

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KIA CORP.,
TOYOTA MOTOR CORP.,

Petitioners,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner.

Case IPR2024-01167
U.S. Patent No. 11,738,659

**PATENT OWNER'S
PRELIMINARY RESPONSE
UNDER 37 C.F.R. §42.107**

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction.....	1
II. The '659 patent.....	2
A. File History of the '659 patent	4
B. POSITA	5
C. Toyota's recognition of importance of the '659 patent.....	6
III. Should the Board reach the merits, institution should be denied because Petitioners have failed to demonstrate any reasonable likelihood of success for any challenged claim.	8
A. Grounds 1-2 (Kleve / Hatton) do not present any reasonable likelihood of success.	9
1. Brief summary of Kleve.....	9
2. Brief summary of Hatton	13
3. The proposed combination of Kleve and Hatton fails to teach or suggest the "coded data includes privilege settings" limitations.	14
4. The proposed combination of Kleve and Hatton fails to teach or suggest that the alleged "memory" has "program instructions for instructing/controlling unlocking and starting of the vehicle."	21
5. It would not have been obvious to combine Kleve and Hatton as Petitioners propose.....	23
6. The Sekiyama references does not cure the deficiencies of Kleve/Hatton.....	26
B. Grounds 3-6 (Mikan) - do not present any reasonable likelihood of success.	26
1. Brief summary of Mikan.....	26

2.	Mikan fails to teach or suggest that the alleged “coded data includes privilege settings.”	27
3.	Petitioners’ secondary references do not cure Mikan’s deficiencies.....	32
IV.	The Board Should Deny Institution Under <i>Fintiv</i>	33
A.	The Board need not address the merits of the Petition because the factors favor denial	34
1.	Factor 1 Favors Denial (Likelihood of Stay)	34
2.	Factor 2 Favors Denial (Timing of Trial); Trial will conclude at least six months before any final written decision	36
3.	Factor 3 Favors Denial (Investment in Parallel Proceedings); before the institution decision, discovery will be near complete and the Court will have held a <i>Markman</i> hearing.	39
4.	Factor 4 Favors Denial (Overlap of Issues).....	42
5.	Factor 5 Favors Denial (Overlapping Parties)	45
6.	Factor 6 Favors Denial (Other Circumstances)	46
V.	The Petition should be denied in view of the co-pending EPR.....	46
VI.	Section 311(B) of the AIA and the SCOTUS Ruling in <i>SAS</i> Prevent Institution	47
VII.	Conclusion	49

TABLE OF AUTHORITIES

	<u>Page(s)</u>
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019 (P.T.A.B. Mar. 20, 2020)	passim
<i>Code200 Uab v. Luminate Networks Ltd.</i> , IPR2020-01506 (P.T.A.B. Feb. 16, 2021)	42
<i>Constant v. Advanced Micro-Devices, Inc.</i> , 848 F.2d 1560 (Fed. Cir. 1988).....	48
<i>eClinicalWorks, LLC v. Decapolis LLC</i> , IPR2022-00229 (P.T.A.B. Apr. 13, 2022).....	37
<i>E-One, Inc. v. Oshkosh Corp.</i> , IPR2019-00161 (P.T.A.B. May 15, 2019).....	37, 41
<i>Force Mos Tech., Co. v. ASUSTek Comput., Inc.</i> , No. 2:22-CV-00469-JRG, 2024 WL 1586266 (E.D. Tex. Apr. 11, 2024).....	35
<i>Immersion Systems LLC v. Midas Green Techs., LLC</i> , PGR2021-00104 (P.T.A.B. Jan. 31, 2022)	37
<i>Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson</i> , No. 2:21-CV-00113-JRG, 2022 WL 17484264 (E.D. Tex. July 7, 2022)	35
<i>Lynk Labs, Inc. v. Samsung Elecs. Co.</i> , No. 2023-2346 (Fed. Cir.).....	48
<i>Mylan Labs. Ltd. v. Janssen Pharmaceutica NV</i> , IPR2020-00440 (P.T.A.B. Sept. 16, 2020).....	36, 41
<i>Netflix, Inc. v. Uniloc 2017 LLC</i> , IPR2020-00008 (P.T.A.B. Apr. 13, 2020).....	37
<i>NXP USA, Inc. v. Impinj, Inc.</i> , PGR2022-00005 (P.T.A.B. May 2, 2022)	37
<i>Samsung Elecs. Co. v. Clear Imaging Research, LLC</i> , IPR2020-01401 (P.T.A.B. Feb. 17, 2021).....	44, 45, 48

<i>Sand Revolution II, LLC v. Cont'l Intermodal Grp.</i> , IPR2019-01393 (P.T.A.B. June 16, 2020).....	39, 45
<i>Scorpcast, LLC v. Boutique Media</i> , No. 2:20-cv-00193-JRG-RSP, 2021 WL 3514751 (E.D. Tex. June 8, 2021)	35
<i>St. Lawrence Commc'ns LLC v. ZTE Corp.</i> , No. 2:15-CV-349-JRG, 2017 WL 3396399 (E.D. Tex. Jan. 17, 2017).....	35
<i>Teso LT UAB v. Luminati Networks Ltd.</i> , IPR2021-00122 (P.T.A.B. Apr. 20, 2021).....	43
<i>U.S. Venture, Inc. v. Sunoco Partners Mktg. & Terminals L.P.</i> , IPR2020-00728 (P.T.A.B. Oct. 1, 2020)	44
<i>Valve Corp. v. Ironburg Inventions Ltd.</i> , 8 F.4th 1364 (Fed. Cir. 2021).....	48

Statutes

35 U.S.C. § 102	46
35 U.S.C. § 311(b)	1, 46, 47
35 U.S.C. § 314.....	1, 33

Patent Owner's Exhibit List	
EX2001	Declaration of Dr. Sam Malek
EX2002	<i>Curriculum Vitae</i> of Dr. Malek
EX2003	<i>Reserved</i>
EX2004	Cover pleading to Defendants' Preliminary Invalidity Contentions, <i>Emerging Automotive LLC v. Kia Corporation, et. al., and Toyota Motor Corp. et al.</i> , No. 2:23-cv-0437-JRG (lead case), No. 2:23-cv-0434-JRG (member case), served March 28, 2024
EX2005	<i>Reserved</i>
EX2006	Judicial Caseload Profile (June 30, 2024): Table C-5, <i>U.S. District Courts—Civil Federal Judicial Caseload Statistics</i> ; Table T-3, <i>U.S. District Courts—Median Time from Filings to Trial for Civil Cases in which Trials were Completed</i>
EX2007	Civil Docket Report for <i>Emerging Automotive LLC v. Kia Corporation, et. al., and Toyota Motor Corp. et al.</i> , No. 2:23-cv-0437-JRG (lead case)
EX2008	Civil Docket Report for <i>Emerging Automotive LLC v. Toyota Motor Corp. et al.</i> , No. 2:23-cv-0434-JRG (member case)
EX2009	U.S. Patent No. 11,295,564
EX2010	<i>Reserved</i>
EX2011	Related Applications Search results for US Patent 11,295,564 from United States Patent Office Global Dossier Public Access Portal
EX2012	U.S. Patent No. 10,493,953
EX2013	U.S. Patent No. 10,614,644
EX2014	U.S. Patent No. 11,094,149
EX2015	<i>Reserved</i>
EX2016	Docket Navigator Median Time-to-Trial Statistics for Judge Rodney Gilstrap (excluding transfers), August 26, 2019 through August 26, 2024
EX2017	Unified Patents, LLC Request for <i>Ex Parte</i> Reexamination of U.S. Patent No. 11,738,659 (Mar. 25, 2024)
EX2018	Unified Patents Website, Members Section, available at https://www.unifiedpatents.com/members

Patent Owner's Exhibit List	
EX2019	Office Action in <i>Ex Parte</i> Reexamination, Application Number 90/019,456 (Sept. 4, 2024)
EX2020	Office Action Response Remarks from Robert B. Kleve (Aug. 14, 2014)

I. Introduction

The Board should deny institution of *inter partes* review of U.S. Patent No. 11,738,659 (1) because Petitioners fail to demonstrate any reasonable likelihood that any challenged claim is anticipated or obvious; (2) because of discretionary considerations; and (3) because § 311(b) of the AIA and the Supreme Court’s ruling in *SAS* prevent institution.

Should the Board consider the merits, the Petition fails to present any reasonable likelihood of success, as the grounds fail to teach or suggest limitations of each challenged independent claim. As one example, the claims recite an “electronic key” and “coded data” that enables functions of the electronic key for “unlocking and use” of a vehicle. During prosecution the inventors amended the claims to further recite that the coded data “includ[es] privilege settings set for additionally limiting types of use of the vehicle.” The Office found no art that teaches this claimed functionality. No asserted reference here teaches it either.

But the Board need not consider the merits and should exercise its discretion to deny institution under *Fintiv*. In the parallel district court proceedings, both Petitioners allege that the same primary references here invalidate the asserted claims. Yet Petitioners have declined to present a *Sotera* or any other stipulation. And the district court will resolve the issues long before the Board will issue a final

written decision, as demonstrated by both the scheduling order entered in the parallel matter and the time to trial statistics at the district court. Indeed, discovery will be near completion before the projected institution decision. Especially considering the substantial resources devoted by the district court—including an in-person hearing to discuss a flurry of technical motions and a claim construction hearing that will occur before the institution decision—the Board should decline to expend additional resources and risk inconsistent holdings.

Lastly, an IPR can only be instituted on “prior art consisting of patents or printed publications.” The Klevor reference of grounds 1 and 2 is neither. Thus, the Board cannot institute these grounds and, under the Supreme Court’s ruling in *SAS*, cannot institute on any ground.

II. The ’659 patent

U.S. Patent. No. 11,738,659 (EX1001, the “’659 patent”) was invented by brothers Angel and Albert Penilla and issued to their company, Patent Owner Emerging Automotive LLC, a family-owned automotive innovation company. EX1001, Face Page. The ’659 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, 1:65-2:2.

The '659 patent describes providing vehicle access to individuals, including an owner or “guest driver,” e.g., a friend, service person, or valet. *Id.* 10:28-39. This access can be provided by an electronic key, or eKey, which allows the holder of the eKey to use the vehicle. *Id.* 10:40-42. An eKey may be sent from a vehicle owner to another person, such as a guest. *Id.* 40-51. The eKey allows use of the vehicle, and can further include privileges for the user, including speed limits, geographic restrictions, amount of time, etc. *Id.* As an example, “the vehicle can be loaned to a child of driving age ... and the child can be provided with restricted use of the vehicle.” *Id.* at 14:51-53. The '659 patent describes creating profiles for users that have privileges set by an administrator. *Id.* at 17:5-13. For example, accounts for a driver may be created with “defined roles,” which can “include a set of privileges,” such as speed limit or geographic privileges. *Id.* at 38:52-62. In this way, logins of user profiles can be controlled. For example, “[a]dministrators can decide which settings are locked for specific logins or roles, which are open for the login user to toggle and which settings are to be enforced.” *Id.* at 17:18-26. Thus “use of the vehicle can be restricted to predefined rules.” *Id.* at 22:24-28.

A vehicle owner or administrator may initiate transfer of an eKey to a user's device, such as a smartphone. *Id.* at 42:17-30, 34:66-44:20. The eKey may provide access to the vehicle, but otherwise have a “set[] level of privileges for the vehicle

during the use of the electronic keys.” *Id.* Via the privileges, “specific vehicle aspects are enabled for the vehicle.” *Id.* at 42:38-40. The user can “then use the electronic Keys to use the vehicle in accordance with the privileges.” *Id.* at 43:17-19.

An owner of a vehicle can assign e-keys to “any number of users,” each having “various privilege settings,” allowing different users to have different privileges. *Id.* at 43:37-40; *see also id.* at 46:18-20 (“Each unique code can then be used to associate those e-keys with the same vehicle, but assigned to different devices/people with different privileges.”). As claimed, a vehicle includes “wireless communication circuitry” that is “configured to receive coded data from [a] mobile device” when the mobile device is “using an eKey.” *Id.* at claim 1. The “coded data enables functions of said eKey,” and “the coded data includes privilege settings.” *Id.*

A. File History of the ’659 patent

During prosecution, the Examiner issued a first Office Action rejecting the claims as anticipated by Zaid or obvious over Zaid in view of Mottla. EX1002, 178, 189. The inventors filed a response, amending independent claims to state the claimed coded data, which enables functions of the eKey, “includ[es] privilege settings set for additionally limiting types of use of the vehicle.” *Id.*, 333, 336. As the inventors explained, while the Zaid reference’s alleged coded data included a “message or time stamp to avoid repeat message attacks,” it did not disclose the

coded data including “privilege settings set for additionally limiting types of the vehicle.” *Id.*, 339.

The Examiner, agreeing that the references did not teach or suggest coded data including privilege settings, withdrew the Section 102 and 103 rejections, and identified a new reference, Shinada, as purportedly teaching those limitations. *Id.*, 344. The inventors, however, explained that Shinada likewise did not teach or suggest any “coded data [that] includ[es] privilege settings.” *Id.*, 511-512. While Shinada taught alleged restrictions, the inventors explained that the restrictions were “defined under the car rental contract,” and not included in the claimed coded data. *Id.*, 511. The Examiner agreed and issued a notice of allowance, citing the “coded data includes privilege settings” requirements as a reason for allowance. *See id.*, 521. Thus, while the Examiner alleged that prior art references taught both coded data and restrictions, he found that the art did not teach the claimed coded data to include privilege settings; he also thus necessarily found that the functionality was not obvious. *See id.* These claimed features are likewise missing from every ground of the Petition.

B. POSITA

Petitioners’ expert opined that a person of ordinary skill in the art “would have had at least a four-year undergraduate degree in electrical engineering, automotive

engineering, or a closely related field and at least two years of experience in the field of access control systems, vehicle electronics, and/or cryptography. Additional education could substitute for professional experience and vice versa.” EX1004, ¶ 85.

For purposes of this preliminary response, Patent Owner and its expert apply this definition, as the Petition fails under any reasonable definition of a POSITA. Malek Dec., ¶¶ 36-37.

C. Toyota’s recognition of importance of the ’659 patent.

Petitioner Toyota and its affiliates’ representations to the Office demonstrate the importance and novelty of the ’659 patent and the challenged claims. Years after the latest possible priority date of the ’659 patent, Toyota and its affiliates filed patent applications seeking to claim substantially similar subject matter as the ’659 patent.

For example, in 2020, Toyota filed an application that issued as U.S. Patent No. 11,295,564. Claim 1 of Toyota’s patent recites “key information” “for unlocking the vehicle.” EX2009, claim 1. It also discusses “permissions for a user of the vehicle to use a predetermined service using the vehicle” and “register[ing] the permission further in association with unique information corresponding to an owner user of the vehicle.” *Id.* In addition to the ’564 patent filed in the United

States, Toyota filed counterpart applications throughout the world including in South Korea, Europe, China, Japan, Brazil, Russia, and Singapore. EX2011. Toyota's later sought and similar claims demonstrate that Emerging Auto's technological disclosures in the '659 patent are cutting edge.

Similarly, in 2018 Tokai Rika, a Toyota affiliate, filed an application that issued as U.S. Patent No. 10,493,953. This patent claims "an electronic key system" which uses an "ID verification" and, based thereon, determining whether to "permit actuation of a smart function." EX2012, claim 1.

Yet again, a Toyota company filed an application in 2018 that issued as U.S. Patent No. 10,614,644. Similar to the '659 patent, claim 1 of Toyota's later-filed '644 patent recites "key information" for "unlocking the vehicle" and "starting the vehicle." EX2013, claim 1. The claims further recite "permission for a user of the vehicle to use a predetermined service suing the vehicle." *Id.*

Toyota in 2017 filed an application that issued as U.S. Patent 11,094,149. Claim 1 of the '149 patent recites "a transmitter configured to transmit ... [a] signal requesting the locking or unlocking" of a vehicle, including "authentication information being uniquely matched with the key unit," to provide reservation information. EX2014, claim 1.

Petitioners’ attempt to cast the features, functionality, and types of systems of the ’659 patent as “prolific” by 2013 (Pet., 1), is belied by Petitioner Toyota and its affiliates’ attempts to claim patent protection for similar features, functionality, and systems years later. Through these later-filed applications, Toyota and its affiliates demonstrated an implicit belief that the earlier-filed inventions of the ’659 patent were novel technology at the time.

III. Should the Board reach the merits, institution should be denied because Petitioners have failed to demonstrate any reasonable likelihood of success for any challenged claim.

As Petitioners fail to present any reasonable likelihood of success for any ground, the Petition should be denied. Petitioners assert two sets of grounds, one set based on Kleve / Hatton, and the other on Mikan. Pet., 2. Neither set of grounds discloses or suggests limitations of the independent claims, including the “coded data [that] includes privilege settings” limitations that were added during prosecution. To account for the failures of the references, Petitioners are forced to rely on obviousness theories supported only by conclusory expert testimony. But a POSITA would not have modified the references based on hindsight as Petitioners suggest: the modifications would not have made sense in the context of the references. Regardless, both sets of grounds fail to present any reasonable likelihood of success.

A. Grounds 1-2 (Kleve / Hatton) do not present any reasonable likelihood of success.

Grounds 1 and 2 are premised on the Kleve and Hatton references. Pet., 2. These grounds fail for numerous reasons. Indeed, neither Kleve nor Hatton teach or suggest the “coded data [that] includes privilege settings” limitations of the independent claims that were added during prosecution. Malek Dec., ¶¶ 54-62. Petitioners also fail to demonstrate that the proposed combination teaches the memory as claimed in the independent claims. *Id.*, ¶¶ 63-64. And even if Kleve and Hatton did teach or suggest these claim limitations, a POSITA would have recognized that it would not have made sense to combine the two references as Petitioners propose in their hindsight-based analysis. *Id.*, ¶¶ 65-71.

1. Brief summary of Kleve

Kleve, EX1005, is directed to a rental car system. Much like the prior art distinguished during prosecution, Kleve does not teach or suggest the claimed coded data including any privilege settings. In Kleve, a vehicle owner creates a profile via a car rental website, offering the owner’s car for rent on the platform. EX1005, ¶ 37. As part of the listing, the Owner creates rental agreement forms that must be agreed to before rental. *Id.*, ¶ 38. For example, there may be a standard form, and the Owner may also create custom forms in the event a vehicle renter wants to use the vehicle for a certain purpose. *Id.*

Vehicle renters (referred to as “Temporary Users”) also set up a profile on the platform and provide “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.” *Id.*

A Temporary User may browse and rent vehicles. A Temporary User may select a vehicle, pay the rental fee and sign the appropriate rental agreement form. *Id.*, ¶ 39. After paying a fee and signing the form, Kleve’s system provides “a virtual key” to the Temporary User. *Id.*, ¶ 39. The virtual key is the Temporary User identification that the user provided to the rental platform. *Id.*, ¶ 63.

Afterward, when the rental period begins, when a “Temporary User arrives at the vehicle within the scheduled rental time, he or she may enter the virtual key using several methods” such as “scan[ning] their finger with the use of a fingerprint scanner.” *Id.*, ¶ 69. The virtual key (e.g., a fingerprint) is authorized before access is granted. *Id.*, ¶ 70. For example, the vehicle may include a fingerprint reader, voice recognition, barcode reader, password input, etc. *Id.*, ¶¶ 63-65.

“The Temporary User’s virtual key may be authorized several ways including, but not limited to, at the vehicle, communicated back to the vehicle rental authorization server using a telecommunications network, or by having the vehicle

Owner verify access using their nomadic device.” *Id.*, ¶¶ 70-71:

[0070] At step 622, when the Temporary User arrives at the vehicle within the scheduled rental time, he or she may enter the virtual key using several methods. One method may include having the Temporary User scan their finger with the use of a fingerprint scanner integrated with the VCS to validate authorization to access the vehicle. The Temporary User's virtual key may be authorized several ways including, but not limited to, at the vehicle, communicated back to the vehicle rental authorization server using a telecommunications network, or by having the vehicle Owner verify access using their nomadic device.

[0071] At step 618, the Temporary User may send the virtual key to the server requesting access to the vehicle, or use a vehicle input device, like camera, microphone, fingerprint scanner or retinal scanner integrated with the VCS to capture his identity and/or payment credentials to enable a keyless drive-away. If it is the scheduled time for the rental, the vehicle may compare the identity credentials just inputted at the vehicle and the one previously sent virtual key to the vehicle from the vehicle Owner to determine authorization. If the

comparison is successful, the vehicle may enable drive-away access to that Temporary User

After verifying the Temporary User and determining his or her identity, the Owner may wish to set restrictions during the rental based on the Temporary User.

Id., ¶ 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.

In these circumstances any “restrictions assigned by the vehicle owner at the start of the rental period ... [are] download loaded to the [vehicle’s] VCS.” *Id.* 75:

[0075] In the illustrative embodiment as shown in FIG. 7 is an overview of a vehicle rental micro-business monitoring process integrated with a VCS. At step 702, the VCS may begin monitoring and report usage of the vehicle to the owner. The system may wait for the rental period to start at step 704. 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. The performance limitations and restrictions downloaded to the VCS may include, but not limited to: setting a top vehicle speed, limiting the cargo load, and alerting the vehicle owner if the driver enters an area deemed to be prohibited by the owner.

The vehicle may be monitored regarding the restrictions and can be disabled if restrictions are exceeded. *Id.*, ¶¶ 41-42.

2. Brief summary of Hatton

Petitioners and their expert provide little discussion of Hatton (EX1008). *See* Pet., 11-12; EX1004, ¶ 105. Petitioners note that Hatton teaches “encrypted data,” and, without considering the reference, argue that it would have been obvious to dynamically and regularly encrypt various aspects of any car system for confidentiality. Pet., 11-13. However, as discussed in Section III.A.5, below, that is incorrect. As Dr. Malek explains, Hatton teaches a vehicle that includes encrypted data during the manufacturing process. EX2001, ¶¶ 47-48. When a user attempts to use the vehicle, e.g., via a fob, the fob sends a “security code” to the vehicle, which the vehicle checks using a “lookup table” for authentication. EX1008, 9:50-63. The purpose of this check is to authenticate the fob, not to preserve confidentiality of the

data. Malek Dec., ¶ 48.

Hatton generally teaches providing the information in a fob to a mobile device so that the mobile device can then act as a fob (e.g., by sending security codes and commands to the vehicle). *Id.*, Abstract; *see also id.*, 14:49-15:36.

3. The proposed combination of Kleve and Hatton fails to teach or suggest the “coded data includes privilege settings” limitations.

The Petition fails to demonstrate any reasonable likelihood of success, as Petitioners’ alleged “coded data” in the proposed Kleve / Hatton combination does not include any alleged “privilege settings,” as required by each challenged claim:

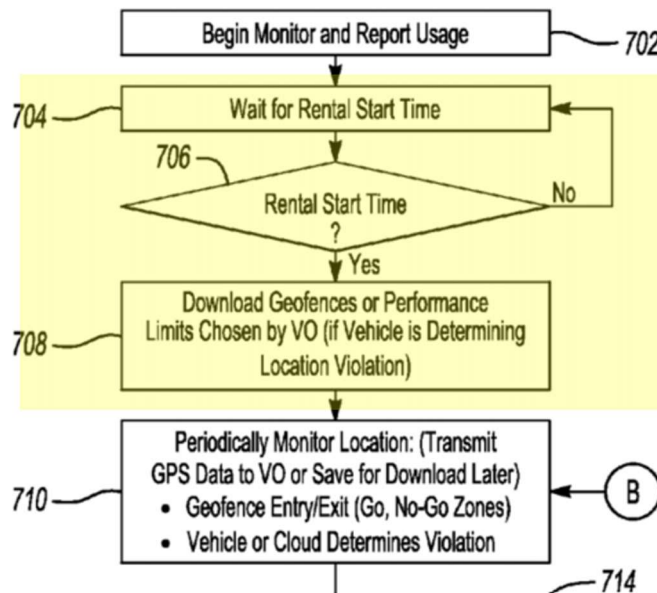
- “the coded data includes privilege settings associated with the eKey for limiting types of use of the vehicle” Claim 1[e];
- “the coded data includes privilege settings set for limiting types of use of the vehicle when using the vehicle” Claim 11[e]; and
- “the coded data includes privilege settings for use of the vehicle when using the eKey” Claim 18[e].

For each of these limitations, Petitioners allege that Kleve’s “virtual key, represented as encrypted data, includes privilege settings that limit types of use of the vehicle.” Pet., 20-21, 28, 35. Petitioners next allege that Kleve discloses “restrictions,” such as “speed, global position coordinates, or load weight

restrictions.” *Id.* The problem with Petitioners’ theory is that Petitioners did not show—and could not have shown—that Kleve’s “restrictions” are included in Kleve’s “virtual key.” Pet., 20-21; *see also* Malek Dec., ¶¶ 55-62.

Nowhere does Kleve teach or suggest that its “virtual key”—the alleged “coded data”—includes any of the “restrictions”—the alleged “privilege settings.” For the “coded data” requirement, Petitioners rely on Kleve’s “virtual key,” as the alleged “coded data.” Pet., 19. Petitioners then rely on Kleve’s “restrictions,” as the alleged “privilege settings,” citing to Kleve at paragraphs 40, 83, and 76. Pet., 20-21. However, none of these paragraphs make any mention of a “virtual key.” *See* EX1005, ¶¶ 40, 83, 76. While Petitioners cite to their expert (Pet., 20), Petitioners’ expert likewise offers not citation or explanation to show that Kleve teaches that its “virtual key” includes any “restrictions.” *See* Malek Dec., ¶ 56.

In fact, Kleve’s “virtual key” is provided before rental time, and Kleve is clear any “restrictions” are not applied provided until the rental period has begun. EX1005, ¶¶ 75 (after “the system detects a rental time start ... [t]he system may begin to download ... restrictions.”), 40 (Owner may set “restrictions for “vehicle being rented.”); *see also id.*, Fig. 7:



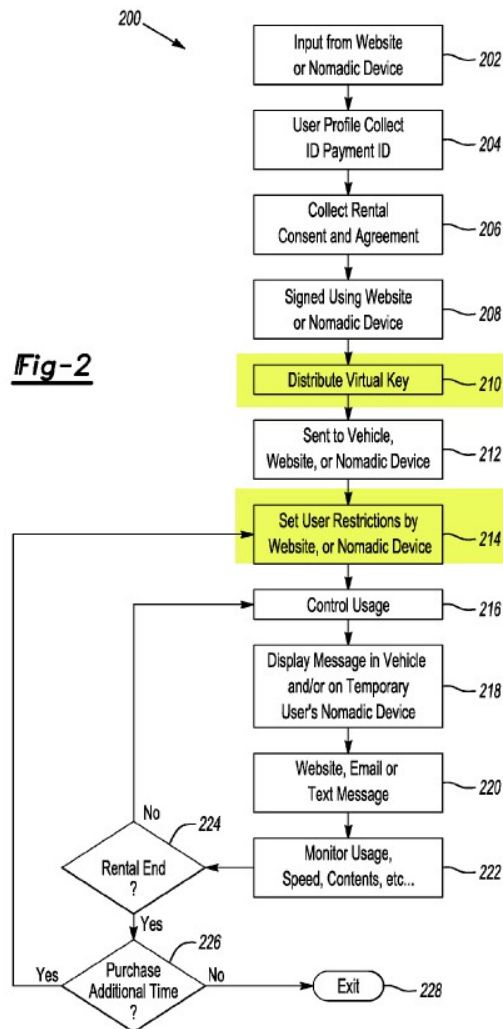
A POSITA would have understood that Kleve does not teach downloading any “restrictions” until rental time because in Kleve, “Temporary Users are not authenticated until they attempt to access the rental vehicle at rental time, which then allows the Owner to determine whether restrictions should be set for the authenticated Temporary User.” Malek Dec., ¶ 55 (discussing EX1005, ¶¶ 40, 70-71, 75).

While Petitioners make no argument that Hatton discloses any “privilege settings,” Petitioners rely on Hatton as suggesting modifying Kleve’s “virtual key” so that it is encrypted. *See* Pet., 12-14, 20-10. Petitioners do not rely on Hatton as disclosing or suggesting modifying the content of Kleve’s “virtual key” to include “privilege settings,” as Hatton does not teach including “privilege settings” in any

coded data; indeed, Petitioners do not allege that Hatton teaches any “privilege settings” at all. As such, neither reference, or their combination, teaches or suggests the alleged “coded data” including any alleged “privilege settings”: Kleve’s “virtual key” does not include any “privilege settings,” and encrypting that key in view of Hatton would not result in the content of the “virtual key” including privilege settings. EX2001, ¶¶ 55-59. As the proposed combination fails to teach or suggest the alleged “coded data” including any alleged “privilege settings,” the combination fails.

As Petitioners fail to demonstrate that the alleged “coded data includes” the alleged “privilege settings,” grounds 1-2 fail. Petitioners did not attempt to demonstrate this claimed functionality because Kleve teaches that its “restrictions” are *not* included in its virtual key. Malek Dec., ¶ 57. Nor would it have been obvious. As Dr. Malek demonstrates, “[a] POSITA would understand that Kleve teaches to ‘set user restrictions’ after the virtual key is distributed and after the step in which the virtual key is ‘sent to vehicle, website or nomadic device.’” *Id.* (citing EX1005, Fig. 2, ¶¶ 39-40). Therefore no “restrictions”—set after the virtual key was made and distributed—could be included in the key. Malek Dec., ¶ 57. Kleve discloses that only “[a]t step 214 [that] 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.” EX1005, ¶ 40. Kleve discloses that this step, step 214, occurs after the virtual key is distributed, in step 210:



EX1005, Fig. 2; *see also id.*, ¶¶ 39-40 (“Owner may set user restrictions” for “the vehicle **being** rented.”). Indeed, while a Temporary user may “intitiate[] the rental event” before the rental period, the system waits until “rental time start” to “begin to download ... restrictions assigned by the vehicle owner at the start of the rental period.” *Id.*, ¶ 75.

Therefore, not only does Kleve not disclose the restrictions being included in the “virtual key,” a POSITA would have understood that they could not have been. Malek Dec., ¶ 57.

Kleve does not disclose including the “restrictions” in the virtual key, which is sent to the device of a Temporary User (a user who temporarily rents a vehicle). Indeed, Kleve discloses that information for the reservation is sent from a server to the vehicle, at the direction of a vehicle owner. Malek Dec., ¶ 60 (citing EX1005, ¶ 39, 62, 66, 75). Kleve specifically discloses that the system “download[s] ... restrictions assigned by the vehicle owner at the start of the rental period ... *to the VCS*” and thus not providing any privileges via the alleged “coded data.” EX1005, ¶ 75 (emphasis added); Malek Dec., ¶ 60. Hatton likewise does not teach including privilege settings in a “virtual key,” and Petitioners offer no argument to the contrary. Pet., 20-21. In fact, Petitioners do not allege that Hatton discloses or suggests any alleged “privilege settings” at all. Pet., 11-12, 20-21.

Recognizing the failure of both references, Petitioners state in one sentence that it “would have been obvious to a POSITA to include the use restrictions within the encrypted data associated with the virtual key in order to prevent tampering by a temporary user,” citing to the “motivation to combine” section. Pet., 21. But that section relies on Hatton as encrypting data and discusses the alleged benefits of

encrypting data in Kleve’s system, including the “virtual key.” Pet., 12-14 (e.g., “[t]here were well-known benefits of using encrypted data for wireless communications”). Even if true, this argument provides no basis for why the “restrictions” would be included in the “virtual key” to begin with. Malek Dec., ¶¶ 61-62.

While neither Hatton nor Kleve teach including restrictions in a virtual key, and Petitioners do not provide any argument why that hindsight modification to the references would have been obvious, Petitioners’ explanation demonstrates why a POSITA would not have found it obvious to modify Kleve (or Kleve and Hatton) as proposed. Petitioners argue that including restrictions “within the encrypted data associated with the virtual key” would “prevent tampering by a temporary user.” Pet., 21. But providing the information within the virtual key—which is distributed to the temporary user’s device—would only provide an opportunity for the temporary user to do just that. Malek Dec., ¶ 61. Kleve already avoids Petitioners’ prevented problem by not providing the “restrictions” to the temporary user and instead downloading them to the vehicle without using the Temporary User’s virtual key as an intermediary. *Id.*

As the restrictions in Kleve are not provided to the Temporary User’s device, the Temporary User would not have an opportunity to “tamper” with the restrictions.

Id. In fact, Petitioners’ proposed modification, supported by neither reference, would inject a vulnerability by providing the restrictions to the user’s device, which could lead to tampering. *Id.* Thus, Petitioners’ theory demonstrates why a POSITA would not have modified Kleve as proposed—as it would lead to a less efficient and less secure system. *Id.* Moreover, if a POSITA would have wanted any benefits from encrypting data, as allegedly taught by Hatton, the POSITA could have just encrypted the data stored and/or communicated in Kleve, without otherwise modifying the system in ways that have no demonstrated benefits and, in fact, introduce vulnerabilities to the system. *Id.*

4. The proposed combination of Kleve and Hatton fails to teach or suggest that the alleged “memory” has “program instructions for instructing/controlling unlocking and starting of the vehicle.”

Each independent claim of the ’659 patent requires memory having a particular type of program instructions:

- “memory ... having program instructions for instructing unlocking and starting of the vehicle” Claim 1[a];
- “memory ... having program instructions for controlling unlocking and starting of the vehicle” Claim 11[a]; and
- “memory ... having program instructions for controlling unlocking and starting of the vehicle” Claim 18[a].

Petitioners fail to demonstrate that their proposed combination teaches or suggests any memory having any of these claimed program instructions. Malek Dec., ¶ 64. For each of these limitations, Petitioners rely on a particular memory in Kleve, HDD and RAM, and that Kleve’s processor enables a rental transaction by activating the vehicle to enable keyless drive away. Pet., 16. As an initial matter, Petitioners do not identify any alleged instructions as being in the previously-identified memory. Moreover, as Dr. Malek explains, “a POSITA would understand that merely ‘activating’ a vehicle is not ‘instructions for unlocking and starting the vehicle’ or ‘instructions for controlling unlocking and starting of the vehicle.’” Malek Dec., ¶ 64. A POSITA would understand “activating” a vehicle to mean making the vehicle operative (e.g., such as setting a flag to indicate that a particular rental agreement is in effect). *Id.* As Kleve explains, a vehicle is active “during a prescribed *rental* period.” EX1005, Abstract (emphasis added). The vehicle is not “started” during the entire rental period or continuously being started. A POSITA would thus not understand instructions to “activate” a vehicle to be instructions for starting and unlocking of the vehicle. *Id.* Petitioners also note that Kleve discloses “to unlock and drive,” but fail to identify any instructions in the identified alleged memory that does this.

5. It would not have been obvious to combine Kleve and Hatton as Petitioners propose.

Even assuming the proposed Kleve / Hatton combination taught or suggested the elements of the independent claims (it does not), it would nevertheless not have been obvious to a POSITA to modify Kleve in view of Hatton as Petitioners propose. Malek Dec., ¶¶ 66-71. In a short summary of Hatton, Petitioners generally argue that the reference discloses communicating with “encrypted data” and generating an alleged “electronic key” using “encrypted data.” Pet., 11-12. Petitioners then broadly argue that it would have been obvious to use “encrypted data for wireless communications,” to provide various benefits. Pet., 12-14. However, the purported benefits that Petitioners and their expert describe are a result of encryption for *confidentiality*, which is not taught by Hatton. Malek Dec., ¶ 67. Hatton instead teaches using encryption for *authentication*. *Id.*, ¶¶ 67-68.

“[A]uthentication is the process of verifying the identity of an entity before granting access to a resource, while confidentiality is a distinct concept involving the protection of information from unauthorized access or disclosure.” *Id.*, ¶ 68. Hatton’s encryption is related to the latter. *Id.* Hatton discloses a vehicle having entry passive start (PEPS) and passive anti-theft security (PATs) controllers, which include certain encrypted data. EX1008, 5:54-7:60, 9:4-17, 9:50-63. Hatton discloses that encrypted data sent from the key/mobile device is checked against the

encrypted data in a PEPS by using a look up table that is stored on the vehicle computing system (VCS). EX1008, 9:50-63. This check authenticates that the key/mobile device is authorized to access the vehicle. Malek Dec., ¶ 68. Hatton’s “encryption” is unrelated to confidentiality and, as Kleve already teaches authentication, a POSITA would not have been motivated to modify Kleve in view of Hatton to add authentication. *Id.*¹ Thus, Petitioners’ argument that “[t]here were well-known benefits of using encrypted data for wireless communications” provides no reason why a POSITA would have combined Kleve and Hatton as proposed. *Id.* And as Hatton’s encryption is not for confidentiality, Petitioners are incorrect that it would prevent unauthorized users from “view[ing] the contents of the messages,” as the “content” is what is sent and checked. *See* Pet., 12.

Moreover, Petitioners do not explain how Kleve could be modified in view of Hatton as proposed. Hatton does not disclose generating any encrypted data at a

¹ As discussed above, Kleve teaches receiving the “virtual key” at the vehicle and providing it to the “rental authorization server” or vehicle Owner for authentication, e.g., by checking the credentials such as a fingerprint. EX1005, ¶ 70. Indeed, during prosecution, Kleve attempted to distinguish art using its “authenticating input [for] identifying a user.” EX2020.

mobile device. Malek Dec., ¶ 69. Hatton discloses that encrypted data is assigned to a vehicle at the manufacturing process. EX1008, 8:24-36, 14:7-18. Thus, it would not have been obvious in view of Hatton to generate encrypted data to include restrictions for use in a rental vehicle because the encrypted data would have already been generated. *Id.* Under Petitioners’ theory, encrypted data would need to be generated each time “restrictions” were created or modified, but Hatton does not have a mechanism for doing this. *Id.*

Petitioners further state that encrypting the data would “simplify[] and facilitate[] use of the virtual key for end users,” but they provide no reason what this means or why it would be. In fact, it would not. Malek Dec., ¶ 70. Petitioners also state that encrypting data would allow key usage “when the vehicle and mobile device cannot connect to a remote server.” Pet., 13. However, the Petition provides no explanation or cite for this proposition. As discussed above in Section III.A.2, Kleve’s vehicle communicates with the server to verify virtual keys, and merely including “restrictions” in the virtual keys and encrypting them would not solve this (*see id.*), and Petitioners offer no reason or citation to the contrary. Petitioners’ expert offers conclusory reasons for the benefits of the proposed combination, but, as Dr. Malek explains, a POSITA would not have found any of those purported benefits to lead to fruition. *Id.* Instead, a POSITA would have understood that the

proposed combination would have resulted in a slower, less efficient system with a poorer user experience—all with no (correctly) identified benefits. Malek Dec., ¶¶ 67-71.

6. The Sekiyama references does not cure the deficiencies of Kleve/Hatton.

Petitioner adds the Sekiyama reference for ground 3, which challenges dependent claim 2. Sekiyama does not cure any of the deficiencies of the proposed Kleve / Hatton combination discussed above, and Petitioners make no argument to the contrary. *See* Pet., 38.

B. Grounds 3-6 (Mikan) - do not present any reasonable likelihood of success.

Petitioners’ second set of grounds, 3-6, attempt to rely on the Mikan reference. While Petitioners allege that Mikan is a 102 reference, they all but concede that it also fails to suggest the “coded data includes privilege settings” limitations added during prosecution. Pet., 44-45. Petitioners identify no “coded data” that “includes privilege settings” in Mikan, and instead revert to an obviousness theory premised on functionality that is not disclosed in any reference, and nevertheless makes no sense. Malek Dec., ¶¶ 77-81. Both sets of grounds fail.

1. Brief summary of Mikan

Mikan (EX1007) is related to a vehicle having a “local database.” EX1007, ¶ 54. The vehicle’s local database includes “a vehicle operation policy” for the vehicle.

Id., ¶ 57. The vehicle operation policy may “indicate to enable, partially enable, or disable a vehicle operation feature.” *Id.*, ¶ 5. Mikan is related to syncing the vehicle’s local database with an external “master database.” *Id.*, ¶ 54. To do so, the master database communicates with the local database so that the local database may “mirror” data in the master database for the vehicle and ensure that the data is consistent. “For example, local database 203 may regularly poll master database 208 to maintain consistent data. In one embodiment, each of local database 203 and master database 208 may communicate an update to the other after a record change.” *Id.*, ¶ 54.

51. When “a user attempt[s] to access or operate [the] vehicle ..., the vehicle retrieves a vehicle operation policy by “querying [the] local database.” *Id.*, ¶¶ 71-72.

2. Mikan fails to teach or suggest that the alleged “coded data includes privilege settings.”

As with the proposed combination of Hatton and Kleve, Mikan fails to teach or suggest any “coded data” that “includes privilege settings,” as required by each independent claim. The claims require (1) that the “coded data” include privilege settings and (2) that the “coded data” is “from the mobile device.” Mikan teaches neither, as the alleged “coded data” does not include any alleged privilege settings and, regardless, no alleged privilege settings are provided, as included in coded data,

“from the mobile device.” Malek Dec., ¶¶ 76-77. While Petitioners argue that Mikan is a Section 102 reference, they cannot proffer any argument or explanation for this claimed functionality. Pet., 44-45. Instead, Petitioners argue that “it would have been obvious.” *Id.* It would not have been, and Petitioners’ hindsight driven excuse for modifying Mikan would not have (and does not) make any sense from the viewpoint of a POSITA. Malek Dec., ¶¶ 76-80.

Petitioners argue that Mikan discloses that when a user attempts to use a vehicle, the vehicle transmits a “secure identifier [that] comprises coded data” such as a “digital signature”. Pet., 44. Petitioners then posit that the alleged “privilege settings” is disclosed by Mikan’s “vehicle operation policies.” Pet., 44-45. However, Mikan does not disclose any “digital signature” that includes any “vehicle operation policies” or any “vehicle operation policies” being “from the mobile device.” Malek Dec., ¶¶ 76-77. Petitioners make no real argument to the contrary. Pet., 44-45.

The Mikan reference involves syncing two databases, a “local database 203” that is “resident within [a] vehicle” and a “master database 208” that is remote from the vehicle. EX1007, ¶¶ 51, 54. The “master database” of Mikan “communicate[s] with [the] local database” for synchronization of the vehicle operation policy for the vehicle of the local database. *Id.* ¶ 54. “For example, local database 203 may regularly poll master database 208 to maintain consistent data.” *Id.* Both databases

include a vehicle ID, a key set for the vehicle, and vehicle operation policies for the vehicle. *Id.*, ¶¶ 58-59. If the master database is updated, the local database synchronizes with the master database. *Id.*, ¶ 69. For example, the “[c]ontrol unit 202 [of the vehicle] or local database 203 may initiate the synchronization to pull updated data from master database 208” or the master database may push data to the vehicle. *Id.* “The synchronization may be a partial or complete refresh of the data.” *Id.* When a user accesses a vehicle, e.g., using a “metal key,” a vehicle operation policy is retrieved by “querying local database 203” of the vehicle. *Id.*, ¶¶ 70, 72. As Dr. Malek explains, a POSITA would have understood that the alleged “privilege settings,” a vehicle operation policy, is not included in any digital signature “from the mobile device” for accessing the vehicle. Malek Dec., ¶ 77. A POSITA would have understood that Mikan’s “vehicle policies” are provided to the vehicle by synchronization with the master database. *Id.* Mikan thus does not disclose or suggest these limitations, and Petitioners offer no real analysis to the contrary.

Instead, Petitioners incorrectly argue, in three sentences, that “[i]t would have been obvious to a POSITA to transmit the vehicle operation policy as additional coded data along with Mikan’s secure identifier.” Pet., 45. Petitioners argue that under its modification, whenever a user attempts to access the car, there would be a transfer of vehicle policies as part of the information for vehicle access. But this

makes no sense. Malek Dec., ¶¶ 78-80. Indeed, the only “benefit” Petitioners conjured for this vast departure from Mikan was that it would “prevent a secondary user from tampering with the use restrictions,” which are assumably Mikan’s “vehicle operation policies.” Pet., 45. However, this is the exact opposite of what the proposed modification would have done. Malek Dec., ¶ 78. By providing “operation policies” to a user’s device to later be transferred to a vehicle, the device user would have an opportunity to tamper with the data on his or her device. *Id.* However, by communicating between the master and local databases without using the user’s device as an intermediary (the functionality that Mikan discloses), the user would not have any opportunity for “tampering.” *Id.* Thus, Petitioners provide no good reason why a POSITA would have modified Mikan as proposed.

Indeed, there is no good reason. If a POSITA sought any benefits of encrypted transmissions, the POSITA would have understood to simply encrypt the transmissions between the local and master databases. Malek Dec., ¶ 79. There would be no need to recreate Mikan’s system to a less secure, less efficient method just to encrypt data. *Id.* A POSITA would have recognized that Mikan’s mobile phone was not required if a POSITA wished to send encrypted information; information from the master database could have been encrypted and communicated. *Id.* As with the proposed Kleve / Hatton combination of grounds 1-2, any benefits

of encrypting information would not support a wholesale change to the system—a POSITA would have just encrypted the information and communications of the disclosed systems.

Not only is there no reason to modify Mikan as proposed, a POSITA would have been highly discouraged from modifying Mikan to have the mobile device send vehicle operation policies to the vehicle. Malek Dec., ¶ 80. Mikan discloses that the local database may “regularly poll master database to maintain consistent data” or that the master database communicates an update to the local database after a record change. EX1007, ¶ 54. Thus, a POSITA would have understood Mikan to place “emphasis on keeping timely and accurate data in the local database.” *Id.* By providing database updates via a mobile device, instead of communication between the two databases, there could not have been any consistent polling or timely updates—instead, data could only be sent in the event the mobile device was in contact with the car—all in a less efficient, less secure manner. *Id.*

A POSITA would also have recognized that sending the vehicle operation policies from the server to the vehicle through an intermediary (i.e., mobile phone) would be inefficient, for multiple reasons. First, adding a phone as an intermediary in the communication between vehicle and server would “slow down the exchange of vehicle operation policies because the policies would need to hop over an

additional device in the network before reaching their destination.” Malek Dec., ¶ 81. Additionally, the entire vehicle operation policies would need to be sent to the vehicle when an alleged electronic key is used to lock, unlock, or start the vehicle. The vehicle operation policies would not change that frequency, resulting in unnecessary transmission of policies to the vehicle. *Id.* This would be contrary to Mikan’s disclosures, which emphasize the importance of minimizing bandwidth usage through selective synchronization of updated/relevant data between local and master database. *Id.*; EX1007, ¶ 69. A POSITA would have recognized that Mikan’s system as disclosed—synchronization of local database with master database—is more efficient than the hindsight modified version of Mikan proposed by Petitioners. Malek Dec., ¶ 81. Under the disclosures of Mikan, vehicle operation policies would be sent when they are changed or determined to be relevant, not arbitrarily as users attempt to access vehicles. Mikan fails to teach or suggest this claimed functionality and Petitioners’ conclusory, unsupported modifications do not cure Mikan’s deficiencies.

3. Petitioners’ secondary references do not cure Mikan’s deficiencies.

For grounds 4-6, Petitioners propose to combine Mikan with various secondary references. However, none of those references cure the deficiencies of Mikan discussed above, and Petitioners offer no argument to the contrary. While

Petitioners add Xiao for ground 4, they make no argument that Xiao cures Mikan's failures for independent claim 1. While Petitioners attempt to attack independent claims 11 and 18 in ground 4, they do not allege that Xiao cures Mikan's deficiencies discussed above with respect to claim elements 11[e] and 18[e]. Pet., 57, 62. While Petitioners attempt to add references for grounds 5 and 6, those references do not cure any deficiencies with respect to the independent claims, and Petitioners offer no argument to the contrary. The Mikan-based grounds, 3-6, present no reasonable likelihood of success. As with grounds 1-2, they fail. The Petition should be denied.

IV. The Board Should Deny Institution Under *Fintiv*.

The Board should exercise its discretion to deny institution under § 314(a).

To do so, the Board balances six factors:

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
2. proximity of the court's trial date to the Board's projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the Petition and in the parallel proceeding;
5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
6. other circumstances that impact the Board's exercise of discretion, including the merits.

Apple Inc. v. Fintiv, Inc., IPR2020-00019, Paper 11 at 5-6 (P.T.A.B. Mar. 20, 2020).

“These factors relate to whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding.” *Id.* In evaluating these factors, the Board takes “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review.” *Id.*

In addition, the USPTO Director issued an “Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation” (“Interim *Fintiv* Procedure”) dated June 21, 2022, which is addressed below.

A balance of the *Fintiv* factors—in view of the Interim *Fintiv* Procedure—warrants denial of institution.

A. The Board need not address the merits of the Petition because the factors favor denial

1. Factor 1 Favors Denial (Likelihood of Stay)

Factor 1—which considers whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted—favors denial of institution. There is no evidence that a court would enter a stay. All evidence points to the contrary.

Emerging Auto filed the parallel district court proceedings on September 20, 2023, which were assigned to Judge Rodney Gilstrap. EX2007; EX2008. Judge Gilstrap has since consolidated the proceeding against Toyota with the proceeding against Kia Corporation. EX2007. Petitioners have not filed any motion to stay in the district court case. *Id.* Even if they were to request a stay pending the outcome of this IPR proceeding, there is no evidence that the court would grant a stay and, indeed, it almost certainly would not. Courts in the Eastern District of Texas, and Judge Gilstrap in particular, disfavor, and as a general rule, deny motions to stay pending IPRs. *See Scorpcast, LLC v. Boutique Media*, No. 2:20-cv-00193-JRG-RSP, 2021 WL 3514751, at *1 (E.D. Tex. June 8, 2021) (Judge Gilstrap reciting bases for denial of earlier motion to stay: “On October 27, 2020, the Defendants filed [their] original motion to stay pending resolution of the IPR. At the time the Defendants filed their original stay motion, the parties had served infringement and invalidity contentions, started the discovery process, and begun preparing for the claim construction hearing. The Court denied that motion.”) (internal citations omitted); *see also e.g., Force Mos Tech., Co. v. ASUSTek Comput., Inc.*, No. 2:22-CV-00469-JRG, 2024 WL 1586266 (E.D. Tex. Apr. 11, 2024) (Judge Gilstrap); *Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson*, No. 2:21-CV-00113-JRG, 2022 WL 17484264 (E.D. Tex. July 7, 2022) (Judge Gilstrap); *St. Lawrence*

Commc'ns LLC v. ZTE Corp., No. 2:15-CV-349-JRG, 2017 WL 3396399 (E.D. Tex. Jan. 17, 2017) (Judge Gilstrap).

The stay is even less likely here, given the significant case progression (discussed in factor 3) and the scheduled jury trial preceding well before the projected final written decision date (discussed in factor 2). The first *Fintiv* factor supports denying institution. *See, e.g., Mylan Labs. Ltd. v. Janssen Pharmaceutica NV*, IPR2020-00440, Paper 17 at 13-14 (P.T.A.B. Sept. 16, 2020) (“We consequently conclude that the balance of facts in the two litigations indicate that no stay is likely to be entered in either, and therefore *Fintiv* factor 1 leans towards denial of institution.”).

2. Factor 2 Favors Denial (Timing of Trial); Trial will conclude at least six months before any final written decision

Fintiv factor 2 weighs in favor of denying institution because the district court is set to complete trial nearly six months before any final decision from the Board would be due.. The jury trial in the Eastern District of Texas litigation is set to commence on July 21, 2025 (EX1024), whereas the Board’s final written decision would be due over six months later on approximately January 30, 2026. “If the court’s trial date is earlier than the projected statutory deadline, the Board

generally has weighed this fact in favor of exercising authority to deny institution under NHK.” *Fintiv*, IPR2020-00019, Paper 11 at 9.

This timeline favors denial, as the Board has previously found that when “a jury trial is scheduled to occur in the related district court litigation approximately four months prior to when a final written decision would be statutorily due,” “these facts weigh in favor of exercising discretion to deny institution.” *Immersion Sys. LLC v. Midas Green Techs., LLC*, PGR2021-00104, Paper 15 at 11 (P.T.A.B. Jan. 31, 2022). Indeed, the Board has repeatedly found that even a one-to two-month period between the trial date and the projected date of a final written decision favors denial. *See, e.g., NXP USA, Inc. v. Impinj, Inc.*, PGR2022-00005, Paper 18 at 8-9 (P.T.A.B. May 2, 2022) (finding two-month period between trial date and deadline for final decision weighed in favor of discretionary denial); *E-One, Inc. v. Oshkosh Corp.*, IPR2019-00161, Paper 16 at 6-9 (P.T.A.B. May 15, 2019) (finding one-month period between trial date and deadline for final written decision weighed in favor of discretionary denial); *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 12-13 (P.T.A.B. May 13, 2020) (factor disfavors institution when “the currently scheduled District Court trial is scheduled to begin two months before our deadline to reach a final decision”); *eClinicalWorks, LLC v. Decapolis LLC*, IPR2022-00229, Paper 10 at 9 (P.T.A.B. Apr. 13, 2022) (determining denial favored where

beginning of jury trial was “roughly one to two months” before final decision was due); *Netflix, Inc. v. Uniloc 2017 LLC*, IPR2020-00008, Paper 13 at 9 (P.T.A.B. Apr. 13, 2020) (finding two-month period between scheduled trial date and deadline for final written decision favored denial).

Additionally, the USPTO’s Interim *Fintiv* Procedure provides that the “[p]arties may present evidence regarding the most recent statistics on median time-to-trial for civil actions in the district court in which the parallel litigation resides for the PTAB’s consideration ... the PTAB will also consider additional supporting factors, such as the speed and availability of other case dispositions. *See* Interim *Fintiv* Procedure, 8-9. Here, the median time-to-trial is 21.1 months and the median time from filing to case disposition in the Eastern District of Texas is 7.8 months. EX2006, Judicial Caseload Profile, Table T-3 at 2, Table C-5 at 2 (June 2024). These statistics evidence trial will occur many months before a final written decision, at a minimum. For Judge Gilstrap in particular, the trial would be between ten to twelve months prior to the final written decision deadline, in February or April 2025 (EX2016) (showing 20-month average time-to-trial, excluding transfers, and median time-to-trial of 18 months).

Judge Gilstrap has already set the jury trial, and that jury trial will conclude well before the Board's projected statutory deadline. EX1024. Thus, *Fintiv* factor 2 favors discretionary denial.

3. Factor 3 Favors Denial (Investment in Parallel Proceedings); before the institution decision, discovery will be near complete and the Court will have held a *Markman* hearing.

Factor 3 strongly weighs in favor of denial because both Emerging Auto and Petitioners will have expended considerable resources in the parallel litigation, including on the merits of Petitioners' invalidity positions, by the time the Board issues an institution decision. *See Sand Revolution II, LLC v. Cont'l Intermodal Grp.*, IPR2019-01393, Paper 24 at 10 (P.T.A.B. June 16, 2020) (noting that investment in invalidity contentions is relevant to this factor).

For factor 3, the Board considers "the amount and type of work already completed in the parallel litigation by the court and the parties at the time of the institution decision." *Fintiv*, IPR2020-00019, Paper 11 at 9. "This investment factor is related to the trial date factor, in that more work completed by the parties and court in the parallel proceeding tends to support the arguments that the parallel proceeding is more advanced, a stay may be less likely, and instituting would lead to duplicative costs." *Id.* at 10.

Here, the Board is projected to issue an institution decision on January 30, 2025. Emerging Automotive served its infringement contentions over a year earlier on January 18, 2024; on March 28, 2024, Petitioners served their invalidity contentions, nearly 10 months before the projected institution decision. EX2004; EX1024. Petitioners' invalidity contentions include claim charts addressing the same primary references, Kleve and Mikan, asserted by Petitioners in every ground of their Petition for the asserted claims in the co-pending litigation. EX2004, 12.²

Toyota and Patent Owner have already spent an entire day in Judge Gilstrap's court in relation to numerous technical motions related to infringement contentions, invalidity contentions, and motions to compel technical documents. EX2007. More are currently before the Court, including Toyota's attempt to modify its technical invalidity case. *Id.*

Additionally, the parties have already exchanged interrogatory responses, exchanged document productions, and completed at least four depositions of technical witnesses. EX2007. Moreover, Emerging Auto has spent hours reviewing materials on a "source code" computer from Toyota and Kia, with more reviews

² While Petitioners rely on the pre-issuance publication of Mikan here and the issued version of Mikan in the district court, the disclosures are the same.

scheduled soon. The Parties are deep into factor discovery and, indeed, the projected institution decision would come only about a month before the completion of fact discovery. EX1024. Indeed, the discovery cutoff in the district court case is March 3, 2025, meaning that a vast amount of discovery will be complete before the projected institution decision that is approximately four weeks earlier. *See id.*

Moreover, before the projected institution deadline, the parties will have fully briefed claim construction issues—none of which are addressed in the Petition—and the district court will have held a claim construction hearing. EX1024.

By the time the Board issues an institution decision, the district court has, and will have, spent considerable time and resources dealing with substantive motions and held a hearing on claim construction. This factor heavily favors denial. *Mylan Laboratories*, IPR2020-00440, Paper 17 at 15, 18 (“Specifically, if, at the time of the institution decision, the district court has issued substantive orders related to the patent at issue in the petition, this fact favors denial.”) (citing *Fintiv*, IPR2020-00019, Paper 11 at 9 and citing *E-One*, IPR2019-00161, Paper 16 at 8, 13, 20).

Moreover, both Emerging Auto and Petitioners will have expended substantial resources in the parallel litigation, including on the merits of Petitioners’

invalidity positions, where—as detailed below—there is significant overlap of issues.

Discretionary denial is therefore favored here, since the parties and the court will have invested substantial time and resources, including substantial motion practice and ongoing fact discovery, by the January 30, 2025 institution decision deadline.

4. Factor 4 Favors Denial (Overlap of Issues)

Factor 4 weighs strongly in favor of discretionary denial because there is substantial overlap between the claims, arguments, and evidence raised in the Petition and in Petitioners’ invalidity contentions in the parallel district court proceeding. Petitioners’ failure to offer any stipulation or other action to reduce the overlap between the proceedings only highlights the concerns of duplicative efforts and conflicting outcomes raised by *Fintiv* and the USPTO’s Interim *Fintiv* Procedure.

The Petition challenges each asserted claim in the district court litigation. In the district court litigation, Petitioners challenge each asserted claim using the same primary references—Kleve and Mikan. EX2004, 12. Petitioners’ common prior art and common challenges to the claims renders the “overlap between the two

proceedings [] substantial.” *Code200 Uab v. Luminate Networks Ltd.*, IPR2020-01506, Paper 10 at 11-12 (P.T.A.B. Feb. 16, 2021).

Moreover, Petitioners’ district court assertion of additional prior art and theories than those asserted here does nothing to alter the degree of overlap between the Petition and their invalidity contentions. *See, e.g., Fintiv*, IPR2020-00019, Paper 15 at 15 (finding the petitioner’s assertion of additional invalidity contentions “not relevant to the question of the degree of overlap for this factor”). Petitioners incorrectly argue that the Petition’s challenge of an additional dependent claim, weighs against discretionary denial (Pet., 69), but the Board has repeatedly ruled that such a fact does nothing to mitigate “substantial” overlap in issues between the proceedings where common prior art is presented and common independent claims are challenged. *Code200 Uab*, Paper 10 at 11-12 (“In light of the common prior art asserted here and in the [] district court case, as well as the common challenge to the sole independent claim and all but two dependent claims of the [challenged] patent, we agree with the Patent Owner that the overlap in issues between the two proceedings is substantial.”); *see also Teso LT UAB v. Luminati Networks Ltd.*, IPR2021-00122, Paper 12 at 10 (P.T.A.B. Apr. 20, 2021) (denial of institution favored where Petition’s prior art references were identified in the district court invalidity contentions, the same independent claims were challenged in both

proceedings, and “the *additional* claims challenged in the Petition are all dependent claims”).

Therefore, with this substantial overlap between the Petition and the parallel district court matter, there are particularly strong “concerns of inefficiency and the possibility of conflicting decisions” if the IPR is instituted. *See, e.g., Fintiv*, IPR2020-00019, Paper 11 at 12 (finding “concerns of inefficiency and the possibility of conflicting decisions [are] particularly strong” where there is substantial overlap).

Accordingly, factor 4 weighs strongly in favor of denial of institution. *See Teso LT, UAB v. Luminati Networks Ltd.*, IPR2021-00122, Paper 12 at 10 (P.T.A.B. Apr. 20, 2021) (finding “the overlap in issues between the two proceedings is substantial” where common art and common challenges to the independent claim were presented in both proceedings); *see also eClinical Works*, IPR2022-00229, Paper 10 at 12 (finding factor 4 weighed in favor of denial where Preliminary Invalidity Contentions showed overlap of asserted claims, art and arguments asserted in the Petition); *U.S. Venture, Inc. v. Sunoco Partners Mktg. & Terminals L.P.*, IPR2020-00728, Paper 10 at 12-14 (P.T.A.B. Oct. 1, 2020) (finding overlap between primary references asserted in Petition and litigation weighed in favor of denial).

Finally, Petitioners offer no stipulation, *Sotera* or otherwise. Petitioners signal that they intend to pursue the same invalidity theories in both forums. *See* Pet., 69. Because “both the Board and the district court would be analyzing and interpreting the same pieces of art, duplicating effort and potentially reaching inconsistent results,” factor 4 weighs heavily against institution. *See Samsung Elecs. Co. v. Clear Imaging Research, LLC*, IPR2020-01401, Paper 12 at 21 (P.T.A.B. Feb. 17, 2021) (finding overlapping claims challenged on the same prior art favored discretionary denial because duplication of work and potential for inconsistent decisions remained despite the petitioner’s stipulation to forego grounds asserted in Petition).

For each of these reasons, factor 4 strongly favors discretionary denial.

5. Factor 5 Favors Denial (Overlapping Parties)

Patent Owner is the plaintiff and Petitioners are defendants in the parallel litigations (EX2007; EX2008), and “because the petitioner and the defendant in the parallel proceeding are the same party, this factor weighs in favor of discretionary denial.” *Samsung v. Clear Imaging*, IPR2020-01401, Paper 12 at 21-22 (quoting *Fintiv*, IPR2020-00019, Paper 15 at 15) (finding factor 5 weighs in favor of discretionary denial given petitioner’s status as co-defendant in parallel litigation). When “a petitioner in inter partes review and a defendant in a parallel district court

proceeding are the same, or where a district court is scheduled to go to trial before the Board's final decision would be due in a related inter partes review, this factor weighs in favor of discretionary denial." *Id.* (quoting *Sand Revolution*, IPR2019-01393, Paper 24 at 12-13). Here, Toyota and Kia are both the petitioners and each is a defendant in the district court litigation, and that district court proceeding "is scheduled to go to trial before the Board's final decision would be due" here. *Id.*

This factor therefore weighs in favor of exercising discretion to deny institution.

6. Factor 6 Favors Denial (Other Circumstances)

There are no "other circumstances" that support institution.

V. The Petition should be denied in view of the co-pending EPR.

The Board should likewise decline to expend its resources to perform a parallel analysis, as the Office is already considering the validity of the '659 patent in a post-issuance ex parte review proceeding brought by Unified Patents.

On March 25, 2024, Unified Patents LLC filed an ex parte review of the '659 patent, challenging all claims. EX2017. Unified Patents is a membership platform that challenges patents that are infringed by its members, and the Toyota petitioner is a member. EX2018, 3.

On September 4, 2024, the Examiner issued an Office Action rejecting all

claims of the '659 patent. EX2019. The Board should not expend its valuable resources reconsidering the validity of the '659 patent when the issue is already before the Office in a parallel proceeding. *See Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*, 84 Fed. Reg. 16,654, 16,657 (Apr. 22, 2019) (“[t]he Board . . . may deny institution under 35 U.S.C. [§] 325(d) of a requested AIA trial proceeding if a parallel Office proceeding, for example, is in a more advanced stage and involves overlapping issues with the proposed AIA trial proceeding.”).

VI. Section 311(B) of the AIA and the SCOTUS Ruling in *SAS* Prevent Institution

The Petition must be denied under 35 U.S.C. § 311(b). Regardless of whether Kleve is prior art under 35 U.S.C. § 102, it cannot be used for IPR. While Section 102 identifies numerous disclosures that qualify as “prior art,” an IPR may only be instituted on a subset of that art. Specifically, §311(b) allows *inter partes* review “only on the basis of prior art consisting of patents or printed publications.” 35 U.S.C. § 311(b). Petitions thus may not be instituted on prior art consisting of “public use” or “sales,” as recited in §102(a)(1) or a patent application that was filed before the effective date, but published after, as contemplated in §102(a)(2).

The '659 patent properly claims priority to U.S. Appl. No. 14/063,638, filed on October 25, 2013, which includes the same specification because it is linked only

by continuations. Pet., 6. As such, there is no, and can be no, dispute that the '659 patent is entitled a priority date of at least October 25, 2013.³ *Id.*; Pet., 6-7.

Kleve is not “prior art consisting of patents or printed publications” as required by § 311(b). Kleve is a patent publication, and thus not prior art consisting of a patent. EX1005, 1. Moreover, Kleve was not published until May 8, 2014 (*id.*), well after the priority date of the '659 patent, whether it be October 25, 2013 or earlier. Petitioners make no argument that Kleve was publicly available before its publication. As such, Kleve is not prior art consisting of a printed publication because “[f]or a reference to qualify as a printed publication, ‘before the critical date the reference must have been sufficiently accessible to the public interested in the art.’” *See, e.g., Valve Corp. v. Ironburg Inventions Ltd.*, 8 F.4th 1364, 1373 (Fed. Cir. 2021) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1568 (Fed. Cir. 1988)). As such, grounds 1-2 of the Petition cannot be instituted because it relies on Kleve.⁴

³ While Petitioners argue that the '659 patent is not entitled to its April 22, 2011 priority date, the Board need not resolve that question to deny institution under any of the arguments presented herein, as the Petition fails regardless.

⁴ Patent Owner recognizes and notes that this issue is currently on appeal before the

Moreover, because the Supreme Court's decision in *SAS Institute, Inc. v. Iancu*, 584 U.S. 357 (2018) prohibits institution on fewer than all petitioned grounds, the entirety of the Petition, grounds 1-6, must be denied. Under *SAS*, because institution is not authorized for grounds 1-2, institution is not authorized for any additional grounds.

VII. Conclusion

For the numerous distinct reasons discussed herein, institution should be denied.

Dated: October 30, 2024

/Jerry Tice/
Jerry D. Tice II
Reg. No. 73,582 (Lead counsel)
Aaron R. Hand
Reg. No. 80,694
Brenda Entzminger
Reg. No. 76,896
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: 650-318-6774
Facsimile: 415-426-4744
jtice@bdiplaw.com

Counsel for Patent Owner

Federal Circuit in *Lynk Labs, Inc. v. Samsung Electronics Co.*, No. 2023-2346 (Fed. Cir.). The Federal Circuit recently held oral argument in the case, and a decision is forthcoming that will address this issue.

37 C.F.R. §42.24(d) CERTIFICATION

The undersigned hereby certifies that this submission, excluding the table of contents, table of authorities, exhibit list, certificate of word count, and certificate of service, contains 10,419 words, as determined using the standard word counting feature of the Microsoft Word program.

Dated: October 30, 2024

/Jerry Tice/
Jerry D. Tice II
Reg. No. 73,582 (Lead counsel)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: 650-318-6774
Facsimile: 415-426-4744
jtice@bdiplaw.com

Counsel for Patent Owner

CERTIFICATE OF SERVICE

Petitioner has consented to e-mail service in this proceeding. Pursuant to 37 C.F.R. §42.6, the undersigned certifies that on October 30, 2024, 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
James R. Barney - james.barney@finnegan.com
Aidan Skoyles - aidan.skoyles@finnegan.com
Nicholas Eitsert - nicholas.eitsert@finnegan.com

QUINN EMANUEL URQUHART & SULLIVAN, LLP
James M. Glass – jimglass@quinnemanuel.com
Quincy Lu - quincylu@quinnemanuel.com
Ron Hagiz - ronhagiz@quinnemanuel.com
Jeffrey S. Gerchick - jeffgerchick@quinnemanuel.com
Brett Watkins - brettwatkins@quinnemanuel.com

Dated: October 30, 2024

/Jerry Tice/
Jerry D. Tice II
Reg. No. 73,582 (Lead counsel)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: 650-318-6774
Facsimile: 415-426-4744
jtice@bdiplaw.com

Counsel for Patent Owner