19. But even if Kleve’s matrix barcode were to meet each of the required features of the claims’ recited “coded data,” neither Kleve nor any other reference discloses or teaches “**the coded data ... including a unique access code**”—let alone “the coded data from the mobile device including *a unique access code received by the mobile device from the server,*” as independent claim 1[f] requires. EX1001, claim 1[f] (emphases added).<sup>3</sup>

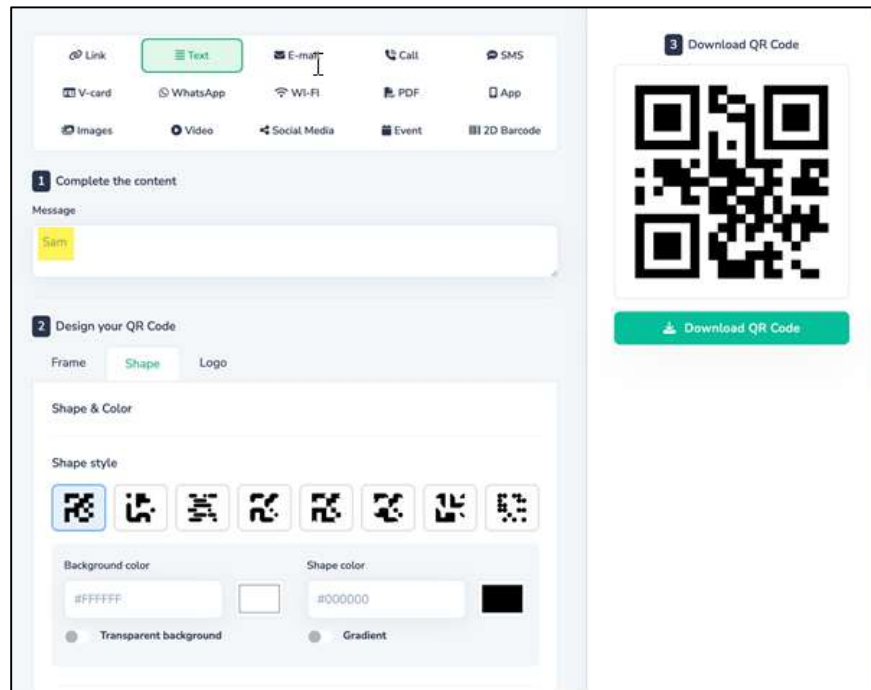
The Petition attempts to fill Kleve’s gaps with expert testimony, but the

---

<sup>3</sup> Emphasis herein added unless otherwise noted.

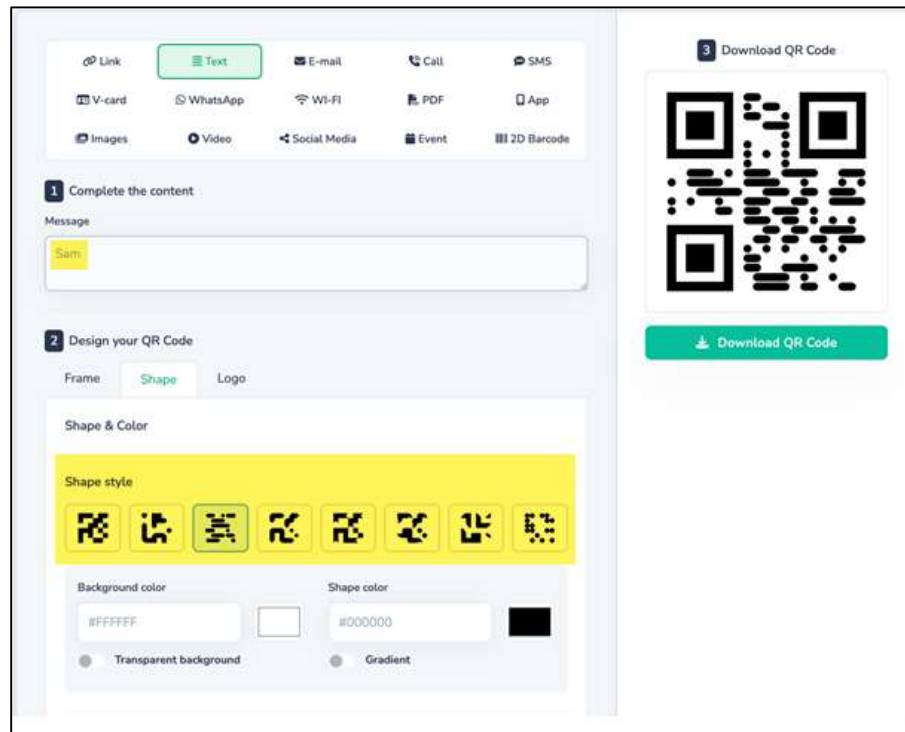
Petition's Grounds crumble after one look at that testimony. Pet. 19-20, citing EX1004, ¶¶ 121-22. For example, rather than point to any actual disclosure in Kleve, Petitioners' expert provides the conclusory opinion that Kleve's "matrix barcode," like "QR codes," by their very nature, "encode a unique access code" or "encode a unique value[.]" EX1004, ¶ 122 (citing EX1005, ¶¶ 44, 69). This is simply wrong.

A QR code, or Quick Response code, also referred to as a matrix barcode, is a two-dimensional barcode that stores information in a grid of typically black and white squares that can be read by imaging devices, such as smartphone cameras. EX2001, ¶ 44, citing EX2012. As Dr. Malek explains, "a QR code is not inherently unique; rather 'a QR code becomes unique only when the data encoded within it is unique.'" *Id.*, quoting EX2012. A QR code may be generated for arbitrary data, regardless of whether that data is unique. EX2001, ¶¶ 44-45. Indeed, publicly available online services, such as qr.io, allow users to generate QR codes for arbitrary input, without any requirement of uniqueness. *Id.* Dr. Malek demonstrates this point using the qr.io website to generate a QR code encoding his first name, "Sam," which is not a unique name. *Id.*



*Id.* A QR code is not even a unique representation of a given piece of information.

*Id.*, ¶ 46. To illustrate this, Dr. Malek again used the qr.io service, this time altering the visual styling parameters of the QR code (e.g., shape style) and generated a different QR code that still encodes the same underlying data—his first name, “Sam.” *Id.*



*Id.*

By this illustration, Dr. Malek shows that “multiple distinct QR code symbols can encode identical information, further demonstrating that a QR code itself is not inherently unique, even with respect to a specific data value.” *Id.*

Accordingly, QR codes, like Kleve’s matrix barcode, do not inherently encode a “unique” value as Petitioners’ expert submits. *Id.*, ¶¶ 43-46; *see also* EX2012. As demonstrated above, a matrix barcode, or QR code, is a way of encoding some information, but there is nothing inherently unique in that representation of data. *Id.*, ¶¶ 43-46; *see also* EX2012. Petitioners’ reliance on expert testimony fails to fill the evidentiary gaps of the reference. A matrix barcode, like Kleve’s matrix barcode is not “well known [] to encode a unique value,” as Petitioners’ expert misstates, and

therefore Kleve's matrix barcode does not teach or suggest claim 1[f]'s recited "coded data from the mobile device including a unique access code received by the mobile device..." EX1001, claim 1[f]; EX2001, ¶¶ 43-46; *see also* EX2012.

Moreover, Kleve itself affirms this *lack of* "unique-ness," likening its "matrix barcode" to a "code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term." EX1005, ¶ 69. In fact, Petitioners and Dr. Almeroth cite to paragraph 69 of Kleve, misstating that

Kleve describes the matrix barcode as a type of "unique Temporary User identification" because, like a fingerprint or photo ID, the matrix barcode contains or encodes unique information (i.e., a unique access code) ...

Pet. 20, citing EX1004, ¶122 (verbatim). This is wrong. One look at Kleve paragraph 69 shows the opposite.

In a first embodiment, where the vehicle owner generates a virtual key, Kleve states: "[a]t step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term." EX1005, ¶ 69. In another "embodiment of generating a virtual key," the reference discloses: "[a]nother exemplary embodiment of generating a virtual key may be done by using Temporary User's credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice

print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614.”

*Id.*, ¶ 69:

[0069] FIG. 6 is an exemplary embodiment of the vehicle rental micro-business distributing and controlling virtual keys using a nomadic device with a vehicle. The vehicle rental micro-business administrative system may consist of a computer system configured to host one or more websites for interaction with a vehicle Owner and Temporary User. In the illustration 600, a server 634 is used to communicate between a vehicle Owner nomadic device 601, a Temporary User nomadic device 611, and a vehicle computing system 621. Using a nomadic device, for example a smart phone, a Temporary User and vehicle Owner may set up user profiles, enter into an agreement and make a payment to initiate the vehicle rental process between the two parties at step 602 and 612. At step 604, the vehicle Owner may then generate a virtual key based on a password generated by the vehicle Owner that may include a matrix barcode or a code word that the Temporary User may enter/send to the vehicle when ready to begin the rental term. Another exemplary embodiment of generating a virtual key may be done by using Temporary User’s credentials including fingerprint recognition, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, phrase for speech recognition, temporary mobile web login IDs and password, or other type of unique Temporary User identification at step 614. At step 616, the virtual key is generated and sent to the Temporary User. The Owner may deliver a virtual key to the vehicle for recognizing the Temporary User having authorization to enable a keyless drive-away at step 606.

Accordingly, Petitioners and their expert misstate Kleve’s description here, and in fact, Kleve excludes any mention of its “matrix barcode” when, in the second “embodiment of generating a virtual key,” Kleve describes multiple examples of “other type of unique Temporary User identification[.]” *Id.*; EX2001, ¶¶ 47-50.

Kleve simply does not teach or suggest any “coded data ... *including a unique access code*,” or any “unique access code” at all, and Dr. Almeroth’s incorrect testimony about QR codes cannot cure the reference’s deficiency here. EX2001, ¶¶ 43, 51.

Because the Petition fails to identify any reference that teaches or suggests the independent claims’ required “unique access code,” the Petition likewise cannot show the remaining independent claim limitations requiring specific features and functionality of that recited “unique access code,” e.g.: (1) the “unique access code functioning for the e-key” (claim 1[i]); (2) “the unique access code is associated with privileges set via the server” (claim 1[g]); (3) the “privileges are for the unique access code” (claim 1[g]); or (4) the recited privileges set by the server being “responsive to a restriction set by an administrator of the vehicle” (claim 1[g]). EX1001; EX2001, ¶¶ 43-51.

The Petition’s failures as to claim 1[f] are, alone, fatal to Grounds 1 and 2. Additionally, because of this lack of the recited “unique access code,” the Petition cannot sustain its burden as to claim elements 1[g], 1[h], or 1[i].

Accordingly, Petitioners have failed to show there is a reasonable likelihood of prevailing as to any claim challenged in Grounds 1 or 2.

**2. Petitioners’ failure to show any reference, alone or in combination, that teaches or suggests “the unique access code functioning for the e-key,” as recited by independent claim 1[i], further highlights the Petition’s failure as to claim 1[f].**

Petitioners cannot meet their burden for claim limitation 1[i], at least because claim 1[i] requires “the unique access code functioning for the e-key,” but the relied upon “matrix barcode” does not teach or disclose this limitation. As shown in Section IV.A.1., for Grounds 1 and 2, the Petition failed to show any teaching or suggestion of the “unique access code” recited by independent claim 1 (and by dependency, all challenged claims). The Petition’s reliance on Kleve’s matrix barcode fails. *See* Section IV.A.1., *supra*. As explained by Dr. Malek and the illustrative examples above, the identified matrix barcode does not encode a unique value, as Petitioners’ expert misstates. EX2001, ¶¶ 43-51.

In any event, Kleve actually discourages any “unique access code functioning for the e-key,” as claim 1[i] requires. Kleve shows that its “matrix barcode” alone is “used as the virtual key” (EX1005, ¶ 44); nothing more is required. Kleve explains, “[o]nce the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and *be used to enter and enable the vehicle drive away event.*” *Id.*

Accordingly, the Petition fails to identify any reference that teaches or suggests the recited “the unique access code functioning for the e-key.” Pet. 22-23.

The Petition's failure to demonstrate that any reference, alone or in combination, teaches this limitation of independent claim 1 is, by itself, fatal to Grounds 1 and 2.

**3. Petitioners have failed to show that any reference, alone or in combination, teaches or suggests the “privileges for the unique access code” or “the unique access code is associated with privileges set via the server,” as recited by independent claim 1[g].**

As shown in Section IV.A.1. above, the Petition does not identify any reference that teaches or discloses claim 1's required “coded data from the mobile device *including a unique access code*,” and therefore claim 1[g]'s requirements for that non-existent “unique access code” are likewise missing. EX1001, claim 1. However, even if a matrix barcode somehow “encodes a unique value” (it does not), and even if Kleve had been shown to teach or suggest a matrix barcode “including unique access code” (it was not), the Petition still fails because the relied upon reference does not teach or suggest the specific “privileges” limitations: “*privileges for the unique access code*” or “a unique access code associated with *privileges set via the server*.” EX1001, claim 1.

While the Petition makes the unhelpful and unexplained assertion that “[e]ach virtual key is tied to a time of use and so the privileges are for the unique access code,” these points are irrelevant to the Petition's burden. Pet. 20-21. When Petitioners argue what must be “tied” to *a virtual key*, this wholly ignores the claim's

requirement that the privileges must be “*for the unique access code,*” with those “*privileges set via the server.*” EX1001, claim 1[g].

Indeed, to accept Petitioners’ argument is to render superfluous all of the independent claim’s requirements of the recited “unique access code.” EX1001, claim 1. The Petition cannot render each of these recited elements meaningless by mere assertion.

Because Petitioners have not identified any teaching that Kleve’s server allegedly “set[s]” “*privileges for the unique access code,*” and have not even bothered to explain how anything “tied” to a virtual key could somehow satisfy these recited elements of independent claim 1, the Petition fails to show any reasonable likelihood it will prevail in showing any challenged claim unpatentable.

4. **Petitioners have failed to show that any reference, alone or in combination, teaches or suggests “the privileges are set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle ... privileges are for the unique access code” as recited by independent claim 1[g].**

Even if Petitioners had shown some disclosure of the recited “unique access code,” and even if Petitioners had demonstrated the required “privileges *for* the unique access code” with those “privileges set via the server,” the Petition is still deficient in its failure to show any privilege for the unique access code that is “*responsive to a restriction set by an administrator of the vehicle,*” where “*the*

*restriction is associated with a mode of allowed use of the vehicle.”* EX1001, claim 1[g].

- a) **Neither paragraph 37 nor paragraph 40 of Kleve teaches or suggests the recited “a restriction” in claim 1[g]’s recited element, “the privileges are set via the server *responsive to a restriction set by an administrator of the vehicle ... privileges are for the unique access code.*”**

For the alleged disclosure of the restriction of claim 1[g], the Petition points to Kleve, paragraph 37, which does not teach any restriction at all, and paragraph 40, which teaches that restrictions can be set at step 214, which is *after* a virtual key has already been generated and distributed. Pet. 20-21. But, as discussed in Section IV.A.3. above, the Petition’s alleged privileges are “tied to the virtual key.” Therefore, any restriction set after the distribution of Kleve’s virtual key cannot be “privileges set via the server responsive to a restriction set by an administrator of the vehicle,” as claim 1[g] recites.

- (1) **The Petition’s quotation from Kleve, paragraph 37, fails because this disclosure does not teach or suggest a restriction.**

At paragraph 37, Kleve teaches that the Owner may set up a user profile by inputting information into the website or nomadic device about the vehicle:

[0037] At step 202, the Owner and Temporary User may set up a user profile using a website or a nomadic device communicating with the site that is stored in a database. The Owner may set up a user profile by inputting information into the website or nomadic device including, but not limited to the make, model and year of the vehicle available for rent. The Temporary User may also fill out a user profile using the website or nomadic device to include, but not limited to, photos of credit cards, photo of forms of ID, facial recognition, voice print recognition, matrix barcode (ex. two-dimensional code), code word or phrase for speech recognition, temporary mobile web login IDs and password, or other types of unique Temporary User identification to validate and pay for the rental service at step 204.

EX1005, ¶ 37.

Petitioners *tell* the Board that Kleve, at paragraph 37, discloses that the “owner sets when vehicle is ‘available for rent’”—but this is clearly not what the reference states. Pet. 21, citing EX1005, ¶ 37. Kleve’s *actual* disclosure at paragraph 37, shown above, is not any restriction, but is instead the owner “inputting information ... including but not limited to *the make, model and year of the vehicle available for rent.*” EX1005, ¶ 37. This input of information is not a restriction.

The Petition’s nonsensical reliance on this disclosure is even more pronounced when that disclosure is applied to the required claim language. For example, the Petition leaves unanswered how Kleve allegedly teaches “privileges are for the unique access code,” “privileges set via the server *responsive to* [owner may set a user profile by inputting information ... the make, model and year of the vehicle available for rent].” Pet. 21, citing EX1005, ¶ 37.

And, as the district court construed the term, the “privileges” that are

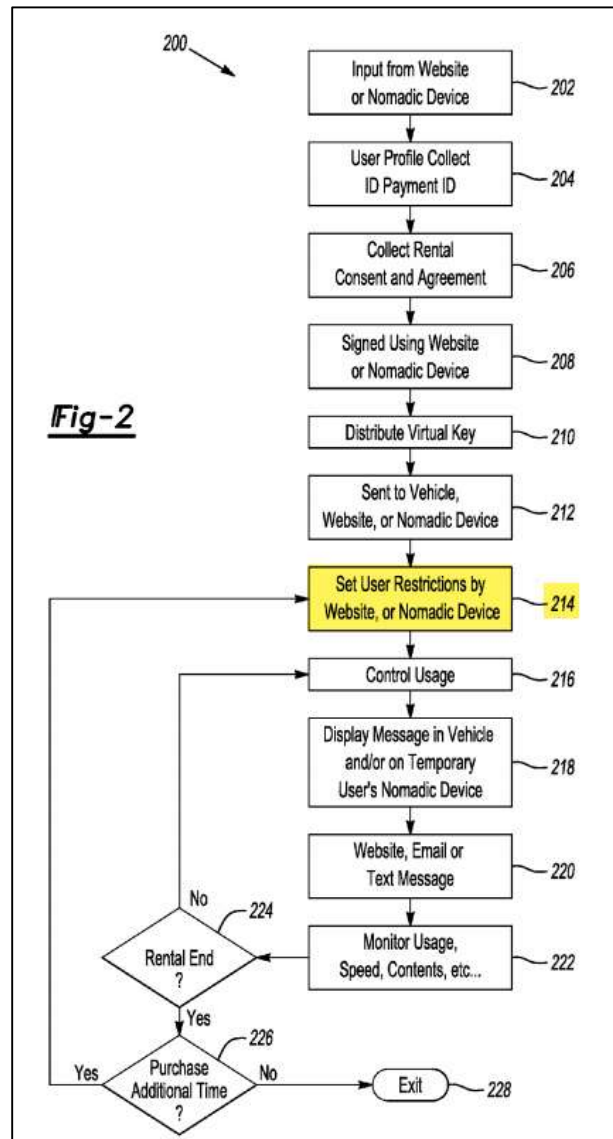
“responsive to a restriction” cannot be merely “unfettered access,” therefore the Petition’s reliance on Kleve at paragraph 37 fails for this reason as well. EX1015, at 12-13; EX1001, claim 1.

- (2) **Kleve, paragraph 40, fails to teach or suggest “privileges are set via the server responsive to a restriction set by an administrator of the vehicle ... privileges are for the unique access code,” as recited by claim 1.**

Petitioners’ reliance on paragraph 40 of Kleve also fails, but this disclosure fails because of *the timing* of when these restrictions are set—which is after distribution of the virtual key. Pet. 21. At paragraph 40 Kleve discloses: “[a]t step 214, the Owner may have access to control usage of the vehicle being rented by the Temporary User.” EX1005, ¶ 40:

[0040] At step 214, the Owner may have access to control usage of the vehicle being rented by the Temporary User. The Owner may set user restrictions by use of the website or nomadic device. The restrictions may be based on, but not limited to, the owner’s selection of parameters including, but not limited to, speed, global position coordinates, or load weight restrictions. At step 216, the control parameters use restrictions may be monitored and if a restriction exceeds a limit the Temporary User and Owner may be notified. The monitoring information may be sent to the Owner through the website, with an email notification, or on the Owner’s nomadic device at step 220. Email notification, text messages or an in-vehicle display message may be sent to notify the Temporary User if a restriction limit has been exceeded at step 218.

But the owner cannot “set user restrictions,” at step 214, until *after* Kleve’s virtual key has already been *distributed*, at step 210:



EX1005, Fig. 2. Accordingly, Petitioners’ alleged “privileges”—“tied” to the virtual key (Pet. 20-21)—cannot be “responsive to” a restriction that is not even set until after the virtual key is distributed, at step 210. EX1005, Fig. 2.

And, in case Kleve’s Figure 2 were not clear enough in showing that “step 214” does not occur until after Kleve’s virtual key has already been distributed, the reference explicitly teaches that its system allows the Owner “control of the vehicle

with the use of *vehicle restriction limits initially set by the Owner at the beginning of the rental term*,” which undisputably occurs after distribution of the virtual key (step 210). *Id.*, ¶¶ 43, 40, Fig. 2. Again, when describing Figure 7, Kleve reiterates *when* a vehicle owner may assign “restrictions”: “*at the start of the rental period*”:

Once the Temporary User initiates the rental event, the system detects a rental time start at step **706**. The system may begin to download performance limitations and *restrictions assigned by the vehicle owner at the start of the rental period* at step **708**.

*Id.*, ¶ 75.

Therefore, as taught by the Petition’s relied-upon reference, restrictions are “*initially* set by the Owner at the beginning of the rental term,” and indeed, the vehicle owner does not even “have access to control usage of the vehicle being rented by the Temporary User” until step 214, *after* a virtual key is distributed at step 210. *Id.*, Fig. 2, ¶¶ 43, 75, 40.

Again, by the claim limitations’ express language, the recited “privileges for the unique access code,” “privileges set via the server” are “*responsive to* a restriction.” EX1001, claim 1. Because Petitioners already alleged the privileges are “tied” to the virtual key (a virtual key that has already been distributed by step 210) (Pet. 20-21), Petitioners’ reliance on Kleve’s paragraph 40 (describing step 214)—unavailable until after the key is distributed—cannot be the recited “restriction set by an administrator of the vehicle” to which “privileges set via the server [are]

*responsive.*” EX1001, claim 1[g].

Therefore, even accepting as true Petitioners’ arguments that (1) Kleve’s matrix barcode somehow “encodes a unique value” that discloses “the unique access code,” and (2) that alleged privileges “tied” to *a virtual key* can somehow satisfy the claim’s recited “privileges for the unique access code”—the Petition still fails in its burden of proof as to claim 1[g] because the alleged “restriction” (Kleve’s “step 214” at paragraph 40) occurs *after the virtual key has already been distributed*.

As with the Petition’s reliance on paragraph 37, paragraph 40 of Kleve cannot satisfy the recited limitations of claim 1: “privileges set via the server *responsive to a restriction set by an administrator of the vehicle* ... privileges are for the unique access code.” EX1001, claim 1.

Accordingly, this failure of proof as to independent claim 1 is fatal to both Grounds 1 and 2.

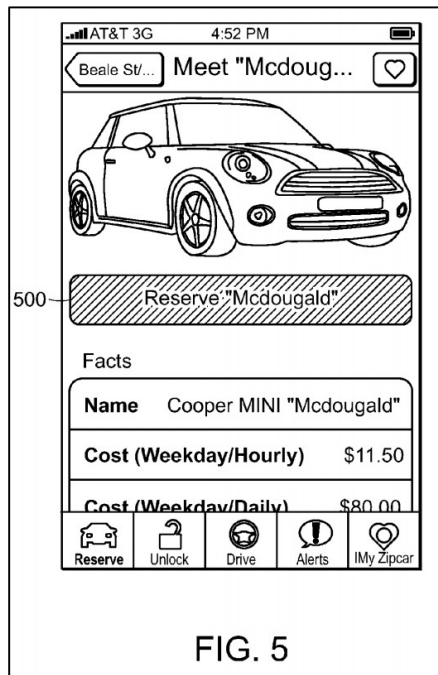
**5. The Petition fails to demonstrate why a POSITA would have been motivated to modify or combine Kleve in view of Mottla.**

To satisfy claim limitation 1[i], reciting “the unique access code functioning for the e-key that is managed via one or more graphical user interface inputs rendered on a screen of the mobile device,” the Petition proposes to combine Kleve and Mottla. However, as demonstrated in Sections IV.A.1.-.2., above, Kleve does not teach or suggest any “unique access code,” let alone any “unique access code

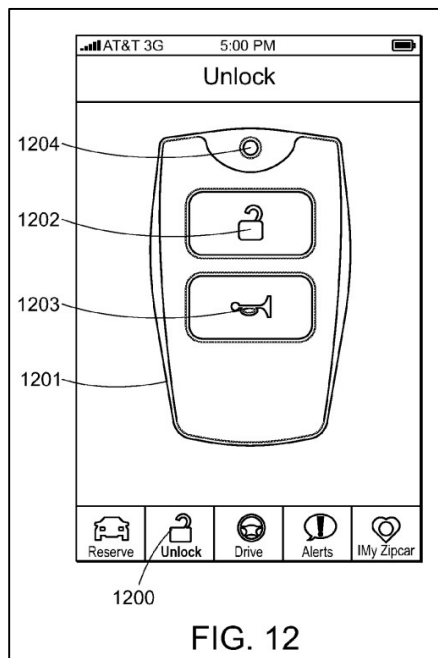
functioning for the e-key.” EX1001, claim 1; *see* Sections IV.A.1.-2., *supra*. Petitioners do not allege that Mottla cures either deficiency of Kleve. Pet. 22-25. Mottla does not disclose the recited “unique access code,” nor do Petitioners allege that it does. *Id.*; EX1006. Accordingly, the combination of references fails to meet the limitations of claim 1[i] regardless of whether the Petition’s proposed combination of references is proper.

It is not, however. EX2001, ¶¶ 52, 58, 63. The Petition first proposes to combine Kleve’s “user interface” (EX1005, Figure 9) and Mottla’s Figure 5, which “illustrates a portion of the user interface for displaying information regarding a selected vehicle” (EX1006, ¶ 15, Figure 5) and Mottla’s Figure 12, which “illustrates a portion of the user interface for displaying an icon for unlocking a vehicle or for making a vehicle sound its horn” (*id.*, ¶ 22).

Mottla is a patent application that discloses mobile applications including a user interface allowing a user to browse reservable vehicles, a user interface to reserve a vehicle, and a user interface which acts like a key-fob. EX1006, Figs. 5, 12, ¶ 33. Examples are shown below as Figures 5 and 12:



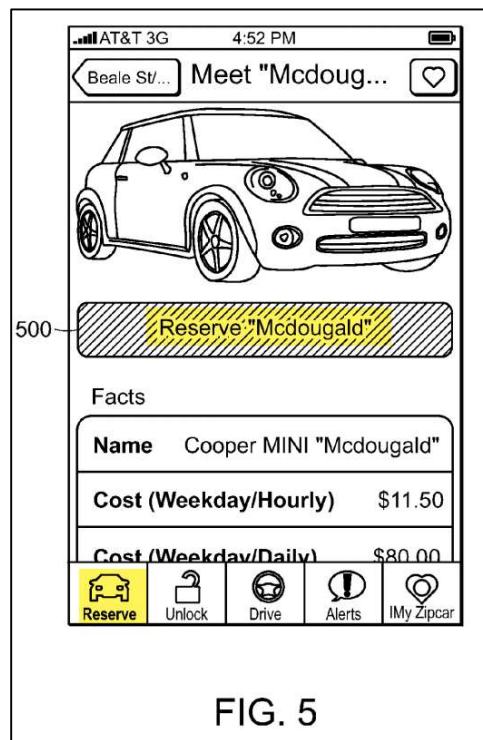
*Id.*, Fig. 5.



*Id.*, Fig. 12.

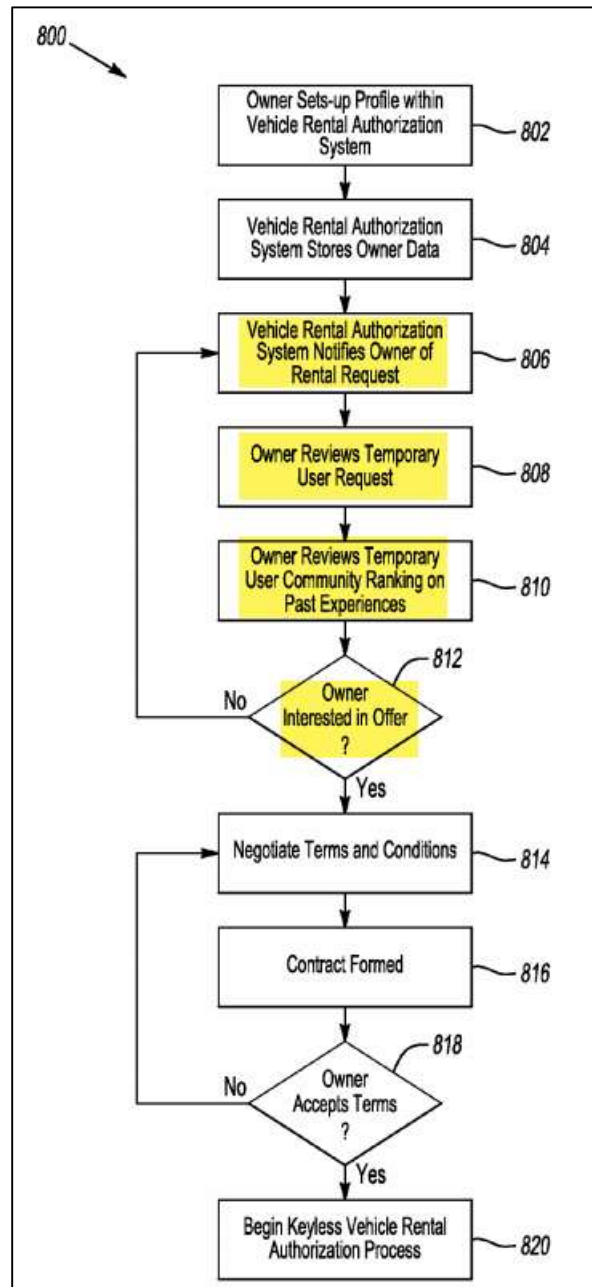
Kleve's teachings actually discourage the proposed modification in view of Mottla. EX2001, ¶¶ 52-55. Kleve's system is intentionally designed to require the vehicle owner to approve or decline any Temporary User's request to rent the vehicle. *Id.*, ¶¶ 55-57. Kleve does not allow, and in fact discourages, the direct "reserve" actions taught by Mottla's user interface. *Id.*, ¶ 58.

For example, Mottla's Figure 5 illustrates graphical user interface inputs which allow a user to make a reservation, i.e., by "select[ing] one or more of the reservable assets," and selecting the "reserve" element 500:



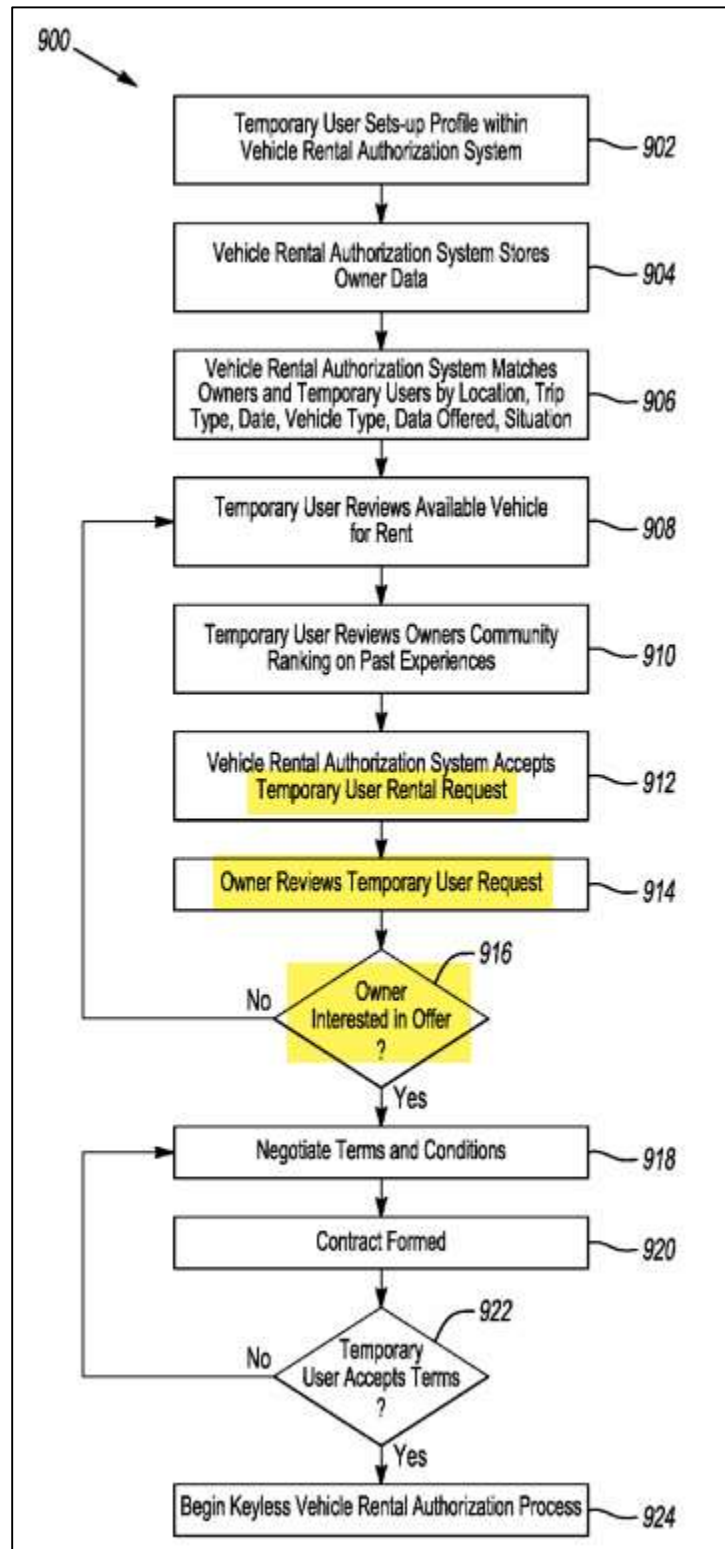
EX1006, Fig. 5, ¶ 27; EX2001, ¶¶ 54-55. Kleve, however, does not allow its "Temporary User" to take the reservation action that Mottla's Figure 5 permits. EX2001, ¶¶ 55-57. Instead, Kleve teaches that the Temporary User may only

“*request*” to rent the owner’s vehicle, then the system will “notify the owner of a *rental request* at step 806,” and at step 808, the “owner reviews [a] Temporary User[’s] *request*,” the owner may further review the “Temporary User Community Ranking” and, importantly, at step 812, the owner must take action to either “decline and wait for the vehicle rental authorization system to notify of any other offers” or “accept the offer.” EX1005, ¶ 84, Figure 8:



As shown in Figure 8 above, and further explained at paragraphs 83 and 84, Kleve teaches that the owner must first “review the requested rental based on what the Temporary User is looking to use the vehicle for,” “when the requested use will be taking place, and where,” “review the Temporary User[’]s profile and rental

history” and Kleve teaches *it is the owner that must ultimately undertake the active operation of accepting or declining the user’s request*. EX1005, ¶¶ 83-84, 89, Figs. 8, 9; EX2001, ¶¶ 55-56. Kleve’s Figure 9, showing the “interface” available to the Temporary User, reiterates Kleve’s teaching on this point—the Temporary User may only “request” to rent a vehicle, which, as an initial matter, must be accepted by the “vehicle rental authorization system” at step 912. *Id.*, Fig. 9. Additionally, that “request” still requires prerequisite actions undertaken by the owner, i.e. review of “request” and if the owner is “interested in offer,” the owner may accept or decline the request. *Id.*, ¶¶ 83-84, 89, Figs. 8-9.



*Id.*, Fig. 9; *see also id.*, ¶ 89 (“If the owner has decided to accept the offer, he may begin the process of developing terms and conditions of the rental period.”).

Accordingly, Kleve actually discourages the Temporary User from taking the direct “reserve” action taught by Mottla’s Figure 5. EX2001, ¶¶ 52, 55-58. In fact, Kleve specifically discourages those actions enabled by the graphical user interface inputs of Mottla’s Figure 5—whereby the user can, *without any approval*, “select one or more of the *reservable assets*” and “*reserve*” that selected vehicle using the Figure 5 interface element 500. EX1006, ¶ 27, Fig. 5; EX2001, ¶ 58.

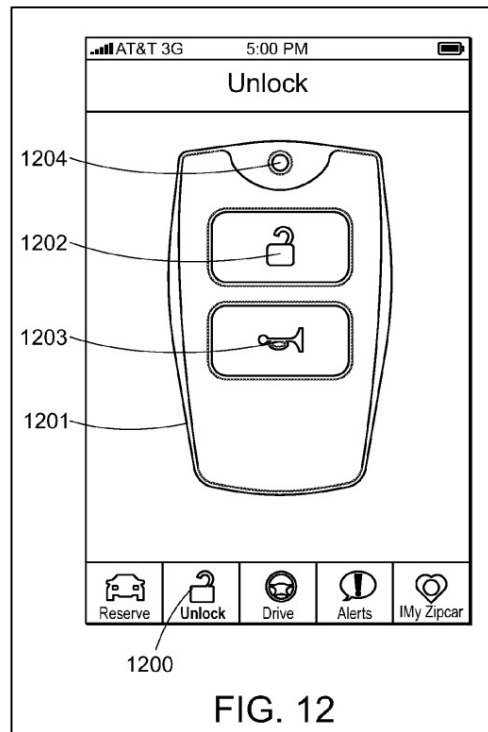
The Petition also fails to demonstrate why a POSITA would have been motivated to modify Kleve’s matrix barcode in view of Mottla’s graphical user interface inputs, shown in Figure 12. EX2001, ¶¶ 52, 59, 62.

Kleve already teaches that the “matrix barcode” *itself* is passively “used as the virtual key,” that this matrix barcode is simply scanned by the vehicle and “used to enter and enable the vehicle drive away event,” without ever requiring that the Temporary User actively select any inputs to enter or start the vehicle. EX1005, ¶ 44 (“Once the Temporary User has the *matrix barcode scanned by the vehicle*, the smart phone may be able to connect with the VCS and be *used to enter and enable the vehicle drive away event.*”):

[0044] Another exemplary example of the vehicle rental micro-business system may include other enhancements including, but not limited to, matrix barcode (ex. two-dimensional code) used as the virtual key being recognized by the VCS. The smart phone may be used to communicate the matrix barcode information to the vehicle rental micro-business system directly. The system may be able to communicate information from the smart phone to the vehicle notifying the VCS of a virtual key. Once the Temporary User has the matrix barcode scanned by the vehicle, the smart phone may be able to connect with the VCS and be used to enter and enable the vehicle drive away event.

*Id.*, EX2001, ¶ 60.

Mottla, by contrast, requires *active input* by the user to select certain buttons for executing certain operations, i.e., “a member selects a lock icon 1200 that causes the mobile device application to display a user interface with another icon 1201 that has a button 1203 for causing a vehicle 104 to sound its horn, or button or buttons 1202 to lock or unlock the vehicle doors.” EX1006, ¶ 33, Fig. 12:



*Id.*; EX2001, ¶ 61.

Petitioners fail to explain how the matrix barcode of Kleve would be combined with the graphical user interface of Mottla or how the two in combination would be expected to function. Pet. 22-25; EX2001, ¶¶ 62-63. Indeed, Kleve teaches that its matrix barcode is a passive mode of communication that is scanned by the vehicle's VCS, without any buttons for the user to select. EX1005, ¶ 44; EX2001, ¶¶ 60, 62. Moreover, Kleve teaches that the barcode is scanned at the vehicle and that this scanned barcode is used to enter and enable the vehicle drive away event. EX1005, ¶ 44; EX2001, ¶¶ 60, 62. Mottla, by contrast, teaches that a member must actively select buttons to unlock a door, sound a horn, etc. EX1006, ¶ 33, Fig. 12; EX2001, ¶ 61. Petitioners do not explain how to combine Kleve's matrix barcode with

Mottla's selectable buttons, let alone why a POSITA would add buttons for "unlocking," for example, when Kleve's matrix barcode already accomplishes this operation when scanned. Pet. 22-25; EX2001, ¶¶ 62-63.

Thus, Petitioners have failed to show that a POSITA would have had an "apparent reason to combine the known elements." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness")). A patent claim "is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR*, 550 U.S. at 418. An obviousness determination based on a combination of references requires finding "both 'that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.'" *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367-68 (Fed. Cir. 2016) (quoting *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1360 (Fed. Cir. 2012)).

For this reason alone, the Petition cannot sustain its burden as to claim 1[i], and therefore both Grounds 1 and 2 fail.

Moreover, because neither reference was shown to teach or suggest the recited "unique access code," or "the unique access code functioning for the e-key," as

recited by claim 1[i], Grounds 1 and 2 fail regardless of whether the combination is proper. Pet. 22-25.

6. **Petitioners have failed to show any reference, alone or in combination, teaches or suggests a “camera capturing video ... during a period of time in which the unique access code is to be active,” as recited by independent claim 1[h].**

While Petitioners reduce independent claim 1 to requiring a “camera,” the Petition ignores the actual claim language recited by the limitation. Specifically, limitation 1[h] recites:

a camera of the vehicle is used for capturing video of an area that includes the vehicle *during a period of time in which the unique access code is to be active*, such that actions taken by a user using an electronic key (e-key) is recorded[.]

It is unsurprising that the Petition fails to identify any disclosure of “a camera of the vehicle [] used for capturing video ... *during a period of time in which the unique access code is to be active*,” as Petitioners failed to identify any teaching or suggestion of any “unique access code” whatsoever. *See* Section IV.A.1., *supra*; EX1001, claim 1. The Petition’s failures with respect to the required “unique access code” of limitation 1[f] are highlighted here as well. The Petition does not demonstrate any “unique access code,” let alone the recited element requiring a “period of time in which the unique access code is to be active[.]” EX1001, claim 1[h].

Because the Petition fails to show any teaching or suggestion that satisfies either “the unique access code,” or “a camera of the vehicle [] used for capturing video ... during a period of time in which the unique access code is to be active,” as recited by claim 1[h], Grounds 1 and 2 both fail.

**B. Petitioners’ Zaid-based Grounds 3 and 4 fail for at least the same failures of proof identified by the Board in IPR2024-00981.**

Petitioners’ reliance on Zaid for alleged disclosure of multiple limitations of independent claim 1 is fatal to Grounds 3 and 4. In IPR2024-00981, the Board already concluded that Zaid’s vehicle owner does not set any restriction for the relied-upon vehicle reservation, instead it is the renter alone who makes a vehicle reservation, for which the server receives “a request that generates an electronic key.” EX2004, 45. The Board already rejected Petitioners’ reliance on an owner announcing or advertising “vehicle availability” or vehicle location” as any alleged “rental period restriction.” EX2004, 45-46. Here, again, Petitioners point to the same failed disclosures of Zaid to try to satisfy multiple limitations of independent claim 1.

In dismissing each of Petitioners’ Zaid-based Grounds in its Final Written Decision on the related ’188 Patent, the Board not only rejected the idea that Zaid’s vehicle owner sets any restriction for the vehicle reservation, the Board also determined that the “vehicle renter uses his or her own account to make a reservation

and to send a request that generates an electronic key.” EX2004, 45. The Board found that Zaid teaches that the relied-upon reservation is made via a *renter’s* social media account, and Zaid offers no “teaching or suggestion that such a user account would encompass the vehicle owner.” *Id.*, 46.

Here, the Petition’s renewed reliance on Zaid is equally misplaced. Petitioners’ identification of alleged “restrictions” by a vehicle owner—announcing vehicle availability, vehicle location—have already been rejected by the Board as failing to teach a restriction of use set by the owner for the reservation. *Id.* Accordingly, the Petition’s reliance here on these same already-rejected disclosures likewise fails to show the independent claim’s recited “privileges set via the server responsive to a restriction set by an administrator, the restriction is associated with a mode of allowed use of the vehicle.” EX1001, claim 1.

### **1. The Zaid Reference (EX1008)**

The inapplicability of Zaid is manifest in the reference itself. EX1008. Zaid is not directed to any vehicle configured to receive a unique access code that is functioning for an e-key, with privileges defined for the unique access code—privileges set via the server responsive to a specific “restriction” set by the owner or administrator of the vehicle. *Id.*; EX1001, Abstract; EX2004, 16-20. Nor does Zaid disclose or suggest the specific kind of restriction for which the unique access code’s privileges are set: “the restriction is associated with a mode of allowed use of the

vehicle.” EX1001, claim 1.

Instead, Zaid discloses that a prospective vehicle renter can log into their Facebook or a similar social networking site, view an ad for a vehicle—an ad placed by a vehicle owner—and, if interested, the renter can click on that ad and make a reservation. EX1008, ¶ 72; EX2004, 45. But, contrary to the Petition’s argument, Zaid teaches “*a customer* uses their wireless communication device 106 to search for and make a reservation for a vehicle, which is communicated to a central server 110.” EX2004, 18; EX1008, ¶¶ 71-77. Once the renter makes the reservation, that reservation is relayed as an encrypted message. *Id.*, ¶¶ 125-127. There is nothing in Zaid suggesting that the owner may set, or does set, any restriction associated with a mode of allowed use of the vehicle, let alone any teaching that Zaid’s server sets privileges for the reservation that are “responsive to” any restriction set by the owner. *Id.*, ¶¶ 72-74, 79-81; EX2004, 45.

Accordingly, Zaid’s reservation, which is made by the renter alone, and, by the Board’s finding, is itself “a request that generates an electronic key,” has no “privileges set via the server responsive to a restriction set by an administrator,” as each of the challenged claims require. EX2004, 45; EX1001, claim 1.

**2. The Board already determined that the alleged “time period” of Zaid’s reservation is not set by the owner as the Petition contends, therefore Petitioners’ Zaid-based Grounds 3 and 4 both fail.**

Petitioners identify Zaid’s “decrypted vehicle reservation” as claim 1’s recited “unique access code,” but rely on the same already-rejected disclosures from Zaid as the recited “restriction” of claim 1. Pet. 52, 54.

Assuming, *arguendo*, Zaid’s reservation were a “unique access code,” Zaid would still fail to teach or suggest independent claim 1’s required limitations of “privileges set via the server *responsive to a restriction set by an administrator* of the vehicle.” EX1001, claim 1.

The Board’s decision in IPR2024-00981 already rejected Petitioners’ allegation that Zaid’s owner updating “vehicle availability and vehicle location” is a “rental period restriction.” EX2004, 45-46. As illustrated below, in their Petition for IPR2024-00981, Petitioners also argued that Zaid’s reservation was “for a specified time period, which is a condition of use of the vehicle.” IPR2024-00981, Paper 3 at 47. There, as here, Petitioners further alleged that this time period or “condition of use of the vehicle” is set “when the owner ‘announces when the vehicle is available for sharing,’ which sets limits on the specific time period for reserving the vehicle,” and, Petitioners alleged, Zaid’s server assigns the reservation a “rental period restriction.” *Id.*:

*“the request includes a condition of use of the vehicle as set by the user via the user account”*: Zaid states that the reservation request “includes a reservation for a specified time period,” which is *a condition of use of the vehicle*. Ex. 1008, ¶69. This condition is *set by the user via the user account* such as when the owner “announces *when the vehicle is available for sharing*,” which sets limits on the specific time period for reserving the vehicle. *Id.*, ¶77; Ex. 1003, ¶219.

As discussed above, Zaid discloses or renders obvious that the server generates an encrypted reservation (*e-key*) and assigns it to a rental period restriction (*condition of use of the vehicle*). Ex. 1008, ¶69. In addition, Harris discloses

IPR2024-00981, Paper 3 (Petition) at 47; *see also* IPR2024-00981, Paper 24 (Petitioners’ Reply) at 22:

The “vehicle reservation application” is for advertising vehicle rentals, and is therefore connected to the “social networking website” on which a renter can “view the advertisement and make [a] reservation.” EX1008, ¶¶72, 77. Thus, when Zaid says the owner can set “when the vehicle is available for sharing,” a POSITA would understand that that is the same “specified time period” that is included in the reservation request. EX1008, ¶¶77, 69.

Moreover, Petitioners pointed to Zaid’s “vehicle reservation” being “booked by a user at a central server.”

Zaid states that a “vehicle reservation is booked by a user at a *central server*,” after which “the central server encrypts the message containing the vehicle reservation.” Ex. 1008, ¶125. A POSITA would understand that the vehicle reservation request

IPR2024-00981, Paper 3 at 44.

In challenging the claims of the '245 Patent, Petitioners again rely on the same disclosures and arguments that were already rejected as allegedly showing an owner announcing / advertising vehicle availability or vehicle location as a “rental period restriction” for the vehicle reservation. EX2004, 45-46.

*Zaid's* access and use privileges are set via the server responsive to a restriction set by a vehicle administrator. *Zaid's* vehicle owner can “update the server(s) (e.g., online vehicle reservation system) of various vehicle related information such as vehicle availability and vehicle location...used by the backend vehicle sharing system to register the vehicle as available for sharing.” *Zaid*, [0079]. Thus, the vehicle owner restricts vehicle availability to particular times. Almeroth, ¶226. Once the user identifies a vehicle, “[t]he vehicle reservation is booked at the server” subject to the owner’s restrictions. *Zaid*, [0080], [0125]. The reservation is then encrypted and distributed to the mobile device and vehicle. Accordingly, *Zaid's* time-limited access and use privileges are set via *Zaid's* central server responsive to the selected time period being within the vehicle owner’s identification of availability. Almeroth, ¶226.

Pet. 54.

In this Petition, the deficiency of these arguments is even more pronounced: *Zaid's* owner updating “various vehicle related information such as vehicle availability and vehicle location”—at paragraph 79—is not the recited “restriction set by an administrator of the vehicle,” as required by claim 1. EX1008, ¶ 79. As

Zaid explains, the owner making a “vehicle availability” update is just an advertisement or announcement. *See e.g.*, EX1008, ¶ 77 (“advertise or announce when the vehicle will be available for sharing”). Zaid’s owner advertising or announcing when the vehicle is available for sharing is just what Zaid says it is, an advertisement or announcement—and that vehicle availability can of course be a year (or more), or months within a year, or weeks within a month, or days within a week, etc. *Id.* Zaid does not teach or suggest the owner advertising the vehicle available for sharing—e.g., 10 months out of the year—as somehow setting forth the “reservation period,” as Petitioners allege. Pet. 54-55.

Indeed, the Board already found that Zaid owner does not set any condition of use for the reservation. Instead, Zaid teaches “the vehicle renter uses his or her own account to make a reservation and to send a request that generates an electronic key”—there is no involvement by the owner in the reservation itself nor any suggestion that such a request to the server would somehow emanate from the vehicle owner. EX2004, 45-46.

For at least these reasons, the Petition fails to show that Zaid teaches or discloses the recited “privileges set via the server responsive to a restriction set by an administrator of the vehicle, the restriction is associated with a mode of allowed use of the vehicle.” EX1001, claim 1. Grounds 3 and 4 fail because of these deficiencies alone.

**C. For Grounds 3 and 4, Petitioners’ reliance on the Examiner’s findings is of no avail, as the Examiner agreed Zaid does not teach or suggest the limitations of claim 1.**

Though the Petition relies heavily on the Examiner’s findings during prosecution, Petitioners fail to explain the Examiner’s agreement that Zaid did not teach limitations of [current] claim 1. For example, the Examiner concluded that Zaid “fails to expressly teach” the claims’ recited “the restriction is associated with a mode of allowed use.” EX1002, 124-25. The Petition tells the Board that the Examiner “ultimately determine[ed] that this limitation is disclosed,” but neglects to also tell the Board that the Examiner had *modified Zaid with another reference, Joao*, for alleged disclosure of the “restriction” limitation. Pet. 53; EX1002, 124-25.

Despite this background, and despite Petitioners’ express reliance on the Examiner’s findings, the Petition does not cite to or explain the actual evidence on which the Examiner relied, the Petition does not even mention or rely on the Joao reference, and in fact the Petition does not rely any other reference for alleged disclosure of the “restriction” limitation Zaid “fails to expressly teach.” Pet. 53; EX1002, 124-25.

**1. The Petition fails to identify any disclosure to satisfy claim 1[i]’s recited “the unique access code functioning for the e-key.”**

For Grounds 3 and 4, the Petition does not point to any disclosure, *from any reference*, which allegedly satisfies the recited “the unique access code functioning

for the e-key[.]” Pet. 56-59; EX1001, claim 1. Instead, the Petition relies on the Examiner’s conclusions, which, if true, not only doom the Petition’s burden of proof as to claim 1[i], but also render nonsensical the Petition’s relied-upon disclosures for claim 1[f]. Accordingly, as detailed below, the Petition’s reliance on this conclusion is fatal to both independent claim limitations 1[f] and 1[i].

While the Petition points to Zaid’s “vehicle reservation” as the claim’s recited “coded data” (Pet. 49) and further points to Zaid’s “decrypted vehicle reservation” as the alleged “unique access code” that is “include[ed]” in the “coded data” (Pet. 52), the Examiner had instead relied on Zaid’s disclosure at paragraph 81 as the alleged “unique access code.” EX1002, 124, citing EX1008, ¶ 81. At paragraph 81, Zaid discloses “the unique increment is in the form of a counter and/or time stamp that indicate[s] the uniqueness of the message to avoid a repeat message attack.” EX1008, ¶ 81. However, this “unique increment” cannot satisfy the claim’s recited “coded data ... including a unique access code,” at least because Zaid teaches that this “unique increment” is not included in Zaid’s “vehicle reservation”—the disclosure Petitioners identify as the claim’s recited “coded data.” Pet. 49.

Zaid discloses that its “unique increment” is not part of the vehicle reservation, but is instead part of every “communication”—included “for each message to avoid a repeat message attack.” EX1008, ¶ 81. Zaid explains that its unique increment is part of *each message*, making each message *unique*. *Id.*

Whether or not the message includes an update, or a vehicle reservation, or any other “communication,” Zaid is clear that it is only *the message* that is taught to include a “unique increment.” EX1008, ¶¶ 81, 130. Because Zaid’s unique increment is not “included” in the vehicle reservation itself—which Petitioners identify as the alleged “coded data”—Zaid’s “unique increment” cannot meet claim 1[f]’s recited “the coded data ... including a unique access code.” EX1001, claim 1.

Additionally, Petitioners failed to point to any disclosure in Zaid that teaches or suggests that its “unique increment” is somehow “functioning for the e-key,” as claim 1[i] requires. To the contrary, as shown above, Zaid’s “unique increment” is a security feature that merely “indicate[s] the uniqueness of the message to avoid a repeat message attack.” EX1008, ¶ 130.

Accordingly, because Petitioners relied only on conclusions from the Examiner for alleged disclosure of “the unique access code functioning for the e-key”—conclusions which do not meet the required elements of claim 1[i] and further contradict the Petition’s own arguments as to claim 1[f]—the Petition fails as to both limitations 1[f] and 1[i]. Pet. 56-59.

**2. The Petition fails to demonstrate why a POSITA would have been motivated to modify Zaid in view Mottla.**

The Petition’s rationale for modifying Zaid with Mottla is facially deficient. For example, Petitioners argue that a POSITA would have been motivated to use

Mottla’s system “*instead of scanning the virtual key*—providing a better user experience while maintaining security.” Pet. 58. But Zaid does not teach or suggest “scanning the virtual key.” EX1008. This argument makes no sense.

Equally nonsensical is Petitioners’ piggybacking on the Examiner’s use of Mottla “to conveniently control the vehicle.” Pet. 56, citing EX1002, 124-25. Petitioners already told the Board that Zaid’s mobile device is used to perform “unlocking requests,” i.e., “the vehicle receives a request from a mobile device that unlocks the vehicle[.]” Pet. 49. But, in seeking to piggyback on the Examiner’s addition of Mottla to Zaid’s teachings, Petitioners never explain why Zaid’s operations for unlocking the vehicle somehow “*inconveniently control the vehicle,*” such that a POSITA would be motivated to look to Mottla for alleged improvement as to “convenience.” Pet. 56-59.

And, as discussed in Section IV.A.5, above, with respect to the impropriety of Petitioners’ combination of Kleve and Mottla, here too, Petitioners fail to satisfy their burden because the Petition does not explain why a POSITA would be motivated to add Mottla’s graphical user interface inputs, e.g., for unlocking the vehicle, when Petitioners concede that Zaid’s mobile device already performs these unlocking requests. *See* Pet. 49; *see also* Section IV.A.5., *supra*.

The alleged combination also fails because Petitioners failed to demonstrate any reasonable expectation of success in making this proposed modification. Pet.

56-59. Because the Petition merely repeats the Examiner’s conclusion—that Zaid’s “unique increment” satisfies the recited “unique access code functioning for the e-key”—the Petition fails to demonstrate *how to combine* the “unique increment” of Zaid with Mottla’s graphical user interface inputs, let alone *how* this undescribed combination *would function*.

Petitioners’ cursory treatment of the Examiner’s findings fails to meet their required burden to show “both ‘that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.’” *Intelligent Bio-Sys., Inc.*, 821 F.3d at 1367–68 (quoting *Kinetic Concepts, Inc.*, 688 F.3d at 1360).

Accordingly, the Petition fails to meet its burden of obviousness, as there is no showing that a POSITA would have been motivated to modify Zaid in view of Mottla. And, as a distinct deficiency, the Petition fails to demonstrate that a POSITA would have had a reasonable expectation of success in doing so.

Regardless, however, the combination still fails to satisfy claim limitation 1[i], for the reasons set forth in Section IV.C.1., above.

**3. The Petition fails to show that Zaid, or Zaid in combination with Kleve, teaches or suggests the recited elements of claim 1[h].**

Zaid’s “camera” is not one which, as claim 1[h] recites, “is used for capturing

video .... during a period of time in which the unique access code is active ...” and Petitioners do not allege that it is. Pet. 55-56. Petitioners therefore propose to modify Zaid with Kleve, relying on the same deficient disclosures for the Petition’s Kleve-based Grounds. *Id.* However, as shown in Section IV.A.6., above, Kleve also fails to teach or suggest this limitation of claim 1. *See* Section IV.A.6., *supra*. The Petition’s combination of Zaid and Kleve does not cure the numerous deficiencies of Kleve, nor do Petitioners allege that it does. *Id.*; Pet. 55-56.

Accordingly, the Petition’s Grounds 3 and 4 fail for at least the same reasons as set forth in Section IV.A.6. *See* Section IV.A.6., *supra*.

## **V. Conclusion**

For the reasons presented above, the Petition should be denied, and no *inter partes* review should be instituted.

Dated: January 23, 2026

/Brenda Entzminger/  
Brenda Entzminger, Reg. No. 76,896

**CERTIFICATE OF WORD COUNT**

The undersigned certifies that the foregoing PATENT OWNER'S  
PRELIMINARY RESPONSE complies with the type-volume limitation in 37  
C.F.R. § 42.24(b)(1). According to the word-processing system's word count, the  
brief contains 10,292 words, excluding the parts of the brief exempted by 37  
C.F.R. § 42.24(a).

Dated: January 23, 2026

/Brenda Entzminger/  
Brenda Entzminger  
Reg. No. 76,896 (Lead counsel)  
Aaron R. Hand  
Reg. No. 80,694 (Back-up  
counsel)  
**BUNSOW DE MORY LLP**  
701 El Camino Real  
Redwood City, CA 94063  
Telephone: 650-318-6774  
Facsimile: 415-426-4744  
bentzminger@bdiplaw.com  
ahand@bdiplaw.com

*Counsel for Patent Owner*

**CERTIFICATE OF SERVICE**

Petitioners have consented to e-mail service in this proceeding. Pursuant to 37 C.F.R. §42.6, the undersigned certifies that, on the date indicated below, a copy of the foregoing document was served by email upon the following counsel at the below email addresses:

Finnegan, Henderson, Farabow, Garrett & Dunner LLP  
Joshua L. Goldberg – [joshua.goldberg@finnegan.com](mailto:joshua.goldberg@finnegan.com)  
James R. Barney - [james.barney@finnegan.com](mailto:james.barney@finnegan.com)  
Aidan Skoyles - [aidan.skoyles@finnegan.com](mailto:aidan.skoyles@finnegan.com)  
Nicholas Eitsert - [nicholas.eitsert@finnegan.com](mailto:nicholas.eitsert@finnegan.com)

QUINN EMANUEL URQUHART & SULLIVAN, LLP  
James M. Glass – [jimglass@quinnemanuel.com](mailto:jimglass@quinnemanuel.com)  
Quincy Lu - [quincylu@quinnemanuel.com](mailto:quincylu@quinnemanuel.com)  
Joseph Milowic - [josephmilowic@quinnemanuel.com](mailto:josephmilowic@quinnemanuel.com)

Dated: January 23, 2026

/Brenda Entzminger/  
Brenda Entzminger  
Reg. No. 76,896 (Lead counsel)  
Aaron R. Hand  
Reg. No. 80,694 (Back-up  
counsel)  
**BUNSOW DE MORY LLP**  
701 El Camino Real  
Redwood City, CA 94063  
Telephone: 650-318-6774  
Facsimile: 415-426-4744  
[bentzminger@bdiplaw.com](mailto:bentzminger@bdiplaw.com)  
[ahand@bdiplaw.com](mailto:ahand@bdiplaw.com)

*Counsel for Patent Owner*